

# ISACA – Serving IT Governance Professionals

– IT-revisjon, IT-sikkerhet og IT-styring (IT governance) fortsatt hovedfokus

Revisorforeningen ISACA vil fortsette sitt fokus på både IT-revisjon, IT-sikkerhet og IT-styring under ny profil. Under slagordene (slogan) *Serving IT Governance Professionals* samler ISACA medlemmer fra flere miljøer og nivåer i ulike organisasjoner.



*Tekst: Stig J. Sunde, CISA, CIA, CGAP, Riksrevisjonen*

I motsetning til revisorforeninger som DnR<sup>1</sup> og NIRF<sup>2</sup> har ISACA<sup>3</sup> en større bredde av fagfolk samlet i en forening som globalt har rundt 50.000 medlemmer, hvorav ca 270 i Norge.

ISACAs medlemmer jobber innenfor revisjon (intern og ekstern revisjon), informasjonssikkerhet på både teknisk og ledelsesnivå i linjen, og som IT-ledere og IT-rådgivere. ISACA ble etablert i 1969 av noen *utbrytere* fra The Institute of Internal Auditors (The IIA<sup>4</sup>), blant annet for å få mer fokus på styring og kontroll av IT (informasjonsteknologi).

I dag ser vi at de øvrige revisorforeninger begynner å få opp øynene for alle risikoene rundt IT. Alle de store foreningene som AICPA<sup>5</sup>, The IIA, IFAC<sup>6</sup>, INTOSAI<sup>7</sup> utarbeider nå flere standarder og veiledninger rettet mot revisjon av informasjonssystemer (IT-revisjon). ISACA sine standarder og veiledninger er et viktig grunnlag for alle disse foreningene, og i flere tilfeller har ISACA bidratt aktivt i de ulike foreningenes arbeid med å frembringe

både standarder og veiledninger for IT-revisjon. Så når du leser materiale rundt IT presentert av disse ulike foreningene vil du som allerede er med i ISACA kjenne igjen mye av innholdet.

## Hvorfor fokus på informasjonsteknologi?

Informasjonsteknologi (IT) er i dag en viktig forutsetning og integrert del av forretningsprosesser i de fleste virksomheter, selv hos de mindre. Vi leverer selvangivelsen elektronisk, moms rapporteres elektronisk via Altinn (www.altinn.no), vi bruker nettbank med største selvfølgelighet, bestiller drosje uten å snakke med noen andre enn en datamaskin. Jeg sitter i Pretoria eller Tromsø og jobber mot min arbeidsgivers systemer på en forhåpentligvis trygg og sikker måte (hvordan vet vi egentlig det?). Avansert bruk av informasjonsteknologi forandrer måten vi jobber på, og hva vi gjør privat også. Flere virksomheter hadde ikke eksistert uten velfungerende, trygge og sikre informasjonssystemer. Når forretningsprosesser blir fullt integrerte gjennom hele virksomheten, og ut mot både kunder og leverandører (og mot myndighetene via altinn), øker det revisors krav til å forstå risikoer ved informasjonsteknologi. Vi kommer ikke utenom.

## Hva tilbyr ISACA sine medlemmer?

ISACA er en forening som samler medlemmer som jobber daglig med å vurdere og håndtere risikoer i og rundt informasjonssystemer. ISACA utvikler standarder, veiledninger og praktiske hjelpemidler for sine medlemmer og skaper et nettverk av fagfolk som medlemmer kan diskutere med.

## Sertifisert IT-revisor og sertifisert IT-sikkerhetsleder (CISA & CISM)



Økt bevissthet rundt risikoer ved IT bidrar til at ISACA får flere og flere medlemmer. ISACA utsteder også den eneste rene IT-revisorsertifiseringen, CISA (Certified Information Systems Auditor). Denne krever bestått CISA-eksamen og fem års relevant arbeids-erfaring. ISACA Norway Chapter arrangerer eksamens-forberedende kurs som dekker store deler av temaene på eksamen.

ISACA har også mange medlemmer som jobber i linjen med informasjonssikkerhet. ISACA utsteder en egen serti-

<sup>1</sup> DnR: Den norske Revisorforening

<sup>2</sup> NIRF: Norges Interne Revisorers Forening (norske delen av The IIA)

<sup>3</sup> ISACA: Fra 2006 er ISACA gjort om til eget navn, og den opprinnelige forkortelsen blir ikke omtalt lengre

<sup>4</sup> The IIA: The Institute of Internal Auditors (NIRF i Norge)

<sup>5</sup> AICPA: American Institute of Certified Public Accountants

<sup>6</sup> IFAC: International Federation of Accountants

<sup>7</sup> INTOSAI: International Organisation of Supreme Audit Institutions



*Stig J. Sunde, CISA, CIA, CGAP, er senior-rådgiver i metodeseksjonen for regnskaps- og IT-revisjon i Riksrevisjonen. Han er styremedlem i ISACA Norway Chapter, leder i NIRF's nettverksgruppe for IT-revisjon, og medlem i The IIA's Advanced Technology Committee. Stig J. Sunde kan nås via epost: 92838248@netcom.no*





fisering for ledere innenfor informasjonssikkerhet, kalt CISM (Certified Information Security Manager). I tillegg til bestått eksamen krever denne også relevant *ledererfaring* innenfor informasjonssikkerhet. Også her tilbyr ISACA Norway Chapter forberedende kurs.

ISACA utviklet på 90-tallet et rammeverk for IT-styring, kalt COBIT, basert på anerkjente eksisterende standarder og rammeverk, inkludert COSO Internal Control Framework fra 1992. Som kjent kom COSO med Enterprise Risk Management-rammeverket i 2004.



På slutten av 2005 kom COBIT 4.0, basert på blant annet den nye COSO ERM. Det er IT Governance Institute som står bak den nye COBIT 4.0. ISACA etablerte IT Governance Institute i 1998 blant annet for å ivareta den delen av medlemmene som jobber innenfor IT-styring (IT Governance). De som jobber med SOX<sup>8</sup> og IT kjenner allerede til COBIT, som er det rammeverket som er benyttet for de IT-relaterte delene i SOX-dokumenteringen. Mer om COBIT finner du på [www.isaca.org/cobit](http://www.isaca.org/cobit).

Mer informasjon om ISACA og IT Governance Institute finner du her:

[www.isaca.org](http://www.isaca.org)  
[www.isaca.no](http://www.isaca.no)  
[www.ITRevisjon.no](http://www.ITRevisjon.no)  
[www.ITGI.org](http://www.ITGI.org)  
(IT Governance Institute)



<sup>8</sup> SOX: Sarbanes-Oxley Act, lov om dokumentering av intern kontroll for børsnoterte selskaper i USA

# COBIT – Rammeverket for IT-Styring lansert i ny utgave

*Tekst: Stig J. Sunde, CISA, CIA, CGAP, Riksrevisjonen*

## Innledning

*Control Objectives for Information and related Technology (COBIT®)* er ute i ny utgave. COBIT 4.0 har nå sterkere fokus på ledelsens styring og kontroll av IT, og hensyntar metoder vi kjenner fra balansert målstyring og benchmarking i form av modenhetsmodeller. COBIT er ett IT Governance-rammeverk, som oversatt til norsk blir *rammeverk for IT-styring* (IT-styring ser ut til å etablere seg som den norske oversettelsen av uttrykket *IT Governance*). Ansvar for styring og kontroll av IT plasseres hos toppledelsen og styret. Disse må sørge for god ledelse, organisasjonsmessige strukturer og prosesser slik at IT støtter opp under virksomhetens strategier og mål.

## IT-Styring balanserer virksomhetens krav til informasjon

COBIT presenterer god praksis for styring av IT på en strukturert måte gjennom inndeling i domener og prosesser. COBIT er utviklet av fagfolk fra ulike bransjer og ulike deler av verden, og representerer en konsensus hos ekspertene på området. COSO ERM, det helhetlige rammeverket for risikostyring, har vært en del av grunnlaget til COBIT 4.0. COBIT prøver således å være et helhetlig rammeverk for IT-styring. Andre standarder og rammeverk har vært en del av grunnlaget i utviklingen av COBIT, og rammeverket forsøker ikke å konkurrere, men å bygge et overbygg hvor andre standarder går mer i dybden på ulike områder (jf. NS 7799 og ITIL m.fl.).

COBIT kobler sammen forretningsmessig mål og krav i forhold til IT, og organiserer IT-aktiviteter i en generelt akseptert prosessmodell. Den synliggjør hvilke IT-ressurser som må være til stede for å sikre god styring og kontroll, i tråd med virksomhetens målset-

tinger. Dette gjøres gjennom definering av kontrollmålsettinger.

Gjennom en forretningsorientering i COBIT legges det til rette for å måle og sammenligne oppnåelsen av mål gjennom blant annet balansert målstyring.



*– COBIT 4.0 har nå sterkere fokus på ledelsens styring og kontroll av IT*

Stig J. Sunde, CISA

## Ett prosessorientert rammeverk for styring av IT

COBIT sin prosessmodell deler IT inn i 34 prosesser fordelt på ansvarsområdene planlegging, implementering, drift og oppfølging. Disse ansvarsområdene oppfattes å dekke alt som må dekkes på IT i en virksomhet, uavhengig av bransje. For å lykkes med prosessene må ressurser som applikasjoner, informasjon, infrastruktur og mennesker identifiseres i forhold til de forretningsmessige behov.

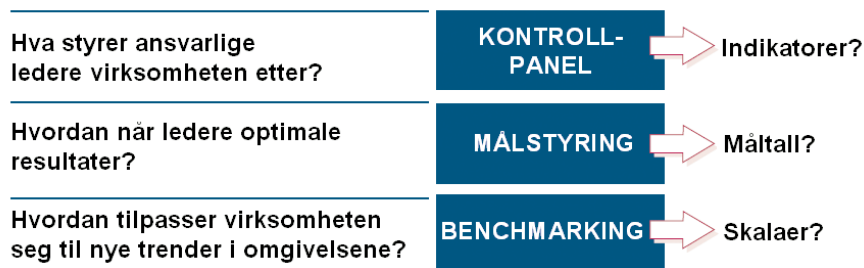
Oppsummert kan man si at for å sikre den informasjonen virksomheten trenger for å nå sine mål, må IT-ressurser styres og kontrolleres gjennom ett sett av naturlig grupperte prosesser.

Men hvordan styrer og kontrollerer virksomheten IT slik at den får den informasjonen den trenger? Hvordan håndterer virksomheten risikoer og sikrer IT-ressursene den er så avhengig av? Hvordan sikrer virksomheten at IT støtter opp om virksomhetens strategier og mål?

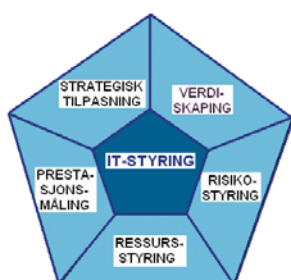
Ledelsen trenger kontrollmålsettinger som definerer mål for implementering av policyer, prosedyrer, rutiner og organisasjonsmessige strukturer som gir rimelig sikkerhet for at:

- Virksomhetens målsettinger oppnås
- Uønskede hendelser blir forhindrede, oppdaget og korrigert

Figur 1 – Ledelsesinformasjon



Figur 2 – Fokuserområder for IT-Styring



**Strategisk tilpasning** fokuserer avstemning av virksomhetens planer med IT-planer; definering, vedlikehold og godkjenning av IT's bidrag til verdiskaping; og avstemning av IT-drift med virksomhetens forretningsprosesser.

**Verdiskaping** handler om iværksettning av IT-planer som sikrer at IT bidrar i tråd med virksomhetens strategi, med fokus på kostnadseffektivitet og reelle verdiskapende IT-tjenester.

**Ressursstyring** handler om optimale investeringer i, og riktig styring av, kritiske IT-ressurser: applikasjoner, informasjon, infrastruktur og mennesker. Hovedfokus er optimalisering av kompetanse og infrastruktur.

**Risikostyring** handler om lederes og medarbeideres risikoforståelse, og klar forståelse av virksomhetens risikoappettitt, forståelse av hvilke regulatoriske krav som skal overholdes, åpenhet om virksomhetens viktigste risikoer, og integrering av ansvar for risikostyring på ulike nivåer i virksomheten.

**Prestasjonsmåling** handler om å følge opp implementering av virksomhetens strategi, fullføring av prosjekter, ressursbruken, prosesser og tjenester, ved bruk av for eksempel balansert målstyring som omsetter strategi til handlinger og tiltak, for å innfri målsettinger som lar seg måle utover tradisjonell økonomistyring.

Ledelsen søker løpende god informasjon for å fatte vanskelige beslutninger om risikoer og kontroll på en best mulig måte. Dette krever kontinuerlig måling av hvor virksomheten er nå, og hva som kan forbedres. Dette gjøres ved hjelp av styringsverktøy. Figur 1 gir en introduksjon til hva COBIT 4.0 presenterer som styringsverktøy.

Benchmarkingen (sammenligning med andre) er basert på Software Engineering Institute's Capability Maturity Modell, mens målstyring er basert på Robert Kaplan og David Norton's balanced business scorecard (balansert målstyring). Aktivitetsmål er basert på COBIT's detaljerte kontrollmålsettinger.

En viktig del av implementeringen av god IT-styring er *leveringsevnen* til de ulike prosessene, og evalueringen av modenheten til disse. Etter å ha identifisert kritiske prosesser og kontroller, vil modenhetsmodellen gi oss avviket mellom eksisterende og ønsket leveringsevne. Ledelsen vil dermed få svar på hva som må til for å nå ønsket nivå, og kunne implementere relevante handlingsplaner og tiltak.

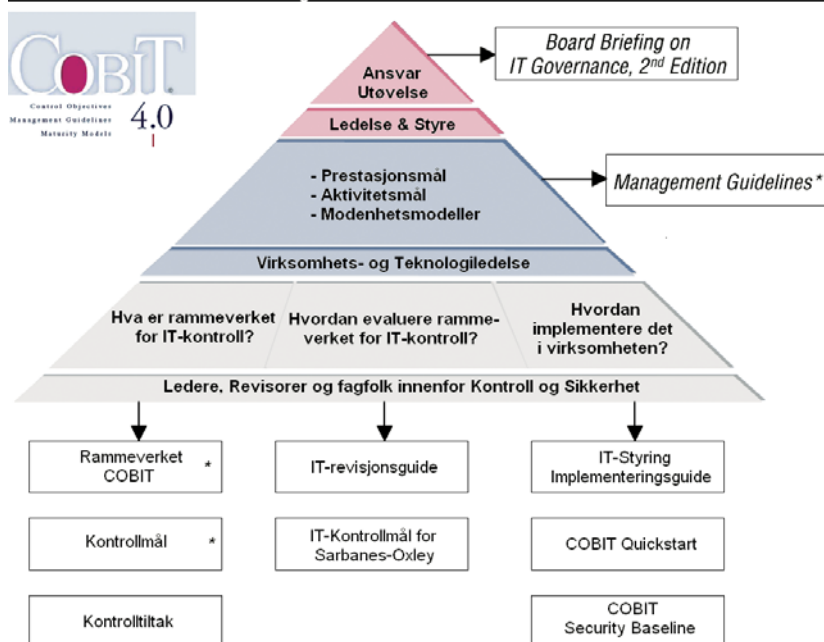
Gjennom COBIT får vi god IT-styring som sikrer at (jf. Figur 2):

- IT er tilpasset virksomheten
- IT er en forretningsdriver og utnytter fordelene ved IT
- IT-ressurser anvendes på en ansvarlig måte
- IT-risikoer styres på en balansert måte

Måling av prestasjon er også en viktig del av god IT-styring. Gjennom COBIT implementerer og følger man opp målbare målsettinger for hva IT-prosessene skal levere (mål) og hvor godt IT-prosessene faktisk gjør det (leveringsevne og prestasjon). Undersøkelser viser at manglende identifisering og synliggjøring av IT-kostnader, verdier og risikoer er en av de viktige driverne for IT-styring. Synliggjøring oppnår man primært gjennom prestasjonsmålinger.

Figur 2 viser fokuserområdene til IT-styring. COBIT's prosessmodell er blitt avstemt mot disse fokuserområdene for IT-styring, og bygger dermed bro mellom hva operasjonelle ledere trenger for å styre og hva toppledelsen trenger for å lede på et mer overordnet nivå.

Figur 3 – COBIT-Produkter

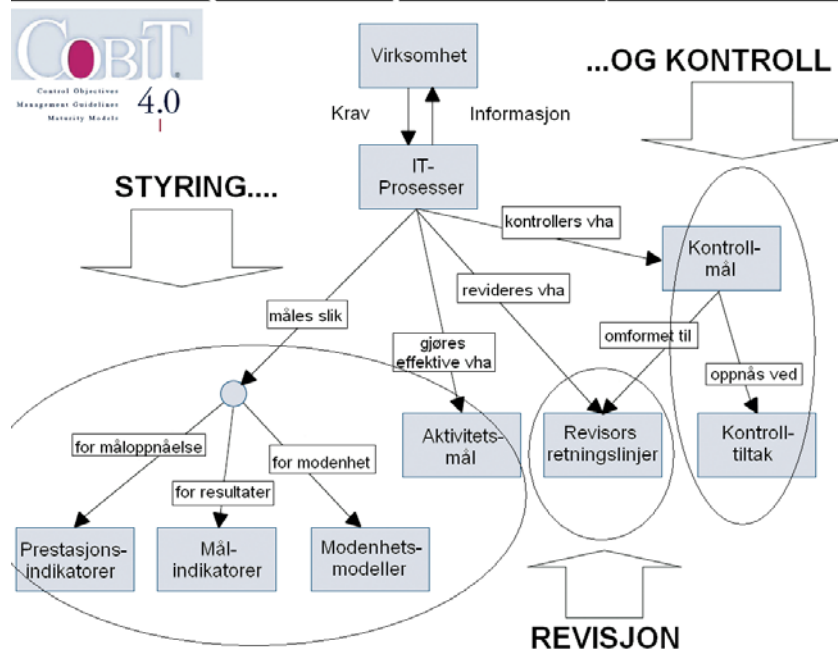


\* Nå integrert i COBIT 4.0  
IT Governance = IT-styring / IT-kontroll

### COBIT-produkter

COBIT fokuserer på hva som kreves for å oppnå god styring og kontroll av IT, på et overordnet nivå, og er avstemt

Figur 4 – Sammenhengen mellom COBIT-komponenter



med mer detaljerte standarder og rammeverk. COBITs produktserie er organisert i tre nivåer, jf. figur 3, for å støtte:

- Styre og toppledelsen
- Forretnings- og IT-ledelsen
- Fagfolk innenfor revisjon, sikkerhet og kontroll

De hvite boksene i figur 3 viser hvilke produkter som henvender seg til de ulike målgruppene for IT-styring. Merk at «IT-revisjonsguide» ikke foreligger før senere i 2006.

I figur 4 summeres opp rammeverket for IT-styring, og viser strukturen for hvordan COBIT styrer og kontrollerer IT. Virksomhetens krav til informasjon danner grunnlaget for IT-prosessen sammen med IT-ressursene, og kontrolleres ved hjelp av kontrollmål og kontrolltiltak. IT styres ved hjelp av aktivitetsmål, prestasjonsindikatorer, målandikatorer og modenhetsmodeller/-evalueringer. Revisor anvender revisors retningslinjer, som er utformet basert på kontrollmålene, i sin revisjon av IT.

### Oppsummering

COBIT er et rammeverk som med tilhørende verktøy gjør det mulig å se kontrollkrav, tekniske forhold og forretningsrisikoer i sammenheng – og ikke minst, kommunisere dette til ulike interessenter. COBIT har blitt en helhetlig god IT-praksis og fremstår som ett paraplyrammeverk for god IT-styring, og bidrar til økt forståelse og

bedre styring av risikoer og muligheter ved IT.

Teksten over er basert på COBITs *executive overview*, og gir bare en kort introduksjon til COBIT og *hva* rammeverket er. *Hvordan* rammeverket anvendes krever mer plass. For mer informasjon om COBIT, sjekk ut [www.isaca.org/cobit](http://www.isaca.org/cobit). Rammeverket kan her lastes ned i sin helhet, forbeholdt ISACA-medlemmer. Ønsker du å bli medlem, se [www.isaca.org/join](http://www.isaca.org/join).

*ISACA etablerte i 1998 IT Governance Institute for å utvikle og forske på bedre metoder for god styring og kontroll av informasjonsteknologi (IT) som støtte til, og driver for, bedre forretningsprosesser. Rammeverket COBIT ble utviklet av ISACA allerede tilbake i 1996, og kom i nye versjoner i 1998 og 2000, og nå sist i 2005.*

*Anvendelse av utvalgte figurer og tekst fra rammeverket er gjort etter skriftlig tillatelse fra IT Governance Institute.*

*Includes content from the COBIT 4.0, which is used by permission of the IT Governance Institute (ITGI).*

*Copyright © 1996, 1998, 2000, 2005 IT Governance Institute (ITGI). All rights reserved.*

