

IT-risikoer og kontroller

Hunton, J.E. kap 3

1

Proessen risikostyring av IT

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

2

IT-risikoer

- Forretningsrisiko
- Revisjonsrisiko
- Sikkerhetsrisiko
- Kontinuitetsrisiko (beslektet med "Fortsatt drift risiko")

3

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

4

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

6

Continuity Risk Avbruddsfri drift

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

7

IT-risiko:

En mulig modell for trusselvurdering

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

8

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
 - ISA 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

11

It-risiko og ÅR

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

12

ISA315 Revisors behov

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

13

ISA315.3 Revisors mål

- Forstå foretaket for å vurdere risiko for feil i regnskapet
 - Forstå enheten (klienten)
 - Identifisere risiko
 - Anslå risiko
- Feil, mislighet
 - På regnskapsnivå
 - På (regnskaps-)påstandsnivå

14

ISA315.12 Forståelse av IK (men A68 forståelse er ikke nok)

- A47. Ledelsens manipulering av IK
 - Overstyring av systembaserte gyldighetskontroller
- A51.c ITs virkning på IK gjennom rapportering
- A53 Manuelle (og automatiserte) elementer i IK
- A54 Manuelle og automatiserte IK-elementers virkning på
 - Transaksjoner (initiering, registrering, behandling og rapportering)
- A51. IT bedrer IK
- A56. IT innebærer spesifikk risiko
 - Programfeil
 - Uautorisert tilgang til data og programmer
 - Manglende vedlikehold av systemer
- A59. Risiko påvirkes av systemets art og karakteristika.
 - Utforming og topologi: Sann tid, nettverk, internettilkoblet, . . .

15

ISA315.13 Relevante kontroller (ikke alle er r., jf A89)

- Revisors forståelse av
 - Kontroller som er relevante for revisjonen
 - Er kontrollen effektive og iverksatt?
- A66. Vesentlig feilinformasjon. Effektivt
 - Forebygge
 - Avdekke og korrigere.
 - Kontrollen skal designes til å være effektiv, dernest være iverksatt

16

ISA315.18 Forstå RIS (jf ISA315 Vedl1.1-7)

- Informasjonssystemets deler
 - A81. Prosedyrer for økonomisk rapportering som fører til årsregnskapet:
 - Initiere
 - Registrere
 - Behandle
 - Rapportere
- Vesentlige transaksjonsklasser
 - Tilknyttet regnskapsmateriale
 - Tabellene (A81)
- Hendelser som ikke er transaksjoner
- Prosesser som produserer regnskapsmateriale
- Kontroller knyttet til transaksjoner

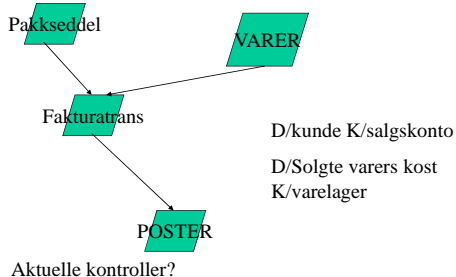
17

ISA 315.18

- A82. overveltning (fra forsystem til hovedbok)
- A82. standardposterings
- A83. ikke-standard posterings
- A84. forretningsprosesser resulterer i transaksjoner til informasjonssystemet

18

Eks. standard post: varesalg



19

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)

20

ISA315.20 Kontrollaktiviteter

- Som revisor mener er nødvendige for å
 - Vurdere risiko for vesentlige feil på påstandsnivå og utforme videre revisjonshandlinger
 - Dvs aktiviteter som er relevante for revisjonen (A89)
- A88. Kontrollaktiviteter
 - Autorisasjon, gjennomgang av resultater, arbeidsdeling

21

ISA315.A95-97 Klientens håndtering av IT-risiko

- A95. Effektiv kontroll
 - Transaksjonenes integritet og sikkerhet (?)
- A96. Generelle kontroller
- A97. Applikasjonskontroller

22

Overvåkning av kontroller

ISA315.22, .A98, ISA315 vedl 1.11-13

- Hvilke kontroller baserer selskapet og revisor sine vurderinger på?
- A89 Har kontrollen fungert i hele perioden?
 - Hvordan bevise det?
 - Er punktmåling tilstrekkelig?
- Vedlegg 1.11: er kontrollen iverksatt?
 - Til rett tid
 - Nøyaktig kontroll

23

ISA315.4 (e) Særskilte risikoer

- Blant identifiserte risikoer
 - De som krever spesiell revisjonsmessig vurdering (.27-.29, .A.119-126)
 - Sannsynlighet
 - Konsekvens
- ISA315.18(f). vesentlige og ikke-rutinemessige transaksjoner

24

ISA315.30 Test av kontroller når substanskontroll ikke er effektivt

- A.127 unøyaktig / ufullstendig behandling
 - Rutinesvakheter
 - 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?
- A.128 Automatiserte forretningstransaksjoner
 - Revisjonsbevis (trans) kun elektronisk lagret
 - Risiko for at trans fjernes, endres
 - Kontroller for å sikre integritet

25

Risiko ved å ta IT i bruk

JH kap 4

26

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

27

Policyområder

- Planleggingspolicy
 - ansvar, tid, hvordan, dokumenterte resultatater, 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

28

Prosjektstyring

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

29

Pragramvareanskaffelse

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

30

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

31

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

32

Utførelse av IT-revisjonen

JH kap 9

33

ISACAs revisjonssyklus og ISAE3000

standarder for attestasjonsoppdrag som ikke er revisjon eller begrenset revisorkontroll

- Planlegging
- Risikovurdering
- Utarbeide revisjonsprogram
- Bevisinnsamling
- Konkludere
- Avgi revisjonsberetning
- Oppfølging
- ISAE3000.3: Praktiserende finansielle revisorer må innordne sin bruk av ISACA std etter ISAE3000
- Effektiv utførelse av oppdraget
 - (jf. ISA300.4 "Måleffektiv", jf COSO "Effectiveness", "Efficiency")
- Vurdere vesentlighet og redusere risiko til akseptabelt nivå
- Tilstrekkelige og hensiktsmessige bevis
- Attestasjonsuttalelse

34

Planlegging

- 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 (ISA402)

35

Risikovurdering

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

36

Revisjonsprogrammet ihht ISACA (jf. ISA300)

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

37

Bevisinnsamling

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

38

Konkludere

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

39

Beretning / rapport

- Ingen legalkrav, men ISACA anbefaler (jf. ISAE3000.49)
 - 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

40

Oppfølging

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

41

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 ISA315 og ISAE3000
- Test av kontroller må utføres
 - ISA315.30 (jf A127-128) Test av kontroller, ikke bare substanskontroll
 - ISA315V1.9(2 pkt) Transaksjonsflyten
 - ISA315.82-83 Behandling av std og ikke-std transaksjoner

42

Hovedelementer i en SAS94-revisjon

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

43
