Menetelmällisyyttä tarkastustyöhön

Hannu Haapa-aho
SysOpen Yhtiöt Oy

Atk-tarkastuksen tehtäväalue

Tietojenkäsittelyyn liittyy aina oleellisena osana valvonta:

- liiketoiminnan tietohallinnolle asettamia tavoitteita ohjaa tietohallintostrategiat,
- hankkeiden ja projektien etenemistä seurataan ja ohjataan valvontaryhmissä,
- tietojärjestelmää rakennetaan projektisuunnitelman mukaisesti projektipäällikön valvonnassa,
- käyttöpalvelusopimukset määrittelevät järjestelmälle annettavat käyttötoiminnot,
- järjestelmään sisäänkirjoittautumiseen tarvitaan salasana,
- henkilötunnukselle tai tilinumerolle lasketaan tarkiste
- jne.

Edellä lueteltuja asioita voidaan kutsua yhteisellä nimellä **kontrollit**. Atk-tarkastuksen tehtäväalueena onkin tarkastuksellisin keinoin varmistua tietojenkäsittelytoimintaan liittyvien kontrollien olemassaolosta ja toimivuudesta ja antaa konsultointiapua tarvittavien kontrollien suunnitteluun.

Tarkastustyön menetelmänä COBIT

Tietojärjestelmien rakentamisessa on jo pitkään käytetty erilaisia kehikkoja, kehittämismalleja, joiden tavoitteena on jämäköittää systeemityötä, ohjata työn tekemistä ja antaa yhteinen keskustelupohja niin tietojärjestelmän tilaajalle, käyttäjälle kuin toimittajallekin.

Kuten tietojärjestelmien rakentamisessa tarvitaan kontrollien suunnittelussa ja niiden toimivuuden arvioinnissa menetelmällisyyttä ja yhteistä kieltä, jota tietojärjestelmien eri käyttäjäryhmät: atk-tarkastajat, liiketoimintajohto tietojärjestelmien rakentajat ja käyttäjät ymmärtävät. Yhteisen mallin tehtävänä on myöskin varmistaa tehdyn työn laatu ohjeistamalla tehtävät ja kuvaamalla syntyvät tulokset.

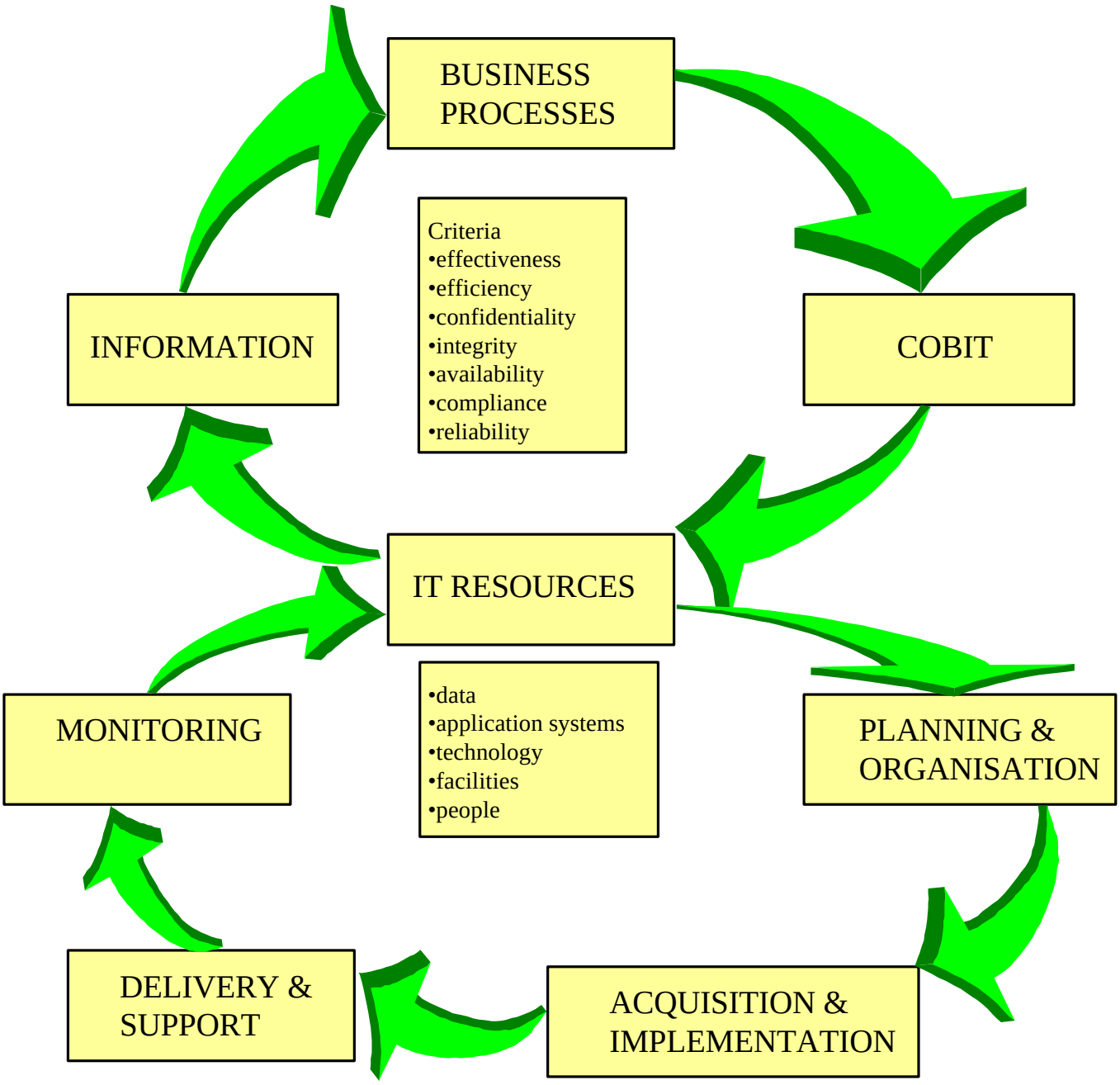
Perinteisesti atk-tarkastajien käytettävissä on ollut runsaasti tietohallinnon eri prosessien ja eri laite- ja ohjelmistoympäristöjen tarkastamiseen liittyviä ohjeita ja kirjallisuutta, mutta ensimmäinen koko tietohallinnon kattava kontrollien arvioinnin, suunnittelun ja tarkastamisen menetelmistö, COBIT (Control Objectives for Information and related Technology), julkaistiin pari vuotta sitten atk-tarkastajien kansainvälisen yhteisön ISACAn (Information Systems Audit and Control Foundation) toimesta.

COBIT:n näkökulma on liiketoimintalähtöinen

COBIT-mallin näkökulma on **liiketoimintalähtöinen** eli kuinka liiketoiminnan tavoitteet saavutetaan ja liiketoiminnan tarvitsemat palvelut tuotetaan mahdollisimman tehokkaalla ja tarkoituksenmukaisella tietotekniikkaresurssien käytöllä.

Tietotekniikkaresursseiksi COBIT-mallissa määritellän tiedot, tietojärjestelmät, teknologiat, laitteet ja henkilöt. COBIT-mallin periaate vapaasti käännettynä kuuluu: ‘Liiketoiminnan tavoitteet määrittelevät tarvittavat tietotekniikkaresurssit, joiden avulla toteutetaan liiletoimintaprosessien tarpeita tukevat tietotekniikkaprosessit (kuva 1).

COBIT-malli on teknologiariippumaton malli, joka soveltuu käytettäväksi kaikissa tietotekniikkaympäristöissä. Malli auttaa johtoa tietojenkäsittelytoimintaan liittyvien riskien arvioinnissa ja tarvittavien kontrolli-investointien suunnittelussa. Käyttäjiä malli auttaa mm. tietojenkäsittely-ympäristön turvallisuuden arvioinnissa, tietojärjestelmien rakentajille malli antaa ohjeita tarvittavien kont-



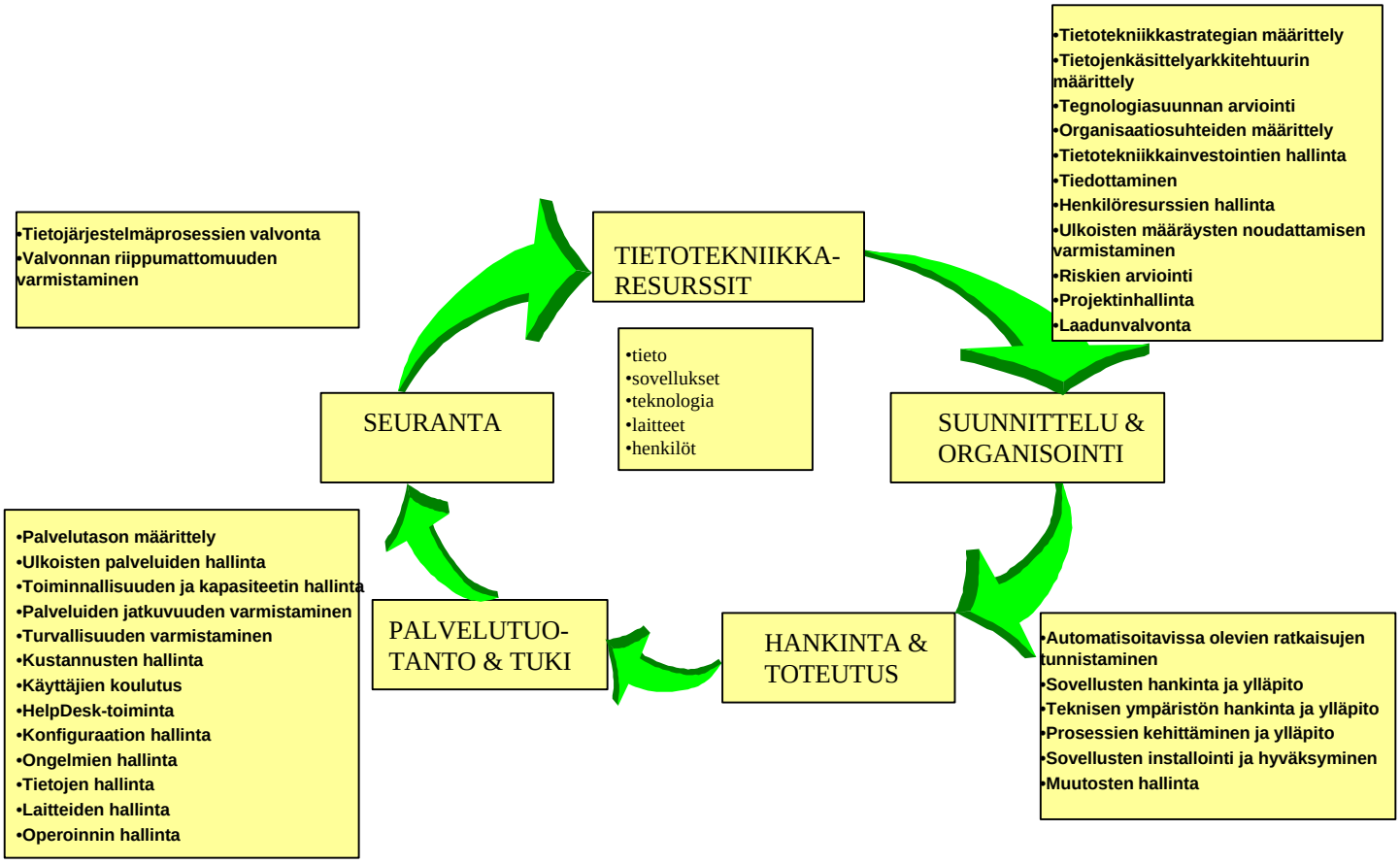
Kuva1: COBIT-malli: Liiketoiminnan vaatimukset tietotekniikalle

rollien suunnitteluun ja atk-tarkastajille malli on sekä tarkastustyötä ohjaava että kontrollitarpeita perusteleva työkalu.

COBIT-mallin rakenne

COBIT-malli jakaa tietojenkäsittelyn neljään päätoimintoon: suunnittelu ja organisointi, hankinta ja toteutus, palvelutuotanto ja tuki ja seuranta. Nämä neljä päätoimintoa sisältävät 32 tietojenkäsittelyn prosessia, siten että koko tietojenkäsittely aina sen johtamisesta palvelutuotantoon ja seurantaan tulee katetuksi. COBIT:n alimmalla tasolla kuvataan kuhunkin tietojenkäsittelyprosessiin liittyvät valvonnan tavoitteet, jotka määrittelevät tietojenkäsittelyprosesseihin liittyvät kontrollit ja joilla varmistetaan liiketoiminnan vaatimusten toteutuminen tietojenkäsittelyssä.

COBIT on herättänyt niin maailmalla kuin meilläkin suurta mielenkiintoa heti julkaisemisesta (1996) lähtien. Toki ennen COBIT:kin atk-tarkastajien käytössä on ollut materiaalia tarkastustyön tueksi, mutta yhtä koko tietotekniikan kattavaa koottua tarkastustyön menetel-



Kuva2: Tietojenkäsittelyn prosessit COBIT:n mukaan jaoteltuna

mistöä ei ole ollut aiemmin saatavilla. COBIT:sta on olemassa myöskin automatisoituja versioita, joissa kontrollitarpeita voidaan etsiä erilaisilla kriteereillä ja joihin voidaan tallentaa tarkastushavainnot ja kehittämisehdotukset sekä tulostaa tarkastusraportit.

COBIT:n kehitteleminen jatkuu ja seuraavaksi on tulossa mm. Organisaation tietojenkäsittelytoiminnan arviointiin liittyviä Self-Assessment-tyyppisiä ohjeita.

Kokemuksia COBIT:n käytöstä

Käytännössä COBIT-menetelmistöstä atk-tarkastustyössä on ainakin SysOpenissa saatu hyviä kokemuksia: COBIT-malli on auttanut mm. tarkastettavan alueen jäsentelyssä ja tarkastustyön suunnittelussa sekä antanut ‘taustatukea’ kontrollitarpeiden perustelussa liiketoimintajohdolle.

Toki ulkoisina tarkastajina työtämme ohjaa ensisijaisesti asiakkaan toimeksianto, mutta COBIT on yleisyytensä takia helppo sovittaa millaiseen kontrollien arviointiin ja tarkastukseen tahansa olipa sitten kyseessä tietohallinnon, sovelluskehityksen tai käyttötoimintojen arviointi. COBIT on myöskin hyvä ‘muistilista’ arvioitaessa suunnitellun tai toteutetun tarkastuksen kattavuutta.

Hannu Haapa-aho
SysOpen Yhtiöt Oy