

Rakenteilla olevan tietojärjestelmän tarkastaminen

*Leena Soikkeli,
KELA, Sisäinen tarkastus*

Rakenteilla olevan tietojärjestelmän tarkastus on yksi tietojärjestelmätarkastuksen osa-alueista. Tietojärjestelmien tarkastuksen ja riskienhallinnan käsikirjan (1) mukaan siinä arvioidaan mm. seuraavia seikkoja: sisältääkö järjestelmä tarvittavat ohjaus- ja valvontatoiminnot; käsittelee否 järjestelmä tietoja täydellisesti, täsmällisesti ja luotettavasti; täyttää否 järjestelmä lakien ja asetusten asettamat vaatimukset; onko järjestelmä toteutettu sovittua systeemityöprosessia noudattaen.

Tietojärjestelmätarkastaja tarkastaa järjestelmäkehitystä kolmella tasolla. Ensin arvioidaan yrityksen käyttämiä kehitysmenetelmiä ja välineitä (kannattavuus, tehokkuus, vertaaminen yleisesti käytössä oleviin järjestelmäkehitystapoihin). Toiseksi tarkastetaan, kuinka hyvin menetelmiä noudatetaan ja välineitä hyödynnetään. Kolmanneksi tarkastetaan, että tietojärjestelmään ja sen käyttöympäristöön on suunniteltu tarvittavat kontrollit (mm. yleiset kontrollit, sovelluskontrollit, ympäristö-, pääsy-, varmistus- ja turvallisuuskontrollit sekä valittuun teknologiaan liittyvät kontrollit). Rajaudun tässä

artikkelissa käsittelemään vain viimeksi mainittua tasoa.

Systeemityöprosessin tarkistuspisteet

Rakentamismallista riippumatta systeemityöprosessissa on tarkistuspisteitä, joissa myös tietojärjestelmätarkastajan tulee arvioida järjestelmän kontroleja, turvallisuutta ja tarkastettavuutta. Tarkastus perustuu projektin eri vaiheissa tuotettuun dokumentaatioon ja osallistujatahojen haastatteluihin. Lisäksi tarkastaja voi aika ajoin osallistua projektikokouksiin asiantuntijana.

Tietojärjestelmätarkastajan rooli on tärkeä varsinkin projektin alkuvaiheissa, sillä mitä myöhemmin jonkin kontrollin tarve havaitaan, sitä kalliimpaa ja työläämpää se on toteuttaa. Se, mitä kontroleja tarvitaan, tulee harkita huolella. Ei ole tarkoituksenmukaista ehdottaa kontroleja, jotka maksavat enemmän kuin mitä uhkia niiden on tarkoitus vähentää.

Määrittäsvaiheen tarkastustehtävät

Alussa mainitussa käsikirjassa on lueteltu systeemityöprosessiin liittyviä tarkastustehtäviä. Esimerkiksi määrittäsvaiheessa niitä ovat seuraavat:

- Tutustu määrittelydokumenttiin.
- Keskustele projektin jäsenien kanssa varmistuaksesi, että kaikki yksiköt, joita järjestelmän käyttöönotto ja käyttö koskee, ovat osallistuneet määrittelyyn.
- Haastattele tilaajayksikön ja muiden järjestelmän vaikutuspiirissä olevien yksiköiden henkilöstöä, jotta voit varmistua, että heidän tarpeensa ja mielipiteensä ovat tulleet esiin määrittelyssä ja että nykyjärjestelmän heikkouksiin on puututtu. Arvioi, onko käyttäjien panos ollut riittävä.
- Varmista, että johto on hyväksynyt projektin aloittamisen ja sitoutunut projektin kustannuksiin (rakentamiskustannuksiin ja arvioituihin käyttökustannuksiin).
- Läpikäy syöttö-, käsittely-, tulostus- ym. määrittelyt ja arvioi käyttäjien tarpeiden täyttyminen.
- Tarkasta kirjausketju (Audit Trail) sekä kontrolli- ja turvapiirteet.
- Mikäli ratkaisu perustuu valmisohjelmiston

hankintaan tai teettämiseen ulkopuolisella, varmistu, että riittävältä määrältä toimittajia on pyydetty ja saatu tarjoukset, jotka kattavat käyttäjien vaatimukset sekä muut toiminnalliset vaatimukset.

- Arvioi, voitaisiinko tietojärjestelmässä käyttää "upotettuja tarkastusmoduuleita". Mikäli soveltuvaa, suunnitelman tulee kattaa myös tämä.
- Vertaa projektisuunnitelman ja budjetin toteutumisen (määritys). Arvioi projektisuunnitelma seuraavalle vaiheelle (järkevyy, kattavuus, realistisuus).

Jälkiarviointi

Rakenteilla olevan järjestelmän tarkastus ei lopu käyttöönottovaiheeseen, vaan käytön vaikiinnuttua suoritetaan vielä jälkiarviointi. Siinä selvitetään mm., täyttääkö järjestelmä yrittäjän johdon ja käyttäjien vaatimukset, toteutuiko hanke suunnitellusti sekä ovatko kontrollit riittävät ja toimivat.

Edellä kirjoitetun olen vapaasti lainannut ja lyhentänyt Tietojärjestelmien tarkastuksen ja riskienhallinnan käsikirjasta. Kirjaa voi suositella henkilölle, joka haluaa tarkemmin perehtyä puheena olevaan aiheeseen tai muihin tietojärjestelmätarkastuksen osa-alueisiin. Lopuksi joitakin ajatuksia mm. Tarkastajan riippumattomuudesta hänen tarkastaessaan rakenteilla olevia järjestelmiä.

Tarkastajan riippumattomuus

Sisäisen tarkastuksen ammattistandardien mukaan tarkastajien tulee olla riippumattomia niistä toiminnoista, joita he tarkastavat. Riippumattomuutta joutuu pohtimaan uusi tietojärjestelmätarkastaja, joka siirtyy yrityksen atk-yksiköstä tarkastajaksi. Tällaista siirtymistä tapahtuu, sillä atk-asiantuntijasta on yleensä helpompi kouluttaa tarkastaja kuin hankkia tarkastusammattilaiselle riittävä atk-osaaminen ja -kokemus. Jos yrityksessä on useampia tietojärjestelmätarkastajia, voidaan helposti välttää tilanteet, joissa joutuisi tarkastamaan omia töitään. Lisäksi tietotekniikan kehitysvauhti pienentää riippumattomuusongelmaa yllättävänkin nopeasti. Jo parissa vuodessa tapahtuu niin paljon muutoksia, että tarkastuskohteita, joissa itse on aikaisemmin ollut mukana, tulee harvoin eteen.

Toinen tilanne, jossa riippumattomuus on otettava huomioon, on tarkastajan osallistuminen kehittämisprojekteihin. Tästä aiheesta keskusteltiin enemmänkin silloin, kun tietojärjestelmä-tarkastus oli uusi sisäisen tarkastuksen erityisosaamisalue. Nykyisin tarkastajan osallistumista projekteihin asiantuntijana pidetään jopa välttämättömänä.

Esimerkiksi kontrollipuutteiden esiin tuominen vasta atk-järjestelmän käyttöönoton jälkeen ei ole yrityksen edun mukaista. Onkin tärkeää, että kaikkea mahdollista asiantuntemusta

käytetään jo projektin alkuvaiheessa. Riippumattomuuden säilyttämiseksi tarkastaja ei saa osallistua päätöksentekoon, vaan hänen on pitädyttävä asiantuntijaroolissaan.

Yhteistyö

Tietojärjestelmätarkastaja ei useinkaan ole ainoa kontrolliasiantuntija järjestelmien rakentamisprojekteissa. Asiantuntijapuna ja lausuntojen antajina voivat olla myös mm. Tietoturvaan, laatutyöhön, riskienhallintaan ja sisäiseen valvontaan erikoistuneet henkilöt. Yhteistyö heidän kanssaan edistää mahdollisten kontrollipuutteiden esilletuloa riittävän varhain.

Rakenteilla olevien järjestelmien tarkastaminen on mielenkiintoinen tarkastuksen osa-alue, joka tietotekniikan nopeassa kehitysvauhdissa haastaa tekijänsä jatkuvaan kouluttautumiseen ja itsensä kehittämiseen.

Lähdekirjallisuus:

(1) Tietojärjestelmien tarkastuksen ja riskienhallinnan käsikirja, Tietojärjestelmien tarkastus ja valvonta ry, toimittanut Esko Nuuttila, ISBN 951-762-537-5.

Yhteystiedot:

Leena Soikkeli

*Tietojärjestelmätarkastaja,
CISA*

Kela, PL 450, 00101 Hki

puh. (09) 434 1243

leena.soikkeli@

kela.memonet.mailnet.fi