IT-revisjon – effektiv revisjon med merverdi

Kontroll av input og output uten å ha god kjennskap til systemene kan føre til manglende kvalitet på og manglende effektivitet i gjennomføringen av revisjonen. IT-revisjon, som vurderer hvordan IT-systemene støtter opp under regnskapsavleggelsen, **er, etter artikkelforfatterens mening, hensiktsmessig for de fleste revisjonsoppdrag.**

Artikkelen er forfattet av:

CISA
Torkil Hindberg
Manager, Advisory KPMG

IT-systemer har historisk ofte blitt behandlet som en «black box» av revisor. Sannsynligvis skyldes dette manglende kunnskap om IT-systemer. Å kontrollere input og output uten å ha noen nærmere kjennskap til eller kontroll av systemene vil imidlertid kunne medføre både manglende kvalitet på, og manglende effektivitet i gjennomføringen av revisjonen.

I finansiell revisjon skal revisor bekrefte at selskapets regnskapspåstander ikke er vesentlig feil gjennom å oppnå revisjonsmålsettingene. IT-revisjon som en del av finansiell revisjon, er betegnelsen på metoder og revisjonshandlinger hvor man vurderer hvordan IT-systemene støtter opp under regnskapsavleggelsen. IT-revisjon vil være hensiktsmessig og effektivt i de fleste revisjonsoppdrag, men dette må ikke forstås som at IT-revisjonen bestandig må gjennomføres av en IT-revisor. Det er fullt mulig, og sannsynligvis mest effektivt, at de enkleste IT-revisjonshandlingene utføres av en «vanlig» revisor, alene eller under veiledning av en IT-revisor. Dette betyr at IT-revisjon gjennomføres istedenfor andre revisjonshandlinger og ikke i tillegg til eksisterende revisjonshandlinger, noe som gir et stort effektivitetspotensial.

IT-revisjon involverer tre parter; kunden, revisjonsteamet og IT-revisoren. Det er svært viktig at både kunden og revisjonsteamet opplever merverdi med IT-revisorens arbeid. Revisjonsteamet trenger sikkerhet for at regnskapspåstandene er riktige (revisjonsmålsettingene oppnådd), mens kunden både må ha sikkerhet for at behandlingen av data skjer på riktig måte, og også behov for forbedringsinnspill i forhold til hvordan systemene kan benyttes mer effektivt og/eller i forhold til smartere og bedre kontroller i transaksjonsflyten. Fokuset i IT-revisjonshandlingene må altså være på bekreftelse av revisjonsmålsettinger og ikke operasjonelle IT-forhold som har liten eller ingen innvirkning på regnskapet.

IT-revisorer og revisorer har sammenfallende interesser. Det vil si å gjøre kundene fornøyde. På denne måten er det større sjanse for å beholde de kundene de ønsker å beholde, samtidig som de viser at de er moderne og fremtidsrettede revisorer for potensielle nye kunder.

Når og hvordan skal man involvere en IT-revisor?

IT-revisor er en spesialist som tas med i revisjonen hvis det foreligger spesifikk risiko knyttet til hvordan IT-systemene anvendes for å avlegge et riktig regnskap. IT-revisoren er spesialist på å forstå og håndtere risikoen som et IT-systems funksjonalitet og anvendelse har på kvaliteten i regnskapsavleggelsen. Involveringen av IT-revisoren kan være forskjellig – dette kommer an på kompleksiteten i problemstillingene. Risikovurdering i forhold til hvordan IT-systemene støtter virksomheten og regnskapsavleggelsen sier noe om risikoen for feil i regnskapet. I mange tilfeller kan det være nyttig at IT-revisoren bare er med i planleggingen for å avklare hvilken risiko IT-systemene innebærer og hvordan dette kan håndteres. Revisjonshandlingene kan, basert på dette, gjennomføres av «vanlige» revisorer hvis kompleksiteten i handlingene ikke er høy.

Ved å involvere IT-revisoren allerede i planleggingen vil man håndtere IT-risikoen i en tidlig fase slik at man sikrer en effektiv revisjonstilnærming. En IT-revisors involvering i planleggingen kan være fra bare en halv times diskusjon med revisjonsteamet til aktiv deltakelse i kartlegging av hvordan IT-systemene påvirker regnskapet, hvilke IT-relaterte kontroller på selskapsnivå som finnes og hvordan kvaliteten på disse påvirker risikoen for feil i regnskapet og til slutt revisjonstilnærmingen – dvs. hvilke konkrete revisjonshandlinger som skal utføres.

Test av kontroller er den mest effektive formen for revisjon. Den mest effektive formen for kontrolltesting er gjennom test av automatiske kontroller i IT-systemene. Årsaken til dette er at automatiske kontroller fungerer på samme logiske måte hver gang, så fremt funksjonaliteten i IT-systemet ikke er endret. På denne måten kan man teste integriteten i hele populasjonen eksempelvis for en transaksjonsstrøm ved bare å teste et sample. Mange av disse kontrollene er standardkontroller i IT-systemene. Et eksempel på en standardkontroll er at det ligger inne en sperre som sikrer at man ikke kan fakturere en vare før den er levert. Denne typen kontroller kan fint testes av en ordinær revisor, alene eller med støtte fra en IT-revisor. Ved tilpassede kontroller og mer komplekse transaksjonsstrømmer vil det være behov for å involvere en IT-revisor i testingen.

Detaljtester og analyse som substanskontroll kan være utfordrende å gjennomføre på grunn av store datamengder. Ved å anvende dataanalyse for å gjennomføre substanshandlingene har man mulighet til

en mer effektiv revisjonshandling med bedre sikkerhet. I KPMG benytter vi dataanalyseverktøyet IDEA. Dette kan benyttes av en «vanlig» revisor for de enkleste handlingene og med støtte fra IT-revisjon hvis problemstillingene er mer komplekse. Fordelen med dataanalyse i IDEA er at man kan importere hele populasjonen man ønsker å utføre revisjonshandlingen på til IDEA og gjennomføre de revisjonshandlingene man ønsker på alle relevante data.

Kommunikasjonen med kundene om hvordan vi mener IT-systemene støtter regnskapsavleggelsen, kan være utfordrende, da problemstillingene ofte ligger i et grenseland mellom økonomi og IT. Det kan derfor være nyttig å benytte en IT-revisor for å utarbeide de IT-relaterte forholdene som revisor ønsker å ta opp i brev til ledelsen. Et oppsummeringsbrev eller en presentasjon av den gjennomførte IT-revisjonen, der man tar opp og kommer med forslag til forbedringer på mindre kritiske forhold og kanskje operasjonelle problemstillinger, gir kunden en merverdi.

IT-revisor bør være med i hele revisjonsprosessen, fra planlegging via test av kontroller og substanstester til avslutning i de tilfeller der risikoen for feil i regnskapet som følge av IT-systemenes funksjonalitet og anvendelse er høy. Involveringen vil variere i omfang og må bestemmes ut fra hva som gir mest sikkerhet og kvalitet i revisjonen.

IT-revisjon i transaksjonsstrømmer

Hvor ofte er det avvik mellom reskontro og hovedbok? I et integrert regnskapssystem er dette umulig hvis systemet er satt opp riktig. Hvorfor er da dette en av de vanligste kontrollene en revisor gjennomfører?

Håndtering av penger og dermed risiko for misligheter utgjør alltid en vesentlig risiko i revisjonssammenheng. Det er derfor svært vanlig å kontrollere at to personer må godkjenne betalinger i nettbanken. Etter min mening gir ikke dette vesentlig sikkerhet for at det ikke foregår misligheter knyttet til utbetalinger. For det første blir stort sett alle betalingsforslag utarbeidet i IT-systemene for så å bli lastet inn i nettbanken. Det er sjelden noen som sjekker at alle disse betalingene er knyttet til reelle fakturaer som vedrører selskapet. Videre er det slik at av (??) alle betalinger som ikke kommer via økonomisystemet, er få ikke-rutine-transaksjoner som uansett følges opp nøye av selskapet, da de ser stor risiko knyttet til dette. For å sikre seg mot misligheter knyttet til penger må man heller sørge for at masterdata på leverandørene er betryggende sikret mot uautoriserte endringer, da det er dette som er grunnlaget for betalingsforslaget fra økonomisystemet. Er det opprettet en falsk leverandør med kontonummeret til en ansatt, hjelper det lite med to personer for å bekrefte betalinger i nettbanken.

Det forekommer svært sjelden at det er vesentlige feil i standard transaksjonsstrømmer. Hvorfor? Fordi det er snakk om logikk som gjentas for hver transaksjon. Med flere tusen, kanskje millioner av transaksjoner, vil en vesentlig feil mest sannsynlig avdekkes gjennom selskapets overvåkningskontroller. Betyr dette at det ikke er nødvendig å revidere transaksjonsstrømmer – nei! Revisjon handler ikke om å finne feil, men om å bekrefte at regnskapet er riktig (ikke innholder vesentlige feil). For å kunne gjøre dette bør revisor stille seg selv spørsmålet «hva kan gå galt?». Ved å bekrefte rutine-transaksjonene gjennom IT-systemene gir dette mer tid til å fokusere på vurderingsposter og vanskelige regnskapsmessige problemstillinger. Dette gir en bedre og mer risikostyrt revisjon samt at det er positivt for økonomien i revisjonsprosjektene.

De vanligste og mest vesentlige transaksjonsstrømmene i et selskap er oppbygd på samme logiske måte – uavhengig av selskap. Vi skal se på ett eksempel; Ordre-til-fakturering.

I stort sett alle ordre-til-fakturering finnes følgende aktiviteter:

- Oppsett av masterdata kunder
- Oppsett av masterdata produkter
- Ordreopprettelse
- Plukking av vare
- Utsendelse av vare
- Fakturering

Ved opprettelse av en ordre kobler man kundedata med produktdata og genererer ordrelinjer. Kundedata kan bestemme leveringsadresse som igjen styrer mva-behandlingen for ordren. Videre kan alle regler for rabatter og bonusavregninger bestemmes av kundedata. Produktdata bestemmer utsalgspris og kostpris for varen. Det er derfor viktig at det er fokus på hvem som har tilgang til å endre masterdata for kunder og produkter og hvilke rutiner som er etablert for å sikre at endringene blir riktige.

Konteringsregler relevante for ordre-til-fakturering ligger ofte knyttet til ordretypen. Det vil derfor normalt være nødvendig å kartlegge hvilke ordretyper som finnes og hva disse benyttes til. Antall ordretyper vil bestemme hvor mange transaksjonsstrømmer som må revideres. Dette vil være en sentral del av den forretningsforståelse revisor må ha for å utføre de riktige revisjonshandlingene.

Etter at ordren er opprettet, produseres det en plukkliste som benyttes til plukking av varer på varelageret. Verken etablering av ordren eller produksjon av plukklisten gir regnskapsmessig konsekvens. Plukklisten kan reservere varer på lageret, men vil ikke påvirke lagerverdien, da varene fortsatt ligger på varelageret. Det er derfor ikke nødvendig å ha fokus på plukklisten i revisjonen.

Når varene er plukket og klare til å sendes, utarbeides det en pakkseddel. Ved opprettelse av pakkseddelen blir varene meldt ut av lageret i systemet. Det er derfor viktig å kontrollere at konteringen knyttet til vareuttaket er riktig, dvs. at varekosten blir riktig bokført.

Når varen er sendt og pakkseddel er utarbeidet, kan man fakturere. De fleste systemer forhindrer at du kan fakturere en ordre der varene ikke er tatt ut av lageret,

dvs. pakkseddel er utstedt. Det er derfor viktig å kontrollere at det ikke er mulig å fakturere en ordre som ikke er levert. En faktureringsjobb skal bare fakturere de ordrer som er levert. Det er derfor viktig å kontrollere dette. Når faktureringsjobben er kjørt, vil alle bokføringer knyttet til salget være prosessert. Det er derfor viktig å sjekke at konteringsreglene knyttet til faktureringen er riktig. Det vil si at inntekt, mva og kundefordring er riktig bokført.

Det er selvsagt også viktig for revisor å kontrollere at alle utleverte ordrer er fakturert og bokført. Det finnes også i de fleste systemer en rapport for levert ikke fakturert. Denne rapporten kjøres ved hver periodeslutt for å avdekke ev. leverte ordrer som ikke er fakturert. Det er viktig at innholdet i denne rapporten verifiseres.

For å kontrollere at funksjonaliteten i transaksjonsstrømmen fungerer, er det tilstrekkelig å følge en ordre fra opprettelse til fakturering og påse at kontrollene fungerer. I og med at logikken er den samme for alle ordrer som går gjennom systemet, vil alle ordrer «oppføre» seg på samme måte og man har derfor sikkerhet for at aller ordrer er prosessert på riktig måte med riktig bokføring. Hvis det er flere ordretyper med forskjellig logikk, vil det være nødvendig å se på en ordre for alle ordretyper.

Riktig datagrunnlag

Hvordan vet man at de dataene som systemet gir oss i form av rapporter og beregninger er riktige og har fungert gjennom hele perioden? Det er her generelle IT-kontroller kommer inn. Tradisjonelt sett har revisjon av generelle IT-kontroller vært det som man har forbundet med IT-revisjon. Vi har endret fokus. Revisjon av generelle IT-kontroller har liten hensikt så fremt man ikke kan knytte dem opp mot risiko for feil i dataene på regnskapspåstandsnivå. Det betyr at de generelle IT-kontrollene man velger å teste, indirekte skal ha påvirkning på revisors mulighet til å bekrefte revisjonsmålsettingene (CEAVOP). Ved å teste generelle IT-kontroller verifiserer man at ingen uautoriserte personer har hatt tilgang til å gjøre noe i systemene – gjennom hele perioden. Det kan dreie seg om å gjøre endringer i logikken i systemet og masterdata eller ved å initiere og prosessere transaksjoner som ligger utenfor de enkelte personers myndighetsområde. Ved å verifisere at arbeidsdeling er implementert i økonomisystemene vet man at ingen har vært inne og gjort noe med systemene og man kan dermed stole på den funksjonaliteten og de data som ligger i systemet. For eksempel vet man da at ingen andre enn de som har lov til å endre på bankkontonummer hos leverandører kan gjøre denne endringen.

Endringer er nødvendig i moderne IT-systemer. Nye lovkrav, behov for å effektivisere/automatisere forretningsprosesser, nye rapporteringskrav osv. gjør det nødvendig å endre funksjonaliteten eller rapportene i systemet. Hvis man ikke har kontroll på disse endringene, vil dette kunne føre til at økonomisystemene ikke fungerer som de skal og det kan dermed føre til feil i regnskapet. Ved å bekrefte at revisjonskunden har kontroll på hvem som kan godkjenne, teste og implementere endringene i systemet har man sikkerhet for at den funksjonaliteten man vet fungerer fra før ikke er endret, samtidig som man får sikkerhet for at endringene også fungerer som de skal. Det gir også sikkerhet for at alle slike endringer er autorisert.

Gjennom gode tilgangs- og endringskontroller får man sikkerhet for at integriteten i systemet og dataene er ivaretatt og at man dermed kan bygge på logikken i systemene i revisjonen.

IT-revisjon

IT-revisjon er altså revisjonsteknikker der man evaluerer hvordan IT-systemene støtter regnskapsavleggelsen. IT-revisoren er en spesialist som deltar som en del av revisjonsteamet hvis risikoen knyttet til anvendelsen av IT-systemene er for stor til at en vanlig revisor har kompetanse til å håndtere den. IT-revisjon bør anvendes på de fleste kunder og svært mange av IT-revisjonshandlingene kan gjennomføres av «vanlige» revisorer, enten alene eller under veiledning fra en IT-revisor. Ved i større grad å anvende IT-revisjon i finansiell revisjon vil man kunne effektivisere og forbedre kvaliteten på revisjonen ved enkelt å bekrefte rutinetransaksjoner ved å bygge på automatiske kontroller. Samtidig vil anvendelse av dataanalyser som verktøy gi bedre effektivitet og kvalitet i substanskontrollene. På denne måten frigjør man tid til å kunne gjøre bedre handlinger på ikke-rutine-transaksjoner og vanskelige regnskapsmessige problemstillinger.

IT-revisjon i finansiell revisjon:

Planlegging

- Hvordan IT-systemene påvirker regnskapsavleggelsen: Kartlegging av hvilke IT-systemer som har påvirkning på regnskapet, hvordan de påvirker og risikoen for at funksjonalitet og anvendelse av systemene kan medføre vesentlige feil i regnskapet.
- ELC: Kartlegging og testing av IT-relaterte kontroller på selskapsnivå for å avdekke hvordan ledelsen i selskapet har kontroll på at IT-systemene støtter regnskapsavleggelsen på en tilfredsstillende måte.
- ITGC: Kartlegging og testing av selskapets kontroller for forvaltning, endring og tilgang til IT-systemene.

Kontrolltesting

- Kartlegging av hvordan transaksjonsstrømmene initieres, prosesseres og bokføres i IT-systemene.
- Automatiske kontroller: Kartlegging og testing av automatiske kontroller (funksjonalitet som sikrer eller forhindrer hendelser i IT-systemene).
- IT-avhengige kontroller: Kartlegging og testing av IT-avhengige kontroller (systembaserte rapporter og skjermbilder som benyttes for manuelle kontrollformål).

Substanskontroller

- Dataanalyse for å gjennomføre analyse og test av detaljer som substanskontroll. KPMG benytter IDEA som verktøy for dataanalyse.