



ID-nummer: [REDACTED]

Eksamensbesvarelse i

REV 24031

REGNSKAPSORGANISASJON OG SYSTEMER

FAGOPPGAVE

Utleveringsdato: 6. april 2010

Innleveringsdato 4. mai 2010

Studiested: BI Nettstudier

Sammendrag

Denne oppgaven er besvarelse på eksamensoppgaven i REV 24031 i Regnskapsorganisasjon og systemer for BI Nettstudier våren 2010.

Oppgaven har fire deler. Første del omhandler internkontroll og gjør rede for COSO-modellens struktur og viktige komponenter. Videre går jeg spesifikt inn på hvordan rutiner og instruksjoner inngår i denne modellen. Justeringsreglene for merverdiavgift ble innført 1.1.2008 og jeg vil diskutere bakgrunnen for disse justeringene samt skrive en instruks for økonomisjef og en rutinebeskrivelse for oppfølging av justeringsreglen for merverdiavgift.

Del 2 omhandler risikoanalyse. Den tar utgangspunkt i risikoen for feil knyttet til varebeholdninger og hvordan dette påvirker regnskapet. Jeg viser et eksempel på et regnskap hvor varebeholdningene er så store at de kan påvirke selskapets resultat og balanse. Videre vil jeg se på internkontrolltiltak som kan redusere risikoen i dette spesifikke tilfellet, og til slutt vil jeg gå nærmere inn på hva som kan anses som operasjonell risiko knyttet til varebeholdningen.

Personopplysninger i lønssystemet er tema i oppgavens del 3. Her gjør jeg rede for lovbestemmelser som vedrører registrering og oppbevaring av personopplysninger i lønssystemet før jeg foreslår kolonner i systemet som er nødvendig for å bokføre lønnskostnaden automatisk. Videre ser jeg på hvordan opplysningene kan beskyttes med kryptering og elektronisk signatur og på hva lovgivningen sier om risikoen for tap av tabellene i regnskapssystemet.

Siste del av oppgaven dreier seg om justering av merverdiavgift og jeg viser hvilke kolonner jeg trenger i regnskapssystemet for å kunne automatisere beregningen av avgiftsjusteringen.

Table of Contents

Sammen drag	2
Oppgave 1: Internkontroll.....	4
a) Redegjør for Coso Modellen (struktur og viktige komponenter).....	4
b) Drøft hvordan rutiner og instruksjer inngår i COSO modellen.....	6
c) Orienter om bakgrunnen for justeringsreglene.....	7
d) Instruks for økonomisjef	8
e) Rutinebeskrivelse for oppfølging av merverdiavgift	9
Oppgave 2: Risikoanalyse.....	13
a) Risiko for feil i regnskapet som kan skyldes feil eller manipulering med varebeholdninger:.....	13
b) Eksempel på regnskap med varebeholdninger: Lines Kiosk og Parfumeri AS	14
c) Gjør rede for internkontrolltiltak som kan redusere denne risikoen for regnskapsmanipulasjon	15
d) Operasjonell risiko	18
Oppgave 3: Personopplysninger i lønssystemet.....	20
a) Gjør rede for lovbestemmelser som direkte vedrører registrering og oppbevaringer av personopplysning i lønssystemet.....	20
b) Kolonner i tabeller for automatisk postering av lønnskostnader.....	22
c) Tilgangskontroller.....	24
d) Konfidensialitet og kryptering	25
e) Elektronisk signatur	26
f) Tabellen går tapt.....	27
g) Har bedriften behov for sikring utover lovkravet?.....	28
Oppgave 4: Justering av merverdiavgift	29
Kildehenvisninger.....	31
Appendix 1: Coso modellen	32
Appendix 2: Regnskap for Line Kiosk & Parfumeri AS.....	33
Vedlegg 3: Rutinen for justering av merverdiavgift.....	36
Vedlegg 4: Tabeller vedrørende justering av merverdiavgift og utleieobjekter.....	39

Oppgave 1: Internkontroll

a) Redegjør for Coso Modellen (struktur og viktige komponenter)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ble opprettet for å forske på uredelig (fraudulent) finansiell rapportering (www.coso.org) og publiserte 1992 rapporten "Internkontroll- et integrert rammeverk"¹. I rapporten presenteres en modell for internkontroll, omtalt som COSO-modellen (se vedlegg 1). I COSO-modellen defineres internkontroll som (norsk oversettelse: Moen og Havstein 2009):

"en prosess, igangsatt og gjennomført av virksomhetens styre, ledelse og ansatte. Den utformes for å gi rimelig sikkerhet vedrørende måloppnåelse innen følgende områder:

- Målrettet og kostnadseffektiv drift (herunder ytelses- og lønnsomhetsmål og beskyttelse av eiendeler)
- Pålitelig regnskapsrapportering og økonomisk informasjon
- Overholdelse av gjeldende lover og regler"

At internkontroll er en prosess vil si at dette er en kontinuerlig og "styrt" aktivitet, snarere enn et resultat. Hensikten er at selskapet skal planlegge, gjennomføre og evaluere internkontrollen. COSO modellen viser at de tre målsettingene kan nås gjennom samspill mellom fem komponenter; kontrollmiljø, risikovurderinger, kontrollaktiviteter, informasjon og kommunikasjon samt overvåking.

Kontrollmiljø kan sies å være grunnpilaren i internkontrollen og beskrives som holdningene til internkontroll i bedriften. I kontrollmiljøet inngår faktorer som organisasjonskultur, styrets og ledelsens holdninger til internkontroll og deres handlinger, de ansattes integritet og kompetanse, myndighetsdelegering og opplæring (www.coso.org). Et godt kontrollmiljø er en forutsetning for god internkontroll.

COSO- modellen sier videre at selskapet må foreta risikovurderinger ut fra eksterne og interne faktorer som kan hindre selskapet å oppnå sine mål. Videre bør selskapet

¹ Internal Control- Integrated Framework, The Committee of Sponsoring Organizations of the Treadway Commission , AICPA 1992

vurdere sannsynligheten for at risikoene inntreffer og hvilke konsekvenser det vil få foretaket. Risikovurderinger må gjennomføres jevnlig ettersom både interne og eksterne forutsetninger endrer seg over tid.

Når man har analysert de risiki bedriften står overfor, må det iverksettes kontrollaktiviteter der hvor det anses som hensiktsmessig. Bedriften må også vurdere hvor mye og hvilken risiko den er villig til å ta. Det vil si at den må definere sin risikoappetitt. Kontrollaktivitetene er prosedyrer og tiltak for å håndtere risiko og sikre at målene for internkontrollen nås. Eksempler på kontrollaktiviteter er arbeidsdeling, avstemminger og fysisk sikring av eiendeler. Det vil alltid være en kost-nytte vurdering på de tiltakene som iverksettes og bedriften skal være klar over at man må ta risiko for å kunne skape avkastning. Helhetsprinsippet (Moen og Havstein, 2009), som sier at bedriften må finne den optimale sammensetningen av kontrollaktiviteter hensyntatt de risiki som bedriften møter og bedriftens risikoappetitt, bør ligge til grunn.

Informasjon og kommunikasjon i COSO-modellen handler om å identifisere, registrere, bearbeide og kommunisere informasjon slik at ledelsen og de ansatte har tilstrekkelig informasjon for å utføre sine oppgaver. Det handler om å produsere relevante rapporter i tide slik at ledelsen kan ta velinformerte beslutninger og at de ansatte kjenner sine ansvarsområder og vet hva selskapet forventer av dem. Informasjon og kommunikasjon dreier seg også om effektiv informasjonsutveksling med eksterne parter (www.coso.org).

Overvåking er det siste elementet i modellen. Det innebærer å analysere og overvåke om den interne kontrollen fungerer som forutsatt og at den er av tilfredsstillende kvalitet. Overvåkingen bør gjøres jevnlig, jmfør definisjonen på internkontroll; det skal være en prosess og ikke et statisk bilde. Dersom det er avvik i internkontrollen skal dette rapporteres slik at ledelsen kan gjøre de nødvendige justeringene i rutiner og retningslinjer. Overvåkingen innebærer også at man følger opp at nødvendige endringer i kontrollrammeverket er gjennomført og gjenspeiler de risiki som bedriften møter.

b) Drøft hvordan rutiner og instruksjer inngår i COSO modellen

Instruksjer og rutiner inngår i COSO- modellen på ulike måter. Instruksjer handler om fordeling av ansvar og myndighet (Moen og Havstein 2009, s 95), for eksempel fra styret til daglig leder. Instruksene inngår dermed direkte i COSO modellen som en del av kontrollmiljøet. Kontrollmiljøet er som nevnt i oppgave 1 a fundamentet for at internkontrollen skal fungere som forutsatt. Formelle instruksjer vil gi et rammeverk for hvordan bedriften ”styres”, og hvor ansvar og delegert myndighet ligger.

Instruksene kan imidlertid ikke overstyre aksjelovens krav om at det er styret som har det overordnede ansvaret. For at instruksene skal ha en positiv innvirkning på kontrollmiljøet er det viktig at styret følger opp både de beslutningene som er delegert og eventuelle avvik. Slik vil nytten av formelle instruksjer øke med et aktivt og involvert styre og dette vil igjen påvirke hele kontrollmiljøet. Delegering av ansvar og myndighet gjelder for alle nivåer i organisasjonen, selv om man da ikke bruker begrepet instruks. For god internkontroll er det en forutsetning at den enkelte er klar over hva han eller hun er ansvarlig for og hvilke beslutninger som kan tas.

Rutiner benyttes for å strukturere den regnskapsmessige behandlingen av det som skjer i de ulike forretningsprosessene (Moen og Havstein, 2009). Rutinene viser hvilke aktiviteter som skjer fra en hendelse eller handling til dette reflekteres i regnskapet. Dette er altså en måte bedriften velger å organisere seg på for å nå sine målsettinger. Å dele forretningsprosessene inn i rutiner gir oversikt over prosessen fra start til slutt og tydeliggjør involverte aktiviteter. Det blir da enklere å bedømme hvor i prosessene risikoen for at det skjer feil eller mislighold er størst. Ved at bedriften beskriver, lager flytdiagram eller lignende kan den blant annet identifisere hvem som er/ må være involvert i prosessen, hvor man er avhengig av IT-systemer, hvor det er kritiske grensesnitt og hvor enkeltpersoner kan ha for mange oppgaver. Dette vil lette arbeidet med å bedømme risiko i prosessen og gjør det enklere for bedriften å identifisere hvor de ønsker å iverksette kontrolltiltak for at regnskapet skal oppfylle kvalitetskravene i bokføringsloven. Enkelte av kontrollaktivitetene vil typisk ha en slags rutinebeskrivelse knyttet til seg. Det kan for eksempel være der kontrollaktiviteten er etterkontroll, som avstemming. Det viktig å skille mellom

rutinen i forretningsprosessen og kontrollaktiviteten, ettersom kontrollaktiviteten er en "sjekk" på at rutinen er fulgt.

Operasjonell risiko er risikoen for manglende effektivitet og måloppnåelse i den daglige driften (Moen og Havstein, 2009, s 100), se mer om dette i oppgave d. Med en klar ansvarsfordeling, gode rutiner og hensiktsmessige kontroller vil sannsynligheten for at bedriften når sine mål øke og det kan være med på å redusere den operasjonelle risikoen. Videre må man se rutiner og instruksjer i sammenheng med kontrollmiljøriskoen. Et dårlig kontrollmiljø, med lite fokus på å følge fastsatte rutiner og retningslinjer, vil øke risikoen selvom rutinene i utgangspunktet er svært gode. Gode rutiner kan derfor ikke erstatte kontrollaktivitetene fordi selskapet må forsikre seg om at rutinene faktisk følges.

I tillegg til rutinene som bedriften har for å nå sine forretningsmål, bør det også utarbeides rutiner for å følge opp feil og avvik som avdekkes og bruke denne informasjonen for å forbedre internkontrollen. Hvordan dette gjøres må sees i sammenheng med bedriftens størrelse og bransje.

Rutinene spiller også en viktig rolle når det gjelder å beholde kunnskap i bedriften /stillingen ved endringer i ansettelsesforhold.

c) Orienter om bakgrunnen for justeringsreglene

Justeringsreglene ble innført 1.1.2008 og omhandler rett og plikt til justering av tidligere fradragført inngående merverdiavgift for kapitalvarer dersom forutsetningene for fradraget endrer seg. Kapitalvarer er i innstillingen til Odelstinget "Inns. O. Nr. 94 (2006-2007) definert som fast eiendom og driftsmidler over en viss verdi. Odelstingsproposisjon nr 59 (2006-2007) viser til fire hovedgrunner for innføring av justeringsreglene:

1) Kapitalvarens natur: Kapitalvarer skal benyttes over lang tid i virksomheten og det er derfor mulig at forutsetningene for fradragretten kan endre seg i bruksperioden. Retten til fradrag på kjøpstidspunktet kan dermed være misvisende og ikke representativ for varens bruk gjennom deler av varens levetid. En mulighet til å

justere for inngående merverdiavgift, vil føre til en merverdiavgiftsbehandling som mer korrekt reflekterer bruken av varen.

2) Incentiv til å tilpasse seg fradragene: Kapitalvarer er gjerne kapitalintensive og dette, sammen med lang brukstid kan gi insentiv til for eksempel å gå til innkjøp av noe i næringsformål for siden å ta det i bruk privat.

3) Harmonisering med regelverk i EU: Innstillingen viser også til at tilsvarende justeringsregler som det som ble innført i 2008 blant annet er vanlig i alle EU landene.

4) Problemer i dagens regelverk: Det fremgår av Ot.prp.nr 59 at dagens regelverk kan virke konkurransevridende og at det er lite fleksibelt. Regelverket er konkurransevridende fordi situasjonen på kjøpstidspunktet ikke nødvendigvis tilsvarer situasjonen ved bruk. En bedrift som øker bruken av en kapitalvare i avgiftspliktig virksomhet burde få et økt fradrag slik at han konkurrerer på like vilkår som en bedrift som har høyere andel i avgiftspliktig virksomhet i utgangspunktet. Regelverket anses som lite fleksibelt fordi dagens tilbakeføringsbestemmelser i merverdiavgiftloven § 21 tredje ledd bare gjelder fast eiendom og ikke kapitalvarer. I tillegg er det bare er anledning til full tilbakeføring av fradragført inngående merverdiavgift, det er altså ingen forholdsmessig justering. Den korte frigjøringstiden kan også gi incentiv til tilpasning til loven (se punkt 2).

Hensikten med det regelverket som ble innført 1.1.2008 var at det skulle virke begrensende på tilpasninger for å unngå merverdiavgift og motvirke konkurransevridninger. I tillegg skulle avgiftsberegningen i størregrad gjenspeile reelle forhold, både faktiske og økonomiske.

d) Instruks for økonomisjef

En instruks er en "ordre, forskrift eller samling av ordensregler, f.eks. for en arbeidsplass, for en stillingsinnehaver eller for bruken av utstyr" (Store norske leksikon online, [ww.snl.no](http://www.snl.no)). Av en instruks skal det fremgå hva som skal overholdes

/ gjøres innenfor et gitt område, snarere enn en detaljert beskrivelse om hvordan noe skal gjøres. Det vil fremgå av rutinebeskrivelsen jf. oppgave 1e.

Instruks for økonomisjef:

Omfang:

Denne instruksjonen gjelder for oppfølging av justeringsreglene for merverdi.

Oppgaver:

Instruks for økonomisjef som særskilt regulerer økonomisjefs ansvar vedrørende justeringsreglene for merverdiavgift.

Økonomisjefen har delegert ansvar fra daglig leder og rapporterer til daglig leder.

Økonomisjefen har daglig ansvar for:

- Utarbeidelse og oppdatering av rutiner for justering av merverdiavgift
- Å påse at rutinene for justering av merverdiavgift følges
- Å utarbeide et hensiktsmessig kontrollrammeverk for justering av merverdiavgift
- Å påse at kontrollrammeverket til "en hver tid" gjenspeiler de risiki som foretaket møter (vil normalt gjøres gjennom en jevnlig gjennomgang av internkontrollen)
- Å regelmessig presentere kontrollrammeverket for bedriftens styre, herunder forklare hvordan endringer internt eller i bedriftens omverden er reflektert i kontrollrammeverket (vil normalt gjøres gjennom en generell gjennomgang av internkontrollen).
- Å påse at avdelingen innehar tilstrekkelig kompetanse for å utføre nødvendige oppgaver, herunder ansvar for kompetanseutvikling og rekruttering

e) Rutinebeskrivelse for oppfølging av merverdiavgift

Jeg antar i denne oppgaven at hvert utleieobjekt kun har en leietaker, men at denne ikke nødvendigvis er avgiftspliktig for hele sin næringsvirksomhet.

Denne rutinebeskrivelsen er utarbeidet for regnskapsmedarbeider som er ansvarlig for oppfølging av merverdiavgift og rapportering til myndighetene. I praksis vil det være

hensiktsmessig med en beskrivelse som er enda mer detaljert i forhold til det regnskapssystemet som bedriften bruker.

Rutinebeskrivelse for oppfølging av justeringsreglene for merverdiavgift.

Rutinen gjelder for merverdiavgift (mva) knyttet til nybygg, på- eller ombygning (heretter byggekostnadene) for bedriftens eiendommer. Videre gjelder den dersom summen av byggekostnadene per utleieobjekt i løpet av et år har en inngående mva større enn 100 000 kroner. Justeringsreglene gjelder i ti år etter hendelsen fant sted.

Ved anskaffelse av ny eiendom føres eiendommen inn i bedriftens eiendomsregister. Ansvarlig for registrering er den som har ansvar for kontraktsinngåelse (heretter selger). Ved prosjekter på eiendommer (nybygg, om- eller påbygging) i eiendomsregisteret, skal ansvarlig prosjektleder inkludere økonomiavdelingen i planlegging for tidlig å kunne avgjøre behandling av mva knyttet til prosjektet. Alle fakturaer relatert til prosjektene sendes økonomiavdelingen for registrering og bokføring i regnskapssystemet. Økonomisjef skal godkjenne klassifiseringen av prosjektene som kapitalvarer eller om det anses som vedlikehold eller drift av eiendommen. Vurderingen gjøres ut fra hvorvidt standarden på bygget endres og begrunnelsen registreres i eget skjema, underskrives og arkiveres sammen med relevante bilag. Regnskapsmedarbeider er ansvarlig for arkivering i henhold til bokføringsloven. Dersom en eller deler av en eiendom vurderes solgt skal økonomiavdelingen også være involvert i prosessen for å kunne fastslå konsekvenser for mva- behandlingen.

Ved inngåelse av leiekontrakt vil det være behov for spesiell informasjon om leietaker for å kunne følge opp merverdiavgiftsforpliktelsene. Det er bedriftens selger, sammen med juridisk ansvarlig, som har ansvar for inngåelse av leiekontrakten. Bedriften har standardiserte kontrakter hvor det fylles ut opplysninger om leietakers avgiftsstatus. Leietaker plikter i henhold til kontrakten å informere utleier dersom han foretar endringer i sin avgiftsstatus. Leietaker plikter også å informere om på- eller ombyggings tiltak utført for egen regning på eiendommen.

Selger sender kopi av signert kontrakt til regnskapsmedarbeider og lagrer original i brann- og tyverisikkert skap hos juridisk ansvarlig.

På bakgrunn av inngått leiekontrakt oppdaterer regnskapsmedarbeider regnskapssystemet med nødvendige opplysninger om leietaker (på reskontro over utleieobjekter), blant disse leietakers avgiftsplikt. Systemet vil da beregne fradragsprosent på fullføringstidspunktet for eiendommen og opprinnelig fradrag for inngående mva.

Det er i hovedsak selger/driftsansvarlig som har kontakt med leietaker. Ved opplysning om endring i avgiftsstatus eller oppsigelse av avtale skal dette skriftlig sendes videre til regnskapsmedarbeider. Videre plikter drift å informere regnskapsmedarbeider dersom lokaler blir stående tomme eller utsatt for brann.

Økonomiansvarlig skal hver annen måned, 14 dager før termin for mva-betaling sende mail til selskapets selgere med en oversikt over alle eiendommene innenfor justeringsregelgrensen, og be om tilbakemelding på endringer i utleieforhold. Eventuelle opplysninger selger har oppgitt i perioden, inkluderes i utgående mail. Alle selgere skal bekrefte eller endre opplysningene for å sikre fullstendighet og riktig periodisering. Dersom regnskapsmedarbeider ikke får tilbakemelding tar han direkte kontakt med selger. Regnskapsmedarbeider registrer eventuelle endringer i regnskapssystemet på den dato endringen fant sted. Typer endringer er forhåndsdefinert i systemet. Det blir automatisk beregnet ny fradragsprosent per utleieobjekt.

Dersom forskjellen mellom ny og opprinnelig fradragsprosent for det enkelte utleieobjekt er mindre enn 10 prosentpoeng er ingen justering av merverdiavgiften.

Dersom differansen mellom fradragsprosentene er større enn 10 prosentpoeng og endringen skyldes opphør av virksomhet eller overdragelse av utleieobjektene til andre, skal justering av inngående merverdiavgift foretas samlet for den resterende delen av justeringsperioden.

Dersom differansen mellom fradragprosentene er større enn 10 prosentpoeng, men endringen ikke skyldes opphør av virksomhet eller overdragelse av utleieobjektene til andre, skal justering av inngående merverdiavgift foretas årlig.

Dersom det er kun en del av fast eiendom som endrer bruk eller overdras får det ingen konsekvenser for justeringsplikten.

Systemet er satt opp slik at kombinasjonen av inndata for differanse i fradragprosent og type endring i utleieforhold gir beskjed om hvorvidt det skal være samlet eller årlig justering av merverdiavgiften.

Systemet beregner justeringsbeløp per utleieobjekt. Økonomiansvarlig tar ut rapport for økonomisjefen gjennomgang, signering og arkivering for kontrollformål.

Rapporten viser beløp per utleieobjekt og opprinnelig fradragbeløp slik at økonomisjefen kan vurdere rimeligheten i tallene. På bakgrunn av godkjent rapport fyller regnskapsmedarbeideren ut og sender normal omsetningsoppgave med spesifikasjon av eventuelt justeringsbeløp samlet for alle utleieobjektene

Årlig gjør juridisk ansvarlig en gjennomgang av alle kontrakter i arkivet som er inngått eller endret inneværende år, og avstemmer dette mot eiendomsregisteret. I etterkant av dette gjør regnskapsmedarbeideren en årlig gjennomgang av alle eiendommer i eiendomsregisteret for å identifisere hvilke eiendommer som ligger innenfor rammen av eiendommer med justeringsplikt.

Se vedlegg 3 for flytdiagram av rutinen for oppfølging av merverdiavgift

Oppgave 2: Risikoanalyse

- a) Risiko for feil i regnskapet som kan skyldes feil eller manipulering med varebeholdninger:

Risiko for feil i regnskapet kan skyldes bevisste og ubevisste feil, samt manipulering av varebeholdningen. En varebeholdning som ikke er korrekt kan føre til at resultatregnskapet viser uriktig varekostnad samt feil beholdning av varer under tilvirkning og ferdig tilvirkede varer. Balanseposten som påvirkes er varebeholdningen (Moen og Havstein 2009, s 210). Kvalitetskravene til balansen vil dreie seg om at varelageret eksisterer og tilhører bedriften, samt at det er riktig verdsatt. Dette vil igjen påvirke posten(e) i resultatregnskapet.

Riktig verdsettelse av varelageret er avhengig av riktig kvantum, riktig (kost-)pris og riktig kvalitet på varene. Feil kvantum kan oppstå ved at mottatte kvantum varer ikke tilsvare bestilt kvantum eller at de ikke registreres på lageret/i logistikksystemet og dermed holdes utenfor bedriftens regnskap. Avvik kan også skyldes tyveri fra lageret eller at uttak ikke registreres riktig. Det kan også skyldes feil ved direkte målinger av varelageret, som for eksempel at varetellingen ikke er riktig fordi varer som ikke er på en forhåndsdefinert liste ikke telles eller at man ikke tar hensyn til kvaliteten på varen. At bedriften deler lager med andre eller har solgte varer på lager kan også gi utfordringer, ved at bedriften bevisst eller feilaktig innlemmer varer den ikke eier i varelageret.

Risiko for at varelageret er feil priset kan skje som følge av at de opprinnelige prisdataene er registrert feil, det vil si at tabellene for faste data i systemet ikke er korrekte. Det kan også ha skjedd uautoriserte endringer i dataene, enten ved at brukere har gjort feil eller bevisst endret dataene eller at uautoriserte personer har fått tilgang. I tillegg kan svikt i, eller manglende, rutiner føre til at prisene ikke er oppdatert slik de skal. Av regnskapsloven § 5.1 følger det at varer er omløpsmidler og skal vurderes etter laveste verdis prinsipp (§ 5.2). Manglende kompetanse eller retningslinjer i bedriften kan føre til at varelageret ikke klassifiseres riktig, noe som kan føre til konsekvenser for anslag for virkelig verdi og anskaffelseskost. Videre er

bedriften avhengig av at systemene som behandler og beregner data om varelageret gjør dette korrekt.

Risiko for feil eller forringelse av kvalitet kan skyldes at oppbevaringen skjer under ikke-optimale forhold. Det kan også være at varenes kvalitet ikke kontrolleres ved mottak eller at uautorisert tilgang til lageret forringer kvaliteten på varene. Lang lagertid/dårlig lagerstyring av ferskvarer eller varer som er "in" (klær, ukeblader) kan føre til at disse går ut på dato og at verdien reduseres. Et optimalt lagernivå vil også kunne redusere risikoen for ukurans i framtiden.

En annen feilkilde i regnskapet kan være at ledelsen ikke er villige til å ta tap. Det betyr at selv om tap i varelageret er påvist, ønsker ledelsen ikke å presentere bedriftens riktige resultat.

b) Eksempel på regnskap med varebeholdninger: Lines Kiosk og Parfymeri AS

Regnskapet for Lines Kiosk og Parfymeri AS er valgt ut på grunn av størrelsen på varebeholdningen i forhold til totale eiendeler, og på grunn av varekostnadens andel av inntektene. Bedriften har negativ arbeidskapital (omløpsmidler – kortsiktig gjeld), og likviditetsgrad 1 (omløpsmidler / kortsiktig gjeld), som sier noe om bedriftens evne til å dekke sine betalingsforpliktelser, er 0,92. Det er anbefalt å ha en likviditetsgrad høyere enn 1,5. Den finansielle stillingen til selskapet per 31.12.2008 kan gi incentiver til å vise frem et bedre regnskap enn det som er korrekt, for eksempel fordi eieren ønsker tilgang på ny kapital eller vil selge bedriften. Se regnskapet i vedlegg 2.

Fra regnskapet kan vi se at salgsinntektene i 2008 er høyere enn i 2007. Dette kan indikere noe høyere salg eller kun en generell prisøkning. Feil kan oppstå dersom prislistene i IT-systemene ikke er korrekt oppdatert. For små varer vil det også kunne skje at salg holdes utenfor regnskapet eller registreres feil. Typisk eksempel er hvis kontanter legges igjen på disken fordi kunden har det travelt. Dersom kontantene blir registrert kan det hende at ekspeditøren ikke husker helt hvilken vare det dreide seg om. Videre er vareforbruket lavere enn året før samtidig som bedriften har et høyere

lagernivå. Det kan være en risiko for at varer ikke er registrert på lageret, at varer på lageret ikke tilhører bedriften eller at det er feil i periodiseringen i regnskapet. De to siste punktene kan skyldes bevisste feil, eller at varer er levert rett før årsskiftet og faktura ikke mottatt og det er dårlige rutiner for avsetninger.

Videre er det typisk både for kiosk og parfymeri-bransjen å være utsatt for tyveri/nasking. Små og billige varer kioskbransjen og små luksusprodukter som passer i vesker og lommer gjør at svinn kan være betydelig. Bedriften har fokus på nærings- og nytelsesmidler. Dette er typisk varer med holdbarhetsdato og ferskvarer, men også for eksempel aviser og blader, alle med høy risiko for ukurans (svinn). Ettersom regnskapet ikke gir separate tall for svinn antar jeg at dette er inkludert i vareforbruket. Endringene i vareforbruk og lager kan derfor skyldes at svinn var et langt større problem i 2007 enn i 2008.

Som nevnt innledningsvis er bedriftens økonomiske situasjon slik at den gir incentiv til å ikke gi korrekt informasjon. Ved å rapportere et lavere lagernivå vil bedriften kunne oppnå en positiv egenkapital. En omklassifisering av gjelden fra kortsiktig til langsiktig vil også gi et noe bedre inntrykk av soliditeten. Videre ville det gitt et bedre resultat dersom bedriften ikke hadde tatt inn alle varekostnadene. Man kan i tillegg tenke seg at bedriften lar de ansatte kjøpe varer billig for å redusere lønnskostnader og unndra avgifter til myndighetene. I Lines regnskap ser vi at lønnskostnadene har økt vesentlig fra 2007 til 2008, det skyldes sannsynligvis ekstra personell, men tatt i betraktning utviklingen i varekostnad kan man også tenke seg muligheten for feil klassifisering av kostnader.

- c) Gjør rede for internkontrolltiltak som kan redusere denne risikoen for regnskapsmanipulasjon

Det er en rekke tiltak Lines Kiosk og Parfymeri AS kan iverksette for å begrense risikoen for feil i regnskapet relatert til varelageret. Når det gjelder prislister i IT-systemene som benyttes (logistikksystem og regnskapssystem)/kasseapparatet må det være rutiner for at listene oppdateres regelmessig og at eventuelle endringer alltid skal godkjennes av daglig leder. Dette gjøres for eksempel ved at kun daglig leder

kan oppdatere IT-systemet. Det kan være hensiktsmessig å ha et kasseapparat/system som benytter strekkodene som er på varen, slik kan man sikre at kostprisendringer registreres og salget kan kobles opp til lagersystemet. Kasseapparatet bør videre registrere ekspeditør slik at man kan se tilbake på salg per ansatt. Bedriften bør videre ha retningslinjer for at kunder ikke får legge igjen kontanter på disken, samt at de ansatte ikke får ha kontanter på seg. Private kontanter skal oppbevares i vesker/lommebøker på "pauserommet". Dette for å unngå feil, samt beskytte de ansatte mot mistanke om å unndra kontanter.

Når det gjelder bestilling av varer bør dette fortrinnsvis være initiert av logistikksystemet, når lagerbeholdningen når et minimumsnivå. Bestillingen bør kun gjøres av daglig leder ettersom lagernivået har stor innvirkning på resultatet. Lagernivået bør være avklart i daglig leders instruks og /eller diskuteres jevnlig med styret. Ikke autoriserte bestillinger fører ikke nødvendigvis til at det er feil i regnskapet, men kan føre til et uhensiktsmessig nivå på lagerbeholdningen og dermed redusert lønnsomhet for bedriften. Systemgenererte bestillinger vil redusere risikoen for ikke autoriserte bestillinger. Ved bestilling av varer bør ordrebekreftelsen registreres/tas vare på og systemet bør registrere hvem som har initiert bestillingen. Dersom bestillinger ikke initieres av systemet bør man benytte forhåndsdefinerte formularer for å øke sannsynligheten for at alle nødvendige opplysninger blir registrert.

For å sikre at Lines Kiosk og Parfymeri AS mottar det kvantum varer som er bestilt med riktig kvalitet, bør det gjøres en kontroll av mottatte varer mot pakkseddel og mot ordreliste. Pakkseddel og ordreliste signeres av de som utfører kontrollen, for å sikre kontrollspor. Det bør være arbeidsdeling mellom den personen som sender bestilling og den som kontrollerer mottak av varer, for å sikre at ingenting blir holdt utenfor regnskapssystemet. Alle mottatte varer skal registreres i logistikksystemet. Dette gjøres mot pakkseddel, forutsatt at denne er kontrollert mot faktisk mottak av varer. Lines Kiosk er registrert med 6-10 ansatte. Det indikerer at det kan være vanskelig å alltid ha optimal arbeidsdeling. Dersom det er mulig bør tre forskjellige personer bestille, kontrollere mottak og registrere i systemet, men det krever videre at mange har tilgang til IT-systemene. Et alternativ er at man alltid er to når varene

kontrolleres, den ene har adgang til å bestille varer mens den andre kun har mulighet til å registrere mottak. Antagelig kan IT-systemet settes opp slik at den som bestiller ikke har anledning til å registrere mottak av samme ordre.

Varer på lager må sikres mot uautorisert uttak og mot forringelse i verdi/kvalitet. Først og fremst gjøres dette med fysisk sikring av lageret. Kiosken kan ha et eget lager, et bakrom eller alle varer i butikken. Uansett må området sikres mot for eksempel brann og tyveri. Et eksternt lager eller bakrom bør beskyttes med nøkler eller kode. Uoversiktlige områder i butikken kan for eksempel sikres med videokamera. Mye av risikoen knyttet til lager, varer og arbeidsdeling må i kiosk og parfymeribransjen anses som forretningsrisiko på grunn av varens natur, tilgjengelighet i butikken og tilgangen på kontanter. At varene sikres mot kvalitetsforringelse kan gjøres gjennom at man har tilpasset for eksempel temperatur og luftfuktighet dersom varene er sensitive for dette. I kiosk gjøres dette typisk ved å ha kjøleskap/områder med riktig temperatur. Selskapet bør jevnlig (i henhold til bokføringsforskriften § 6.1) ha vareopptelling for å avstemme varelageret mot det som er registrert i logistikksystemet samt avgjøre om kvaliteten på varene er som antatt. En slik gjennomgang vil gi en pekepinn på om bedriften kan stole på internkontrolltiltakene rundt logistikksystemet. En mengde varer som frukt, mat, drikkevarer, aviser, blader og til en viss grad bøker, er utsatt for kvalitetsforringelse ved lang tid på lager. Lagerstyringen bør derfor være optimalisert også for denne type varer. God kontroll med varenes kvalitet gjør også at bedriften kan sette ned prisene på varer som nærmer seg utløpsdato og dermed kanskje redusere tap noe. For ukurante varer bør det være en godkjenningprosedyre som involverer daglig leder, slik at varer ikke feilaktig klassifiseres som ukurante. Dette vil også hjelpe bedriften med å identifisere grunnen til ukurans og iverksette tiltak.

Dersom Lines Kiosk har et eksternt lager bør uttak herfra kontrolleres mot plukkseddel, ordreliste eller lignende (Moen og Havstein 2009). Igjen kan arbeidsdeling være utfordrende, da registreringen bør gjøres av en annen person enn den som er gjør det fysiske uttaket fra lageret.

For å kontrollere risikoen for feil klassifisering, periodisering og verdsettelse av varelageret må bedriften sørge for opplæring av personalet og at det eksisterer

retningslinjer og prosedyrer for de oppgavene som skal utføres. At daglig leder har fokus på at regler og retningslinjer blir overholdt vil være med på å skape et godt kontrollmiljø i bedriften. Det innebærer for eksempel at daglig leder ikke utfører oppgaver alene der de ansatte må være to.

d) Operasjonell risiko

Operasjonell risiko defineres av Basel Committee on Banking Supervision som: "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events (*Sound Practices for the Management of Operational Risk*). Selv om denne definisjonen er laget for finanssektoren er den overførbart til andre områder. At rutiner og retningslinjer ikke er hensiktsmessig utformet svekker effektiviteten i bedriften og kan føre til at mål ikke nås. For varelager kan man for eksempel peke på rutinen for bestilling av varer. Dersom bedriften har satt for lavt triggerpunkt for bestilling av varer risikerer bedriften å gå tom for varer og dermed miste salg. Dersom triggerpunktet er for høyt vil bedriften ha for høyt lagernivå og drive med for høy arbeidskapital. For høyt lagernivå kan både føre til høyere ukurans i varene, økt mulighet for tyveri og er direkte ineffektivt. Konsekvensene vil være de samme dersom rutinene er riktige, men de ansatte glemmer eller velger å ikke følge dem. Det kan også være at selv om man tror at de ansatte har tilstrekkelig kunnskap til å utføre oppgavene, er dette ikke tilfellet. Komplekse IT-systemer kan også være hinder for måloppnåelse fordi vanskelige systemer kan føre til unødige feil flere steder i rutinen rundt varelager. Det kan være feil i bestillingen, i registreringer av mottatte varer eller det kan være vanskelig å definere og ta ut relevante rapporter slik at ledelsen kan ta velinformerte beslutninger. I tillegg kan logistikksystemet ha flere grensesnitt noe som øker risikoen for at feil kan spre seg og det er vanskelig å oppdage "følgefeil". Dickstein (2009) snakker om at risiko generelt er knyttet til en forventning om avkastning, for eksempel markeds eller kredittrisiko. Imidlertid påpeker han at operasjonell risiko ikke har denne bindingen. Redusert operasjonell gir kun mulighet for et lavere tap. Potensielt tap kan imidlertid være stort og det er derfor ledelsen i bedriften også er opptatt av å styre operasjonell risiko. Dicksteins utsagn passer også godt med Basel komiteens definisjon av operasjonell risiko; man forventer ikke at

prosedyrene ikke er optimale eller at noen lar være å følge oppsatte rutiner. At dette blir korrigert vil heller ikke gi bedriften noen ekstra avkastning. Dickstein deler operasjonell risiko inn i ti kategorier. Første kategori er ”eksternt og internt mislighold”, for eksempel tyveri, at ansatte gjør uttak fra varelageret til privat bruk eller ikke registrerer mottatte varer i systemet. Videre er ”overholde lover og regelverk” en kategori. For et større selskap kan det være utfordringer knyttet til hvordan man klassifiserer varelageret i regnskapet i ulike land eller hvordan man estimerer sannsynligheten for tap. ”Feil i utførelsen av oppgaver” inneholder blant annet at varer registreres feil i systemet, at prislistene ikke er oppdatert eller at selskapet ikke mottar de varene de har bestilt. Feil i ”fysisk sikring” kan blant annet omfatte sikring av lagerlokaler slik at ansatte unngår skader, mens eksempel på ”feil i informasjonssikkerheten” kan være at uvedkomne får kjennskap til tilgangskoden til lageret. Videre er ”feil i IT-systemene” en komponent i operasjonell risiko. Det kan være at logistikksystemet ikke registrerer mottatte varer riktig og at det fører til et ikke-optimalt lagernivå. ”Upassende foretningsprinsipper” er en kategori som inneholder blant annet kundeservice eller at lagermedarbeidere unnlater å rapportere om feil de har oppdaget på varene kan inngå i denne kategorien. ”Juridisk risiko” inkluderes i operasjonell risiko og man kan her tenke seg alvorlige feil eller mangler på varer som kan føre til skader og påfølgende saksøking av bedriften. Siste kategori er ”disaster recovery” som handler at flere uforutsette hendelser slår til på samme tidspunkt. Det kan for eksempel være at bedriftens logistikksystem bryter sammen.

Oppgave 3: Personopplysninger i lønssystemet

- a) Gjør rede for lovbestemmelser som direkte vedrører registrering og oppbevaringer av personopplysning i lønssystemet

Det er først og fremst "Personopplysningsloven" og "Helseregisterloven" som regulerer personvernet i Norge. I tillegg er vi bundet av EU direktiv 95/46 EF og "Lov om Schengen informasjonssystem" med våre samarbeidsland.

Personopplysningsloven vil være den mest relevante i forhold til lønssystemet. Jeg vil derfor konsentrere meg om denne og bare kort kommentere enkelte bestemmelser i Helseregisterloven.

Både Personopplysningslovens (POL) og Helseregisterlovens (HRL) formål er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Se mer i lovens § 1. Videre er det sentralt at registrering krever samtykke fra den opplysningene gjelder eller at kravet er nedfelt i lov, POL § 8 og HRL § 5.3. POL § 8 definerer grunner til at man kan oppbevare og behandle personopplysninger. Det kan for eksempel være for å oppfylle en avtale, som å utbetale lønn, eller å oppfylle en forpliktelse, som årsoppgave (lønnsoppgave) til myndighetene. Grunnkravene til behandling av personopplysninger er i lovens § 11. Her fremgår det blant annet at behandlingsansvarlige kun skal behandle personopplysninger når dette er tillatt og til de formål som er saklig begrunnet i behandlingsansvarliges virksomhet. Hensikten arbeidsgiver har med å lagre opplysninger vil videre også reguleres av regelverk for den gjeldende oppgave. For eksempel vil utbetaling av lønn og pliktig rapportering til myndighetene medføre behov for lagring av personnummer, se bokføringsforskriften § 5-6. Registrering av fødselsnummer reguleres eksplisitt i personopplysningsloven § 12.

Når personopplysninger behandles skal konfidensialitet, integritet og tilgjengelighet sikres, jf. POL § 13. Her fremgår det også at dokumentasjon på informasjonssystemet og sikkerhetstiltakene skal være tilgjengelig.

Loven har videre krav om internkontroll (§ 14) og viser til at det skal etableres og vedlikeholdes systematiske tiltak for å sikre at kravene i loven er overholdt, herunder

sikre personopplysningenes kvalitet. Disse tiltakene skal dokumenteres.

Personopplysningsforskriftens § 3-1 har spesifikk informasjon over hvilke rutiner som skal utarbeides. Det stilles videre krav til at den som behandler dataene ikke kan endre behandlingen av dataene utover det som er skriftlig avtalt med den som er ansvarlig for dataene (§ 15). Dataene kan heller ikke overlates til andre.

Både POL og HRL har bestemmelser om innsyn. POL § 18 viser til den registrertes rett til å vite hva som er registrert, hvordan disse data behandles samt informasjon om den som behandler dataene. HRL § 22 har spesifikk informasjon om innsyn. Innsynet kan begrenses jf. POL § 23 og HRL § 25. Videre har lovene bestemmelser om informasjonsplikten databehandlingsansvarlige har, se HRL § 20, § 23-24, POL § 19-21.

Lagring av personopplysninger fremgår i POL § 28. Personopplysninger skal ikke lagres lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Videre lagring skal være i henhold til annen lovgivning (for eksempel arkivloven) eller de skal slettes. Man kan imidlertid lagre opplysninger for historiske og vitenskapelige formål dersom samfunnets interesse overstiger ulempene dette medfører for den enkelte. § 15 viser videre til at opplysninger ikke kan overlates til andre for lagring eller bearbeiding.

Dersom personopplysninger skal behandles med elektroniske hjelpemidler skal dette meldes Datatilsynet, jf. POL § 31. Meldeplikten omfatter også generell behandling av sensitive opplysninger, men dersom disse opplysningene ikke er gitt uoppfordret kreves det i tillegg konsesjon, jf. § 33. Unntak fra melde- og konsesjonsplikten fremgår av forskriften til personopplysningslovens kapittel 7. § 7.16 omfatter spesielt personellregistre.

Andre aktuelle lover vedrørende personopplysninger er Arbeidsmiljøloven (AML) og Folketrygdloven. Kapittel 5 i AML viser blant annet til arbeidsgivers registrerings- og meldeplikt for personskader og sykdom og Folketrygdloven pålegger blant annet arbeidsgiver å føre statistikk over sykefravær (§ 25-2).

b) Kolonner i tabeller for automatisk postering av lønnskostnader

Tabellen i oppgaven inneholder faste data om de ansatte. Faste data er opplysninger som påvirker eller er knyttet til mange transaksjoner (NOU 2002-20). Hver ansatt er identifisert med en unik kode, personnummer eller ansattnummer jf.

bokføringslovens krav om dokumentasjonshenvisning (§3 bokføringsforskriften) og kravet om sporbarhet (Moen og Havstein, 2009). Lønnssystemet har gjerne flere tabeller med faste data, og alle faste data skal entydig kunne identifiseres. Kodene benyttes for å fortelle IT-systemet hvordan data skal oppbevares og behandles. Når systemet er satt opp for å automatisere postering av lønnskostnader, krever dette en transaksjonstabell som på forespørsel henter data fra de faste tabellene og foretar beregninger i henhold til instruksjonene som gis.

Hvilke data som må lagres fremgår av lovkrav. I følge ligningsloven § 6-2 har arbeidsgiver plikt til å levere oppgave over de ytelser som er gitt til den ansatte. Dersom lønnskostnadene skal bokføres automatisk, må tabellene inneholde all den informasjon som er nødvendig for rapportering til myndighetene i henhold til loven. I tillegg til det som skal rapporteres i henhold til ligningsloven, sier bokføringsforskriften § 5-6 at lønnsoppgavepliktige ytelsene skal inneholde fødselsnummer, navn og stilling, skattekommune og tabellnummer og/eller trekkprosent. Ytelsene skal være spesifisert per konto for hver termin og ytelser som er arbeidsavgiftspliktige skal rapporteres samlet per avgiftssats og kommune. Skattebetalingsloven pålegger videre arbeidsgiver å foreta forskuddstrekk av skatt fra arbeidstaker. Dette setter rammer for hvordan systemet bygges opp.

For automatisk postering av lønnskostnader er derfor følgende kolonner nødvendig, i tillegg til de som er nevnt i oppgaven:

Fødselsnummer/ personnummer: dette følger av bokføringsforskriften § 5-6 og er nødvendig for entydig å identifisere hvilken person opplysningene relaterer seg til. I tillegg vil bedriften benytte ansattnummer for entydig identifisering internt i bedriften. Dette vil redusere bruken av personnummer.

Navn og stilling: skal også fremgå i henhold til forskriften § 5-6

Skattekommune: skal fremgå i henhold til bokføringsforskriften § 5-6.

Skattekommune kan avvike fra bostedskommune for eksempel på grunn av pendling eller flytting og det er derfor ikke tilstrekkelig å lagre informasjon om den ansattes postadresse. Postadresse vil være nødvendig for lønns- og trekkoppgaven, sammen med skattekommunenummer.

Av ligningsloven § 6-2 om lønnsoppgaven og forskrift om levering av lønnsoppgave er det i tillegg behov for:

Tabellnummer/trekkprosent/ekstra skattetrekk: disse opplysningene er nødvendige for å kunne automatisere beregningene av forskuddstrekk i henhold til skattebetalingsloven § 5-4.

Lønn (ligningsloven § 6-2): avhengig av bedriftens avlønningssystem må det finnes opplysninger om fast lønn, evt. overtid og kategorier for overtidsbetaling. Dersom bedriften har et timeregistreringssystem kan opplysninger om timer og oppfylging av dokumentasjonskravet om ansatte på timelønn registreres i dette.

Andre ytelser (ligningsloven § 6-2): pensjon, livrente, eventuelle fradrag, styregodtgjørelse, reise-, diett- og representasjonsgodtgjørelser og godtgjørelse for dekning av utgifter i forbindelse med arbeid eller verv, samt andre innberetningspliktige opplysninger som arbeidsgiver måtte tilby arbeidstaker. Disse krever separate kolonner i systemet siden de skal innberettes separat på egne koder.

Videre er det behov for tabell med feriepengesats og arbeidsgiveravgiftssats for å gjøre nødvendige beregninger og sykefraværsdøgn for å føre statistikk over sykefraværet (jf. Folketrygdloven § 25-2). Arbeidsgiver må også registrere bankkontonummer for å kunne foreta utbetalinger til den ansatte. Ansatt dato og sluttdato benyttes i logiske beregninger for at det ikke skal utbetales lønn for perioder den enkelte ikke var ansatt.

Automatisk bokføring av lønn risikoen for feil dersom systemet er konstruert riktig og det kan beskytte mot uautorisert tilgang og endringer. Det er imidlertid krevende å sette opp systemet og har andre utfordringer relatert til dokumentasjon og spesifisering i henhold til lovverket, jf. oppgave f.

c) Tilgangskontroller

At personopplyninger skal sikres fremgår blant annet av personopplysningsloven som drøftet tidligere. Inkludert i internkontrollen bør bedriften derfor ha spesifikke kontroller for lønssystemet. Det finnes to hovedkategorier av kontroller relatert til IT-systemer (Moen og Havstein, 2009), henholdsvis applikasjonskontroller og generelle kontroller. Tilgangskontroller vil typisk rette seg mot uautoriserte endringer i systemet, samt at uvedkomne har tilgang til fortrolige opplysninger. Dette faller gjerne i kategorien generelle IT-kontroller men omfatter også kontroller utenfor IT-miljøet.

Når det gjelder kontroller utenfor IT-miljøet er det nærliggende å starte med tilgangen til bygningen hvor selskapet holder til og området lønningsavdelingen befinner seg i. Selskapet vil ønske å vite hvem som er i lokalet og å kunne identifisere ansatte ved hjelp av id-kort. En vil registrere besøkende ved å gi dem egne besøkskort, samt ha regler for at de ikke skal gå rundt på egenhånd (Tipton og Krause, 2007). Videre kan bedriften velge å begrense tilgangen til lønningsavdelingen med tilgangskode. Dersom det ikke gjøres kan man ha avdelingen i et avgrenset område hvor det er lite gjennomgang. Avdelingen bør også ha en egen printer slik at sensitive utskrifter ikke kommer på avveie. Jevnlige avhending av uhentet utskrift vil også redusere denne risikoen.

På den IT-messige siden bør bedriften begrense antall pc'er som har tilgang til lønssystemet og begrense antall tilganger til disse pc'ene. Det kan gjøres ved å opprette en tabell som definerer brukertilganger i systemet. Tilgang krever da at systemet verifiserer hver bruker, gjerne ved bruk av både bruker-ID, smartkort eller lignende samt passord. Tilgangen til systemet bør knyttes til den jobbposisjonen man har og den informasjonen man har behov for, og skal ikke automatisk følge med dersom man endrer stilling (Tipton og Krause, 2007). De generelle kontrollene i IT-miljøet bør begrense tilgangen til internett og nedlastning for å redusere risikoen for virus og spyware. I tillegg bør bedriften ha tilfredsstillende brannmurer, antivirusprogram og annen generell IT-sikring. Begrenset tilgang til internett kan også hindre at den ansatte sprer informasjon. Tilgang til å jobbe "remote" bør også

begrenses ettersom bedriften da har mindre kontroll på hvem om har tilgang til opplysningene.

Tilgangen til selve lønningssystemet bør også reguleres i tid slik at dersom programmet er uvirksomt over lengre tid så blir brukeren automatisk logget ut.

Bedriften bør regulere tilgangen til å avhende maskiner, slik at ikke opplysninger kommer på avveie i denne fasen.

At tilgangskontrollene fungerer som forutsatt kan kontrolleres gjennom å iverksette oppdagende kontroller som gjennomgang av nye tilganger, logger for endring av faste data etc.

d) Konfidensialitet og kryptering

For å sikre konfidensialitet for lagring av personopplysninger kan man benytte asymmetrisk kryptering. Ved asymmetrisk kryptering er det ikke den samme nøkkelen som blir brukt ved kryptering og dekryptering (slik som i symmetrisk kryptering). I asymmetrisk kryptering er det en offentlig nøkkel og en privat nøkkel for hver av deltakerne. En deltakers offentlige nøkkel kan distribueres til alle som vil/skal sende krypterte meldinger til deltakeren. Den enkelte privates nøkkel holdes hemmelig og gjør at bare den enkelte har tilgang til informasjonen som sendes. Et eksempel på en personlig nøkkel er en PIN- kode. Når data krypteres med mottakers offentlig nøkkel og dekrypteres med en mottakers private nøkkel sikres konfidensialiteten i dataene. Det er kun mottaker som kan "åpne" meldingen. I tillegg til settet med nøkler trengs det et sertifikat hvor undertegners identitet blir knyttet til den offentlige nøkkelen. Sertifikatet garanterer koblingen mellom den private nøkkelen og undertegner. Ettersom den offentlige nøkkelen skal /kan distribueres kreves det en infrastruktur for dette, denne kalles Public Key Infrastructure (PKI). PKI er en samling med datasystemer, distribusjonssystemet og rutiner som eksisterer for å håndtere offentlige nøkkelsertifikater (jf. Ot.prp. nr.82 (1999-2000 Om lov om elektronisk signatur).

E-signaturloven har i dag krav om at et sertifikat skal være godkjent (§ 4), men det er ingen etablert standard til sertifikatene. Mange bedrifter og etater er i startfasen med bruk av sertifikater og det gjør at bedriftene står friere ved valg av teknologi og leverandører. På et tidlig tidspunkt kan man si at det ville vært hensiktsmessig med en standard slik at bedriften ikke investerer i noe som ikke blir godkjent. På den andre siden er det ikke alltid hensiktsmessig å velge standarder tidlig da man kanskje ikke har oversikt over alle konsekvenser.

Dersom en standard pålegges av myndighetene vil kostnadene for næringen avhenge av hvor raskt lovforslaget gjøres gyldig. På grunn av mengden deltakere i en slik infrastruktur vil det være tidkrevende å komme frem til en løsning og innfasingen vil ta tid. Dersom deltakerne er klar over hva som er under planleggingen vil de kunne koordinere for eksempel utskiftingen av IT-utstyr.

e) Elektronisk signatur

I tillegg til krypteringen som nevnt i oppgave 3 d, så kan tabellens integritet sikres ved hjelp av elektronisk signatur. Bruk av elektronisk signatur er regulert i lov om elektronisk signatur. Jeg benytter her det loven definerer som ” kvalifisert elektronisk signatur”, altså en avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt av et godkjent signaturfremstillingssystem, jf § 3.3. Med integritet menes at tabellen ikke har vært gjenstand for uautoriserte endringer.

Til bruk for å verifisere tabellens integritet kan man benytte ”sjekksum”, som for eksempel MD5 (Message Digest Algorithm 5). Man vil da ta en MD5-sum av tabellen (jf. forelesningsnotater) og deretter kryptere denne summen ved hjelp av mottakers offentlige nøkkel for å sikre konfidensialitet. Denne krypterte summen kalles digital signatur. Mottaker / neste bruker av tabellen gjentar MD5 beregningen og sammenligner den med den dekrypterte signaturen. Dersom disse er identiske viser det at det ikke er skjedd endringer i tabellen.

f) Tabellen går tapt

Oppgaveteksten i oppgave 3 viser til en tabell med faste data om arbeidstakere. Disse dataene benyttes til å automatisere lønnsberegninger sammen med data fra andre faste tabeller. Bokføringen av lønnskostnaden foregår altså ved hjelp av systemgenererte poster.

I bokføringsloven er det krav til dokumentasjon av bokførte opplysninger etter hver periode med pliktig regnskapsrapportering (§ 5). Videre er det også krav til spesifisering av lønnsoppgavepliktige ytelser.

Det fremgår av bokføringsloven § 4 at regnskapsmaterialet skal sikres mot urettmessig endring, sletting eller tap. Tabellen med lønnsdata må anses som regnskapsmateriale fordi den inneholder opplysninger som er nødvendige for å overholde plikten om lønnsoppgave (bokføringsforskriften § 3.1-9). Videre sier § 13 at oppbevaringspliktig regnskapsmateriale skal sikres mot ødeleggelse, tap og endring. Regnskapsmaterialet skal være tilgjengelig i lesbar form og skal kunne skrives ut på papir i hele oppbevaringsperioden. På utstedelsestidspunktet må dokumentasjonen "låses". Det er verken i forskrift eller lov definert hvordan dokumentasjonen skal låses. I uttalelse om God Regnskapsskikk nr 4 (og Ot.prp. nr. 46 (2003-2004)) fremgår kravet om fysisk produksjon av rapporter med spesifikasjoner (bygger på NOU 2002-20). Dette er ut fra tanken om at fysisk produserte rapporter ikke er redigerbare. Hensikten er å forhindre at data endres i ettertid både bevisst og ved feil. Disse henvisningene tolkes altså slik at data skal skrives ut, enten på papir eller som rapportfiler for elektronisk lagring. Tidligere ble papirutskrifter ansett som ikke redigerbart og dermed som en sikker oppbevaringsmetode, men med utviklingen i teknologi har stadig flere tilgang til å manipulere papirutskrifter. Det er med andre ord ingen krav om kryptering, e-signatur eller annet for oppbevaring og autentisering av regnskapsdata. Selskapene må selv komme frem til en praksis som de mener overholder myndighetenes krav og som godkjennes av revisor.

Kravet om sporbarhet er spesielt utfordrende når det gjelder systemgenererte poster, altså poster hvor det ikke finnes tradisjonelle bilag (NOU 2002-20). For at systemgenererte poster skal bli riktige må det for det første være tilstrekkelig data lagret i systemet og de korrekte "handlingsreglene" for systemet må være definert.

Bokføringsforskriftens kapittel 7.2 har krav om sikkerhetskopi av elektronisk materiale. Man kan anta to former for sikkerhetskopiering, den ene er den kontinuerlige "back up" av regnskapssystemet som gjør at man kan gjenskape rapporter dersom hovedsystemet bryter sammen. Den andre er en sikkerhetskopi av produserte pliktige rapporter slik at disse ikke går tapt.

g) Har bedriften behov for sikring utover lovkravet?

Ettersom loven ikke har krav om hvordan tabellene skal sikres, kan bedriften i utgangspunktet lagre dette som papirutskrifter eller pdf-filer. Det er styret og daglig leder som er ansvarlig for at tabellen sikres hensiktsmessig.

Prinsippet for sikkerhetskopiering og sikring vil være det samme for alle bedrifter. Avhengig av bedriftens størrelse og kompleksitet vil imidlertid behovene være forskjellige. Store og komplekse bedrifter vil ha behov for daglig sikkerhetskopiering av regnskapssystemet. Dette fordi det kan være vanskelig å gjenskape transaksjonene i systemet. Komplekse systemer med mange grensesnitt kan også ha større sannsynlighet for problemer ettersom ulike deler av systemet oppgraderes og forbedres på ulike tidspunkt. I slike faser vil det være spesielt nødvendig med gode rutiner for sikkerhetskopiering og dokumentasjon. Mindre selskap med færre og mer oversiktlig transaksjonsmengde kan kanskje klare seg med sikkerhetskopiering hver måned eller hver gang det produseres pliktige rapporter.

Formen for sikkerhetskopiering vil også være avhengig av karakteristika ved bedriften. Store bedrifter kan ha parallelle systemer og eksterne servere hvor data lagres, mens mindre bedrifter kan lagre data for eksempel på eksterne harddisker. Disse må imidlertid sikres mot uautorisert tilgang og manipulering.

Muligheten til å sikre data ved hjelp av kryptering og e-signaturer i systemet kan være kostbart for bedriften, men det kan også spare kostnader på sikt. Fo eksempel

kan kostnadene til revisjon reduseres ved at det blir mindre gjennomgang av fysiske bilag. Bedriften vil antagelig også bli mer effektiv fordi man unngår å bruke tid på utskrifter og administrasjon og oppfølging av fysisk arkiv. Store organisasjoner kan ha nytte av kryptering og e-signaturer for eksempel når de har deler av sin virksomhet i utlandet eller på flere steder innenlands. Ledelsen har i slike situasjoner mindre oversikt over kontrollmiljøet og kan gjennom kryptering og e-signaturer kontrollere systemene.

Oppgave 4: Justering av merverdiavgift

Eiendomsselskapet har mange utleieobjekter og mange leietakere, og det kan være flere prosjekter som kommer inn under justeringsreglene på hvert utleieobjekt. Dette gjør oppfølgingen til en kompleks oppgave som må defineres nøye. Risikoen for feil er stor og bedriften bør søke å automatisere beregningene i regnskapssystemet. Oppgaven ber om hvilke kolonner som trengs i regnskapssystemet for at dette skal kunne gjennomføres. Oppgaven ser bort i fra påkostninger og jeg tolker dette som kostnader relatert til på eller ombygging. Jeg vil altså kun se på byggekostnaden for utleieobjektet og eventuell justering av merverdiavgift i den påfølgende tiårsperioden. Jeg antar videre at det kun er en leietaker for hvert utleieobjekt, men at denne ikke nødvendigvis har hele sin virksomhet som avgiftspliktig virksomhet.

Oppgaven definerer tabellen RESK som er reskontro for utleieobjektene og inneholder avgiftsrelaterte data om leietaker. Dette vil være hvorvidt leietaker er avgiftspliktig og eventuelt hvor stor del av virksomheten som er avgiftspliktig. I tillegg bør tabellen ha opplysninger om opprinnelige byggekostnader og fradragprosenten og total merverdiavgift (100 %) på ferdigsstillestidspunktet. Videre må den inneholde årstall for ferdigstillelse. Se eksempel i vedlegg 4.

Videre ville jeg hatt flere tabeller for faste data i systemet, slik at jeg kan benytte disse når jeg skal registrere endringer i transaksjonstabellen. Det vil være en tabell med oversikt over mulige endringer som kan få konsekvenser for justeringplikten, en tabell som knytter dato for endring til merverdiavgiftstermin og en tabell som viser hvorvidt justeringen skal være samlet eller årlig, se vedlegg 4.

Når det skjer en endring for eksempel at leietaker reduserer andelen av virksomheten som benyttes i avgiftspliktig virksomhet vil dette registreres i regnskapssystemet. Registreringen vil fremgå i transaksjonstabellen poster. Poster inneholder dato for endring, type endring som velges fra gitte alternativer i systemet. Avhengig av type endring må det oppgis ytterligere informasjon (se oppgave 1 e rutinebeskrivelse). I dette eksempelet vil det være behov for ny avgiftssats for leietaker.

Systemet vil beregne ny fradragsberettiget merverdiavgift for utleieobjektet, slik den ville ha vært på ferdigstillestidspunkt med ny fradragsprosent. Systemet deler videre denne summen på ti ettersom det tilsvarer årlig justering.

Et annet alternativ er at bedriften slutter å leie ut et utleieobjekt. Dette registreres i systemet som opphør og alle forutsetningene for fradrag forsvinner. Registreringen gjøres fortsatt slik at den fremgår i tabellen poster. I tillegg til dato for endring velges opphør som type endring og systemet fyller selv ut opplysninger om ikke lenger avgiftsplikt og 0 som ny avgiftspliktig virksomhet.

Systemet vil beregne ny fradragsberettiget merverdiavgift for utleieobjektet som i dette tilfellet er lik null. I tillegg vil systemet justere for antall år til justeringsplikten bortfaller ettersom avgiften i dette tilfellet skal betales samlet.

Ettersom dette var alle endringene i perioden, bokføres disse. Jeg antar at systemet i den prosessen også kan hente opp opprinnelig fradragsført merverdiavgift og beregne differansen av disse (ny avgift – opprinnelig avgift). Positivt resultat indikerer at selskapet har merverdiavgift til gode, mens negativ betyr at selskapet skylder merverdiavgift. Ved periodeavslutning vil systemet (på forespørsel) lage en systemgenerert post som legger sammen den avgiften vi skylder for utleieobjekt 1 og den vi skylder for utleieobjekt 2.

Ettersom endringen skjer i januar for endret bruk i avgiftspliktig virksomhet beregnes den årlige justeringen for hele året. Beregningen måtte ellers vektas i henhold til antall måneder. Justeringen som gjøres samlet skjer i februar, men her er regelen at justeringen skal inkludere hele det året endringen skjer.

Kildehenvisninger

Bank for International Settlements, 2003, *Sound Practices for the Management of*

Operational Risk, www.bis.org

Dickstein, Dennis I., and Robert H. Flast, 2009, *No Excuses: A Business Process Approach to*

Managing Operational Risk, John Wiley & Sons (e-book: Books 24/7)

Innst. O. Nr 94 (2006-2007), Innstilling til Odeltingen fra finanskomiteen

Kristoffersen, Trond, 2005, *Årsregnskapet- en grunnleggende innføring 2. Utgave*,

Fagbokforlaget

Moen, Tove-Gunn og Bjørgunn Havstein, 2009, *Regnskapsorganisasjon, bokføring og intern*

kontroll, 5. Utgave, Cappelen Akademiske forlag

Norges Interne revisorers forening, COSO, september 2004-oktober 2005, *Helhetlig*

risikostyring – et integrert rammeverk Sammendrag,

NOU 2002: 20 Ny bokføringslov

Ot.prp.nr.59 (2006-2007), Om lov om endringer i lov 19. Juni 1969 nr 66 om merverdiavgift

Ot.prp.nr.46 (2003-2004), Om lov om bokføring

Ot.prp.nr.82 (1999-2000), Om lov om elektronisk signatur

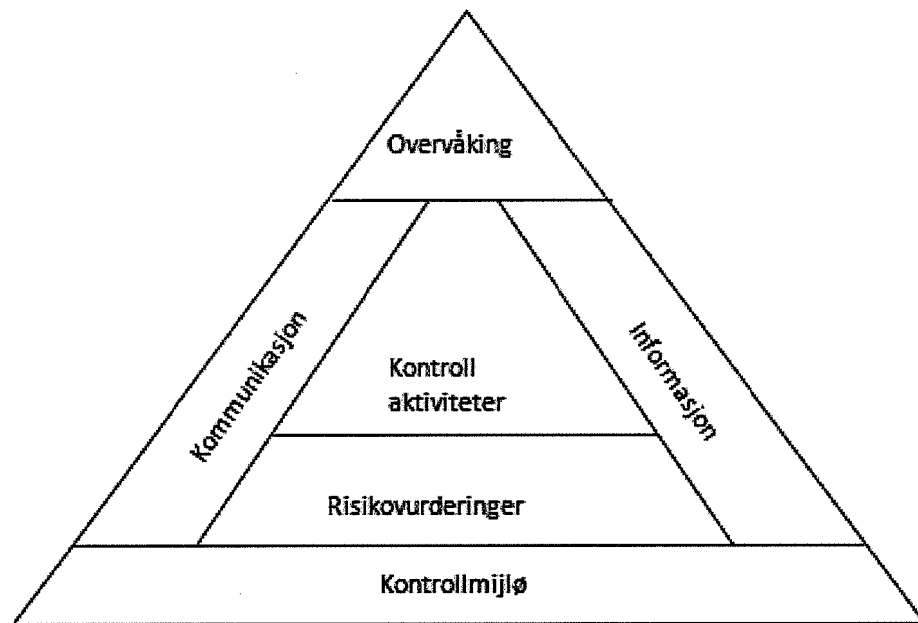
Tipton, Harold F., og Micki Krause, 2007, *Information Security Management Handbook*,

6. utgave, Auerback Publications (e-book: Books 24/7)

www.lovdata.no

www.coso.org

Appendix 1: Coso modellen



Appendix 2: Regnskap for Line Kiosk & Parfumeri AS

Org nr 970 987 894

(kilde: www.proff.no)

Regnskapstall				
RESULTATREGNSKAP	2008	2007	2006	2005
Valutakode	NOK	NOK	NOK	NOK
Sum salgsinntekter	2 971 000	2 941 000	2 985 000	3 074 000
Andre driftsinntekter	478 000	517 000	569 000	624 000
Sum driftsinntekter	3 449 000	3 458 000	3 554 000	3 699 000
Vareforbruk	2 178 000	2 256 000	2 278 000	2 372 000
Beholdningsendring	0	0	0	0
Lønnskostnader	1 026 000	851 000	928 000	951 000
Ordinære avskrivninger	4 000	4 000	4 000	4 000
Nedskrivning	–	–	–	–
Andre driftskostnader	370 000	335 000	307 000	340 000
Driftsresultat	-129 000	12 000	36 000	32 000
Sum finansinntekter	2 000	2 000	2 000	1 000
Nedskrivning fin. anleggsmidler	–	–	–	–
Sum finanskostnader	21 000	16 000	16 000	19 000
Resultat før skatt	-148 000	-1 000	22 000	15 000
Sum skatt	-5 000	-2 000	7 000	7 000
Ordinært resultat	-143 000	1 000	15 000	8 000
Ekstraordinære inntekter	–	–	–	–
Ekstraordinære kostnader	–	–	–	–
Skatt ekstraordinært	0	0	0	0
Årsresultat	-143 000	1 000	15 000	8 000
Utbytte	–	–	–	–
Konsernbidrag	–	–	–	–

BALANSEREGNSKAP	2008	2007	2006	2005
Valutakode	NOK	NOK	NOK	NOK
Goodwill	–	–	–	–
Sum immaterielle midler	0	2 000	0	0
Tomter, bygninger og annen fast eiendom	21 000	25 000	29 000	33 000
Maskiner/anlegg/biler	–	–	–	–
Driftsløsøre/ inventar/ verktøy	0	0	0	0
Sum varige driftsmidler	21 000	25 000	29 000	33 000
Sum finansielle anleggsmidler	21 000	21 000	21 000	21 000
Sum anleggsmidler	41 000	48 000	49 000	53 000
Sum varelager	608 000	538 000	564 000	533 000
Kundefordringer	6 000	9 000	7 000	8 000
Sum fordringer	37 000	23 000	22 000	38 000
Sum investeringer	0	0	0	0
Kasse/Bank/Post	96 000	84 000	99 000	121 000
Sum omløpsmidler	740 000	644 000	686 000	692 000
Sum eiendeler	782 000	692 000	735 000	746 000
Aksje/selskapskapital	100 000	100 000	100 000	100 000
Sum innskutt egenkapital	100 000	100 000	100 000	100 000
Sum opptjent egenkapital	-114 000	28 000	27 000	13 000
Sum egenkapital	-14 000	128 000	127 000	113 000
Sum avsetninger til forpliktelses	0	0	0	0
Pant/gjeld til kredittinstitusjoner	–	–	–	–
Langsiktig konserngjeld	–	–	–	–
Ansvarlig lån	–	–	–	–
Sum langsiktig gjeld	0	0	0	0
Leverandør gjeld	316 000	225 000	241 000	114 000

Skyldig offentlige avgifter	25 000	20 000	24 000	22 000
Utbytte	–	–	–	–
Kortsiktig konserngjeld	–	–	–	–
Sum kortsiktig gjeld	796 000	564 000	608 000	633 000
Sum gjeld	796 000	564 000	608 000	633 000
SUM EGENKAPITAL OG GJELD	782 000	692 000	735 000	746 000
REGNSKAPSANALYSE	2008	2007	2006	2005

Fagområder/bransjer

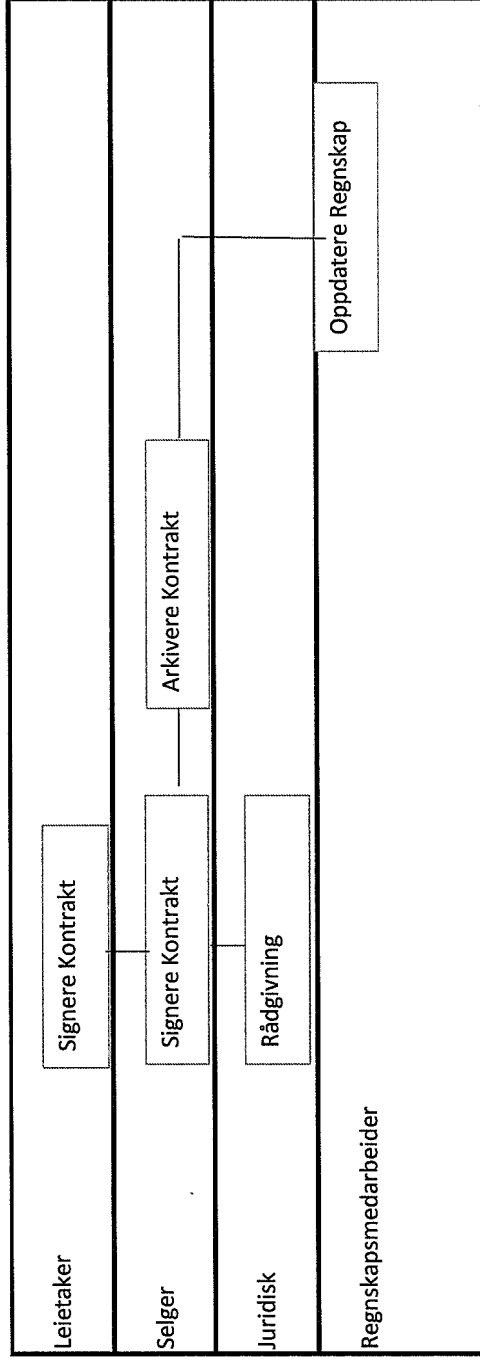
Bransje:

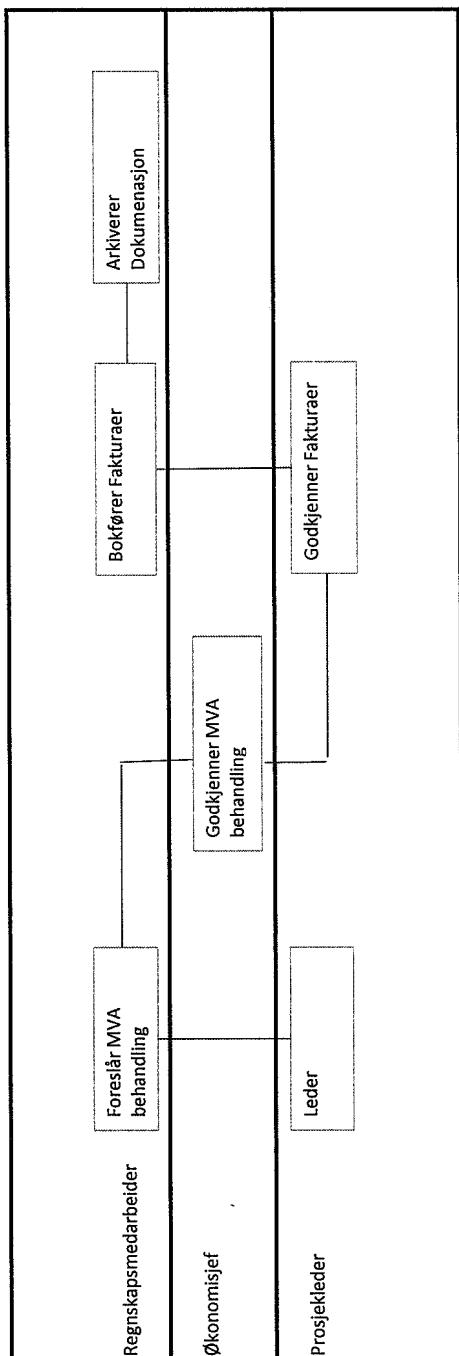
Kosmetikk, parfyme og friserartikler

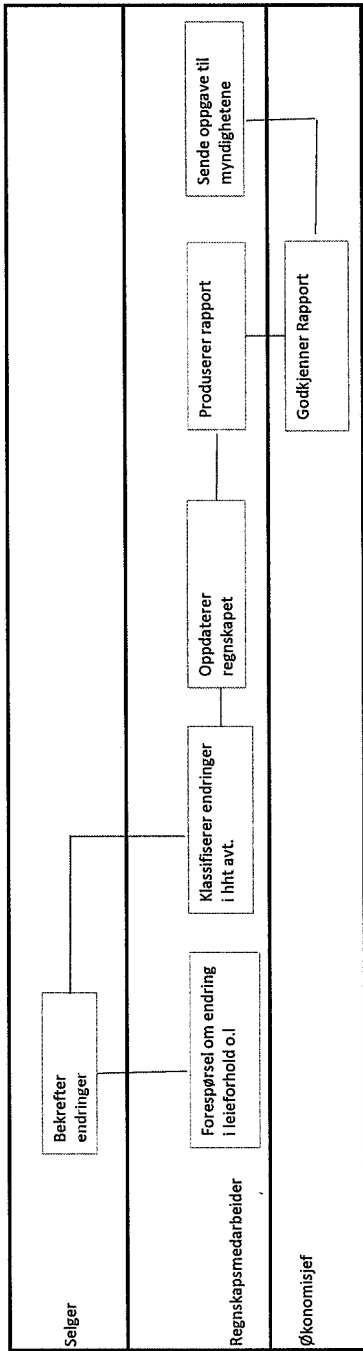
NACE-bransje:

47.112 Kioskhandel med bredt vareutvalg med hovedvekt på nærings- og nytelsesmidler

Vedlegg 3: Rutinen for justering av merverdiavgift







Vedlegg 4: Tabeller vedrørende justering av merverdiavgift og utleieobjekter

Tabell Resk:

Resk kode	Resk nr	Eiendommens gnr/bnr	Leietaker	avgifts- pliktig ?	% i næringspliktig virksomhet	anskaffelses år	anskaffelseskost	total mva	fradrag% på fullføringstids punkt
1150	1		Leietaker Olsen AS	ja	100	2000	2 000 000	500 000	100
1150	2		Fredriksen AS	ja	100	2003	3 000 000	750 000	100
1150	3		Nål og Søm AS Fam. Jensen	ja	100	1980	4 000 000	1 000 000	100
1150	4			nei	0	2005	2 000 000	500 000	0

Andre tabeller for faste data:

Mnd	Mnd kode	MVA termin
Jan	1	1
Feb	2	1
Mar	3	2
Apr	4	2
Mai	5	3
Jun	6	3
Jul	7	4
Aug	8	4
Sep	9	5
Okt	10	5
Nov	11	6
Des	12	6

Endringskode	Endring
1	Endring andel brukt i avgiftspliktig virksomhet
2	Ny leietaker
3	overdragelse, justeringsplikt overføres
4	opphør
5	overdragelse, justeringsplikt overføres ikke

Avgiftsplikt kode	Avgiftsplikt
1	ja
0	nei

Overdragelsekode	Overdragelse
1	ja
0	nei

Tabell for Poster

Tabellen POSTER													
dato for endring	konto	mnd	år	Resk nr	Endrings- kode	Avgiftsplikt	Ny andel i avgiftspliktig virksomhet (1%)	Ved overdragelse (justerningsplikt overføres)	esign	evt. Kommentar			
10.01.2010	1150	1	2010	4	1	ja	80						
02.02.2010	1150	2	2010	2	4	nei	0						

mnd	mva termin	resk	ny mva årlig	ny mva samlet	Gammel Mva årlig	Differanse
1	1	1	$= (80/100 * 500000) / 10$	NA	500000/10	10000
2	1	2	NA	$= (0/100 * 750000) / 10 * (2010 - 2003)$	$= 300000 * 0,25$	-225000
					Sum	-215000

Summen på 215 000 er negativ og det indikerer at forpliktelsen er høyere enn det som ble beregnet på fradragstidspunktet. Selskapet må derfor betale tilsvarende til myndighetene på oppgaven for januar og februar.