IT-risikoer og kontroller

Hunton, J.E. kap 3

Prosessen risikostyring av IT

- Identifisere IT-risiko
- Identifisere (intern-)kontroller for hver risiko
- Dokumentere interkontrollen

IT-risikoer

- Forretningsrisiko
- Revisjonsrisiko
- Sikkerhetsrisiko
- Kontinuitetsrisko (beslektet med “Fortsatt drift risiko”)

Forretningsrisiko

- IT-relatert forretningsrisiko
  - risiko for ikke å nå forretningsmessige mål
    - IT i primær verdikjede
    - IT som støttefunksjon
- Styres ved
  - identifikasjon av risiko
    - kartleggingsmetoder?
  - risikovurdering
  - identifikasjon av relevant kontroll
    - en-til-en sammenheng r::k?
  - dokumentasjon av kontroller

Revisjonsrisiko

- Eksternrevisors feilaktige attestasjon av regnskapet
- IT-revisors manglende avdekking av
  - vesentlige feil i IT-systemets funksjon eller resultater
  - mislighet eller andre forhold som strider mot lov eller bedriftens regler
- Hva med manglende avdekking av lav effektivitet?
- (RR =Iboende R * Kontroll R * Oppdagelses R)

Sikkerhetsrisiko

- Konfidensialitet
- integritet
  - FNP og i tide
  - autorisert prosess
  - (andre integritetsbegreper?)
- tilgjengelighet

- Hvordan måle og dokumentere disse tre?
  - Revisjonsbevis med ulik kvalitet

Continuity Risk
Avbruddsfri drift

- Tilgjengelighet
  - feil
  - Overbelastning
    - Denial-of-service attacks
  - kapasitet
- Sikkerhetskopier, reserveløsninger, etc

IT-risiko:
En mulig modell for trusselvurdering

- 1. Identifisere trusler
  - Sikkerhetsdimensjonene
    - Konfidensialitet
    - Tilgjengelighet
    - Integritet
  - I tide (ajourhold)
  - Nøyaktighet
  - Infrasturktur
- 2. Bestem sårbarheten for trusselen
- 3. Fastsett akseptabelt risikonivå

Måling av risiko

- (For å begrense revisjonsomfang og revidere målrettet og kostnadseffektivt)
- Risikoindikator
  - = svikt i (oppfyllelsen av) et kontrollmål
  - Kontrollmål: fra rammen gitt i revisjonsmetodikken
- ISACA Audit Procedure #1: IS Risk Assessment Measurement
  - vektet rangerings- og skår-variabler

- Eks på måling: Hunton et.al.: Are Financial Auditors overconfident in Their Ability to Assess Risk . .

Aktuelle rammeverk for risikostyring

- Kontroller tilordnes risikoer
- Kontrollmodeller for IK
  - COSO - 5 komponenter
    - kontrollmiljø, risikovurdering, kontrolltiltak, IKT-systemet, overvåkning
  - CoCo, Cadbury
  - ISO (ISO 9000, ISO 17799)
  - SAS 55, SAS 78, SAS94, SAS95
  - RS 315
  - Cobit
  - Trust services
  - Virksomhetsstyring (Sox, Jaap Winthers, børsanbefaling)

Måling og dokumentasjon

- (=Revisjonbevis)
- Grafisk
- Databaseskjema, metadata
- Formelle beskrivelses-språk (UML)
- Selvvurdering/spørreskjema (self assessment)

- Overvåkning / uavhengig bekreftelse

It-risiko og ÅR

- Risiko for
  - feil i regnskapet
  - manglende ajourhold
  - prosedyrefeil (f.eks. manglende sikkkerhetskopi)
  - Kontrollsporsvikt (bevis for regnskapspåstand)

RS315
Revisors behov

- Identifisere og vurdere rikiko for vesentlig feilinformasjon i regnskapet
- Datagrunnlag for risikovurderingshandlinger
- Arbeidsform: revisjonsteamet
- Forutsetninger for foretakets resultatmåling
- Særskilt risiko
  - Mislighet
  - Systemendring herunder regnskapsstandardendringer
- Dokumentasjon av revisors arbeid

RS315

- 2. forstå foretaket for å vurdere risiko for feil i regnskapet
- 35. hvordan utføres resultatmåling
- 39. kan være basert på forutsetningen om nøyaktige data

RS315 INTERNKONTROLL

- 41 og 48. Kontroller som er relevante for revisjonen
  - Knyttet til risikoer for feil i regnskapet
- 49. Kontroller av fullstendig og nøyaktige data dersom revisjonshandlinger bygger på dataene
- 54. Vurdering av IK og teste om IK er iverksatt
  - 56 IT-baserte kontroller kan anses som iverksatt

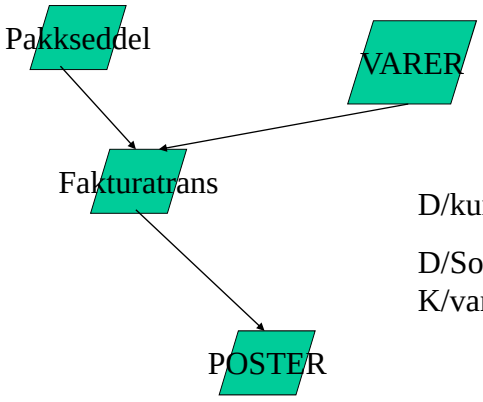
RS315 Manuelle vs automatiserte kontroller i IK

- 57. Kjenne automatiseringsgrad
- 58. Automatiseringens følger for regnskapsrapporteringen
  - Manuelle kontroller
  - Automatiserte kontroller
- 60. IT-risikoer for IK
  - Unøyaktige data eller programmer
  - Uautorisert behandling (manglende data- og program-integritet)
  - Datatap og driftsavbrudd (manglende tilgjengelighet)

RS315 Forstå RIS

- 81. Prosedyrer for økonomisk rapportering som fører til årsregnskapet:
  - Initiere
  - Registrere
  - Behandle
  - Rapportere
- Transaksjoner
- Tabellene
- 82. overveltning
- 83. standardposteringer
- 84. ikke-standard posteringer
- 86. urettmessig overstyring av posteringer

Eks. standard post: varesalg



D/kunde K/salgskonto

D/Solgte varers kost
K/varelager

Aktuelle kontroller?

RS315.87 Håndtering av feil

- Manglende fullstendighet og nøyaktighet
- Kontroll over feilene
  - Omfang og tid
- Evt overstyring og omgåelse av en kontroll
- Tre standardprosedyrer
  - Forkaste transaksjonen
  - Tilbakesending til tidligere rutinepunkt
  - Delvis regnskapsregistrering (observasjonskonto)

RS315.93 Klientens håndtering av IT-risiko

- 90. Vurdere risiko for feilinfo i ÅR og risikotilpassede ytterlige revisonshandlinger
- 91. Kontrollaktiviteter som forebygger, avdekker, korrigerer feilinformasjon
- Har klienten utformet kontrollaktivitetene slik at IT-risikoer hensyntas? (91. revisors behov)
  - 94. Generelle kontroller
  - 95. Applikasjonskontroller

Overvåkning av kontroller 96-99

- Hvilke kontroller baserer foretaket seg på?
- Hvordan håndterer foretaket forhold som kontrollen avdekker?
- De kontrollene som sikrer de data som revisor bygger på
- Vurdere foretakets nøyaktighetsforutsetning i overvåkning av driften
  - Risiko for ledelsesfeil

108. Særskilte risikoer

- Blant identifiserte risikoer
  - De som krever spesiell revisjonsmessig vurdering
    - Sannsynlighet
    - Konsekvens
- 110-111. vesentlige og ikke-rutinemessige transaksjoner

RS315.115-118 Test av kontroller når substanskontroll ikke er effektivt

- 116. unøyaktig / ufullstendig behandling
  - Bortfall av trans ved programfeil
    - Select if bilagstype=14
    - Select if bilagstype=15
    - Hva skjer hvis det kommer en annen bilagstype enn 14 eller 15?
- 117. automatiserte forretningstransaksjoner
  - Revisjonsbevis (trans) kun elektronisk lagret
    - Risiko for at trans fjernes, endres
    - Kontroller for å sikre integritet

Risiko ved å ta IT i bruk

JH kap 4

24

Anbefalinger om organisering (Cobit PO Planlegning og organisering)

- Strategisk plan
- Infoarkitektur
- Teknologisk retning / selskapets behov
- Optimal organisering
- Riktig forvaltning av IT
- Kommunisere og iverksette IT-policy
- Personalledelse
- Regeletterlevelse
- Iverksette risikostyring
- Prosjektstyring, metodisk anskaffelse og utvikling
- Kvalitetsstyring av IT

25

Policyområder

- Planleggingspolicy
  - ansvar, tid, hvordan, dokumenterte resulatater, prioritering
- Organisasjonspolicy
  - struktur, risiko
- Personalpolitikk
  - opplæring, forfremmelser, slutteproseyrer
- Programvare/maskinvarepolicy
  - anskaffelse, standarder, endringer, implementering
- Nettverk
- Sikkerhet
  - testing, tilgang, overvåkning, brannvegger, reaksjoner ved brudd
- Drift
  - organisering, ansvar, inndata, behandlingsformer, feilhåndtering
- Avbruddsfri drift
- Økonomisk styring

26

Prosjektstyring

- Dekke behov (mål)
- Beskrankninger
  - Tid, kostnad, regler, ressurstilgang og kompetanse
- Faser
  - prosjektplan, detaljert tid og ressursplan, oppfølgning av planen (måling), styring (gjenvinne kontroll), formell prosjektslutt

27

Pragramvareanskaffelse

- Strategisk riktig
- SDLC-fasene
  - behov
  - logisk løsning
  - fysisk realisering
  - Implementeridg
  - (drift)
  - (avvikling)
- Enkelte detaljer
  - Livstidskostnad
  - Akternative løsninger
- Risikoer
  - ikke-metodisk arbeid
  - manglende prosjekt- og domene-erfaring
  - tilfeldig og smal faktainnsamling
  - avvik i mål, tid, kostnad

28

Enkelte andre momenter ved SU

- Manglende rutineendring ved endret datasystem(Business Process Reengineering)
- Skille mellom utvikling, test og drift (tilgangskontroll)
  - programbibliotek og databaser
- Innebygge sikkerhet i alle systemkomponenter
- Konverteringstilpasning
  - Gamle dataformater overføres
  - Manglende dataverdier(egenskaper) når objekt overføres
- Testing før implementering
  - enhetstest, modultest, test av hele systemet, belastningstest
- Opplæring og dokumentasjon

29

Endring av applikasjoner

- Endring vs nyutvikling
  - Spm om definisjon av ”ny”
  - Vedlikehold / feilretting vs prosjekter / nyutvikling
- Styrte endringer
  - Behov, beslutning, utvikling, test, implementering
  - Versjonsstyring
- Planlegging av implementering
  - Dataformat-konvertering
  - Kontrollspor

30

Utførelse av IT-revisjonen

JH kap 9

31

ISACAs revisjonssyklus og SA3000

(standarder for attestasjonsoppdrag som ikke er revisjon eller begrenset revisjon)

- Planlegging
- Risikovurdering
- Utarbeide revisjonsprogram
- Bevisinnsamling
- Konkludere
- Avgi revisjonsberetning
- Oppfølgning

- SA3000.3: Praktiserende finansielle revisorer må innordne sin bruk av ISACA std etter SA3000

- Effektiv utførelse av oppdraget
  - (jf. RS300.2 ”Måleffektiv”, jf COSO ”Effectiveness”, ”Efficiency”)
- Vurdere vesentlighet og redusere risiko til akseptabelt nivå 32
- Tilstrekkelige og hensiktsmessige bevis
-
- Attestasjonsuttalelse
-

32

Planlegning

- Revisjonens omfang (Scope)
  - Hva som skal gjøres er avhengig av oppdraget
    - F. eks. applikasjonsgjennomgang, gjennomføre (Cobit-)kontroller, vurdere generelle kontroller, osv.
- Vesentlighet
  - Finansielle transaksjoner
  - Ikke-finansielle transaksjoner
    - Systemkostnad, kritikalitet, omstillingsevne, . . . ?
- Tredjepartsdrift
  - Uttalelser fra serviceorg revisor (RS402)

33

Risikovurdering

- IT-risikoer ved drift
- Vesentlighet og kritikalitet
- Selvvurdering av internkontrollen

34

Revisjonsprogrammet ihht ISACA
(jf. RS300.3: Revisjonsstrategi og plan)

- Revisjonsomfang (Scope)
- Revisjonsmål
- Revisjonshandlingene
- Planlegging og rapportering av revisjonen

35

Bevisinnsamling

- Observere driften
- Undersøke spor (logger)
  - Endring, tilgang, autoriseringstabeller
- Systemdokumentasjon
- Analyseprogrammer i ACL, IDEA e.l.
- Utvalgstesting

36

Konkludere

- Er revisjonsmålene nådd
- Var revisjonshandlingene tilfredsstillende
- Rapportering til oppdragsgiver
  - Dilemma:
    - Kontrollrapport negative avvik
    - Endringsagent

37

Beretning / rapport

- Ingen legalkrav, men ISACA anbefaler (jf. SA3000.49)
  - Organisasjonsnavn
  - Tittel, signatur, dato
  - Revisjonsmål: hvilke og resultat
  - Revisjonsomfang og begrensning i revisjonsomfang
  - Målgruppe for rapporten
  - Standarder som revisjonen har fulgt
  - Detaljert beskrivelse av vesentlige funn
  - Delkonklusjoner
  - Forslag til forbedringer og rettelser
  - Relevante hendelser etter avslutningen av revisjonen

38

Oppfølgning

- Diskutere med den reviderte om endringer og korreksjoner
- Følge opp
  - Etter en fastsatt tid, eller
  - I neste revisjonssyklus

39

SAS94 ITs virkning for IK (se også JH fig 3-5)

- SAS94 er amerikanske standard, men
  - Kan gi typiske momenter for revisjonen
  - Må sammenholdes med RS315 og SA3000
- Test av kontroller må utføres
  - RS315.115 Test av kontroller, ikke bare substanskontroll
  - RS315.81 Transaksjonsflyten
  - RS315.83-84 Behandling av std og ikke-std transaksjoner

40

Hovedelementer i en SAS94-revisjon

- Fysisk system og miljø
- Systemadministrasjon (OS, DBMS, rot-passord)
- Gjennomgang av applikasjoner
- Nettverkssikkerhet
- Avbruddsfri drift, tilgjengelighet
- Vurdering av dataintegritet

41