

IKT-revisjon - som del av internrevisjonen

Nasjonal Fagkonferanse i Offentlig Revisjon 2010

26. oktober 2010

Kent M. E. Kvalvik, kent.kvalvik@bdo.no

INNHold

Litt bakgrunnsinformasjon	
Personalia	3
NIRFs nettverksgruppe for IT-revisjon	4
Hvorfor?	
Informasjonsteknologi og risiko	5
Operasjonell IT-revisjon	8
Krav i standard	9
Hvordan?	
IT-revisor og andre revisorer	11
IT-kompetanse	16





LITT BAKGRUNNSINFORMASJON

Personalia

- Leder for Technology Risk Services i BDO AS *
 - Technology Risk Services er BDOs avdeling for finansiell og operasjonell IT-revisjon, IT-sikkerhet og -rådgivning
- 17 års erfaring innen IT, hvorav de 11 siste årene knyttet til styring og kontroll av IT
- Mastergrad i IT-ledelse, internrevisjon, risikostyring og prosjektledelse
- Relevante sertifiseringer er CGEIT, CIA og Dipl. IR
- Har vært styremedlem og medlem av ulike komitéer i ISACA i en årrekke
- Nåværende leder av NIRFs nettverksgruppe for IT-revisjon

* BDO er Norges og verdens femte største revisjons- og rådgivningselskap, med kontorer over hele landet og nærmere 600 ansatte



LITT BAKGRUNNSINFORMASJON

NIRFs nettverksgruppe for IT-revisjon

Formål

- Øke alle internrevisorers kunnskap om informasjonsteknologi
- Bygge bro mellom ikke-IT-revisorer og IT-revisorer, med den hensikt å øke nytten og verdien av internrevisorers arbeid for sine virksomheter

IT-nettverket arbeider for

- å være et nettverk for IT-interesserte revisorer
- å bringe sammen interne revisorer, eksterne revisorer og spesialister på IT-revisjon
- å integrere IT-revisjon i målsettingen ved all operasjonell revisjon
- at virksomhetenes behov for revisjon av prosesser hvor IT inngår skal bli dekket på en forsvarlig måte



INFORMASJONSTEKNOLOGI OG RISIKO

Integrert i virksomhetens prosesser

- En samlet forståelse av både IT-miljøet, linjeaktiviteter og prosesser er en forutsetning for en effektiv og målrettet internrevisjon
 - IT-løsningene blir en stadig større og mer integrert del av virksomhetens prosesser
 - All lagring og behandling av data skjer hovedsakelig i IT-systemene
 - Interne kontroller blir i økende grad innebygget i IT-systemene
 - Dokumentasjon og revisjonsbevis ligger i IT-systemene



INFORMASJONSTEKNOLOGI OG RISIKO

Endringer i risikobildet

- Bruk av informasjonsteknologi gir muligheter for å redusere risiko på en rekke områder
 - men kan samtidig introdusere nye, vesentlige risikoområder og feilkilder
- Det er lav risiko for tilfeldige feil i kontroller eller ved behandling av data og transaksjoner i IT-systemer
 - men dersom det oppstår en feil, er det derimot ganske sannsynlig at feilen gjelder alle transaksjoner av samme type eller periode



INFORMASJONSTEKNOLOGI OG RISIKO

Manglende tilpasning til virksomheten

- Automatiske kontroller i IT-systemene kan gi forbedret og mer robust internkontroll
 - men de må være tilpasset prosessene de understøtter
- Stadig økt bruk av rammeverk for god praksis både for IT-prosesser, IT-kontroller og IT-risiko
 - men manglende tilpasning av standardiserte rammeverk og sjekklister til virksomheten kan gi falsk trygghet av effektivitet og kontroll



OPERASJONELL IT-REVISJON

Formålet med operasjonell IT-revisjon er å tilføre nødvendig IT-kompetanse til internrevisjonsfunksjonen

- risikovurdering
- planlegging
- gjennomføring
- oppfølging



KRAV I STANDARD

- Standarden for internrevisjon (IIA 1210.A3) sier
- ”Interne revisorer skal ha kunnskaper om de viktigste risikoer og kontrolltiltak innenfor informasjonsteknologi, og tilgjengelige teknologibaserte revisjonsteknikker for å utføre sine tildelte arbeidsoppgaver.”
- ”Det forventes imidlertid **ikke** at **alle** interne revisorer skal ha samme **ekspertise** som en internrevisor som har **IT-revisjon** som sitt primære ansvarsområde.”
- I *Revised Standards* gjeldende fra januar 2011 er dette uendret



Metoder, rammeverk og verktøy er rimelig enkelt å håndtere.

Virksomhetsforståelse, kommunikasjon og samarbeid er vanskeligere - også for IT-revisorer

IT-REVISORER OG ANDRE REVISORER

Suksesskriterier





IT-REVISORER OG ANDRE REVISORER

Virksomhetsforståelse og risikovurderinger

- Revisjonsteamet må se på IT som en av mange risikoområder som må håndteres
- IT-revisor må forstå
 - virksomheten og revidert enhets målsetninger
 - virksomhetens overordnede system for risikostyring
 - aktuelle regulatoriske krav
 - faktiske verdidrivere



IT-REVISORER OG ANDRE REVISORER

Integrasjon med revisjonsteam

- IT-revisor bør være en naturlig del av revisjonsteamet
- IT-revisor bør delta på alle planleggingsmøter og statusmøter
- IT-revisor bør involveres tidlig
- For spesifikke IT-revisjoner bør revisjonsledere med ansvar for berørte enheter og/eller prosesser involveres i planlegging og rapportering



IT-REVISORER OG ANDRE REVISORER

Kommunikasjon

- Jevnlig kommunikasjon fra start til slutt, både med øvrig revisjonsteam og revidert enhet
- IT-revisor må evne å formidle hvilke konsekvenser IT-revisjonen kan ha for øvrige revisjonsområder og prosesser
- Funn fra mer tekniske IT-revisjoner må kunne relateres til faktisk risiko for virksomheten
- Tilpasse kommunikasjon til mottager



IT-REVISORER OG ANDRE REVISORER

Gi verdi

- Bruk av IT-revisjon må tilpasses beste kost/nytte for revisjonsoppdraget
- IT-revisjonen må søke å bidra til forbedret styring og kontroll med IT-miljøet, både hos revidert enhet og i virksomheten generelt
- Involver øvrige revisorer slik at generell IT-kompetanse i internrevisjonen økes



IT-KOMPETANSE

Grunnleggende IT-kunnskap for alle

Fra GTAG ”Informasjon, Teknologi, Kontroll”

- Kunnskap om hvordan IT blir brukt og om relaterte risikoer, og evne til å bruke IT som en ressurs i utføringen av revisjonsarbeid, er grunnleggende for revisorens effektivitet på alle nivåer.
- The IIAs ”International Advanced Technology Committee” har identifisert tre kategorier av IT-kunnskap for internrevisorer
 - Alle revisorer
 - Revisjonsledere
 - Teknisk spesialist i IT-revisjon



IT-KOMPETANSE

Kategorier IT-kunnskap - Alle revisorer

- Grunnleggende forståelse for sentrale begreper innen informasjonsteknologi
 - Grunnleggende kunnskap om IT-sikkerhet og vanlige sikkerhetsmekanismer
 - Grunnleggende forståelse av IT-kontroller og hvordan IT-miljø påvirker forretningsdriften og vice versa
- Sikre tilstrekkelig kunnskap for overordnet å identifisere og forstå IT-risiko



IT-KOMPETANSE

Kategorier IT-kunnskap - Revisjonsledere

- Grunnleggende IT-kunnskap, pluss
 - Nok forståelse til å behandle IT i planlegging, gjennomføring og rapportering
 - Forstå trusler og sårbarheter forbundet med automatiserte prosesser
 - Nok kunnskap til å kunne vurdere bruk av IT-verktøy i revisjonsvurderinger og tester
 - Nok kompetanse til å sikre at revisjonsmedarbeider har tilstrekkelig IT-kunnskap for gjennomføring av revisjoner
- Sikre målrettet bruk av IT og forstå hvordan revisjonsanbefalinger påvirker virksomhetens risikobilde og måloppnåelse



IT-KOMPETANSE

Kategorier IT-kunnskap - Teknisk spesialist i IT-revisjon

- Det er på dette nivået en vanligvis forbinder IT-kunnskap med IT-revisjon
 - tekniske IT-spesialister med dybdekompetanse innen et eller flere teknologiområder
- Også tekniske spesialister i IT-revisjon må fungere på ledelsesnivå, og relatere sine observasjoner og anbefalinger til virksomhetens risikobilde og måloppnåelse
- Må ha kunnskap om underliggende teknologi, og være kjent med trusler og sårbarheter forbundet med teknologien
- Aktuelle sertifiseringer her kan være CISA og CISM fra ISACA, spesifikke produktsertifiseringer fra leverandører og mer avanserte kurs i bruk av automatiserte IT-verktøy
 - Sikre nok teknologisk kompetanse til å vurdere hvordan kontroller i underliggende teknologi påvirker prosessene og kontrollmiljøet



Når virksomhetsforståelse, kommunikasjon, samarbeid og grunnleggende IT-kompetanse er på plass, kommer rammeverk, metodikk og verktøy av seg selv! *

* I hvert fall nesten av seg selv...



Spørsmål og diskusjon...

