

Tietojärjestelmätarkastus - mitä ja miksi ?

*Esko Nuutila,
PSP sisäinen tarkastus*

Valvonta on osa johtamista tai ohjausta suunnittelun ja toteuttamisen ohella. Tarkastus taas on yksi tapa toteuttaa tätä organisaation johdon velvollisuuksiin ja oikeuksiin kuuluvaa valvontaa. Artikkelissa puhutaan jatkossa yksinkertaisuuden vuoksi vain tietojärjestelmätarkastuksesta. Asiat pätevät kuitenkin myös yleisesti kontroleihin, riippumatta siitä, kuka niitä arvioi tai suunnittelee.

Tietojärjestelmätarkastus käsittää kaikki ne tehtävät, joilla tutkitaan ja arvioidaan tietojenkäsittelytoimintaa, sen johtamista ja valvontaa. Sen tavoitteena on tarkastaa ja varmistaa, että organisaation tietojenkäsittelytoiminnalla on kyky:

- saavuttaa organisaation päämäärät ja tavoitteet sekä käyttää resursseja mahdollisimman tehokkaasti ja taloudellisesti.
- tuottaa oikeaa tietoa, varmistaa tietojen saatavuus, säilyttää tietovarastojen eheys, varmistaa toiminnan jatkuvuus ja turvata organisaation omaisuus, myös tiedot.

Tietojärjestelmätarkastus varmistaa, että organisaation tietojenkäsittely-ympäristön valvontajärjestelyt ovat riittävät, tarkoituksenmukaiset ja toimivat oikein. Tietojärjestelmätarkastuksen rooliin kuuluu myös osaltaan varmistaa, että organisaation tietojenkäsittelyssä noudatetaan lakeja, toimialaa koskevia yms. määräyksiä sekä

organisaation omia toimintatapoja.

RISKIT

Riskitietoisuus on hyvä lähtökohta tarkastustoiminnan suunnittelemiselle ja kohdentamiselle. Se edellyttää riippuvuuksien ja haavoittuvuuden arviointia. Valtaosa tietojenkäsittelyyn kohdistuvista riskeistä on tavanomaisia käyttövirheitä, teknisiä vikoja, häiriöitä ja ohjelmavirheitä, jotka suuren tietotekniikkariippuvuuden takia saattavat vaikuttaa moniin osajärjestelmiin ja estää palvelut aiheuttaen taloudellisia vahinkoja. Riskit kohdistuvat käyttöympäristöön ja sen varustukseen, laitteisiin, ohjelmistoihin, tietoihin, rekistereihin, tietokantoihin, verkkoihin, tiedonsiirtoon, tulostukseen sekä tietohallintoon ja henkilökuntaan.

KONTROLLIT

Kontrollit ovat menettelytapoja ja toimintoja sen varmistamiseksi, että toiminta saavuttaa tavoitteensa. Kontroleja ovat kaikki ne toimenpiteet, joiden tarkoituksena on häiriöiden, puutteiden, virheiden ja väärinkäytösten ennalta ehkäisy, havaitseminen ja vähentäminen. Tietojenkäsittelytoiminnan kontroleilla pyritään myös turvaamaan tietojenkäsittelyn olosuhteet, töiden suorittamisen oikea-aikaisuus, toiminnan ja sitä kuvaavan informaation luotettavuus, omaisuuden säilyminen, liiketoiminnan jatku-

vuus sekä taloudellisuus ja kannattavuus.

Hyvin suunnitellussa tietojärjestelmässä on ohjelmoidut kontrollit, joilla valvotaan sen kaikkia päätoimintoja. Kontrollijärjestelmä sisältää:

- Sisäiset kontrollit. Niillä suojellaan omaisuutta ja tietojen luotettavuutta.
- Toiminnalliset kontrollit, joilla valvotaan päivittäistä toimintaa ja varmistetaan, että toiminta tukee liiketoiminnan tavoitteita
- Hallinnolliset kontrollit, joilla varmistetaan toiminnan tehokkuus ja johdon periaatteiden ja ohjeiden noudattaminen.

TIETOJÄRJESTELMÄ- TARKASTUKSEN TAVOITTEET

Tietojärjestelmätarkastuksen määritelmästä voidaan johtaa mm. seuraavat tarkastuksen tavoitteet: omaisuuden turvaaminen, tietovarastojen eheys sekä järjestelmien tehokkuus ja taloudellisuus.

Omaisuuden turvaaminen

Tietojenkäsittely-ympäristöissä säilytettävään omaisuuteen kuuluvat esim. laitteistot, ohjelmistot, tietovarastot, dokumentaatio ja käyttötarvikkeet. Niiden turvaaminen on varmistettava riittävän tehokkailla kontroleilla. Laitteistot, ohjelmistot ja tietovarastot voivat tuhoutua tai ne voidaan va-

rastaa. Myös tietokonekeskusten fyysinen turvallisuus on tärkeää.

Tietovarastojen eheys

Eheysvaatimus tarkoittaa, että tietovarastossa ei ole puutteita, tiedot ovat oikeita ja että ne ovat ajan suhteen yhdenmukaisia.

Eheysvaatimus on erittäin keskeinen, onhan oikeiden tietojen käytettävyys ehdoton edellytys oikeille päätöksille.

Organisaation päämäärät ja voimavarojen käyttö

Hyvin usein tietojärjestelmätarkastajat keskittyvät turvallisuusasioihin. Vaikkakin ne ovat oleellisen tärkeitä tarkastuskohteita, niin ei pidä myöskään unohtaa muita määritelmän mukaisia alueita. Tietotekniikan tehokkaan ja taloudellisen käytön arviointi organisaation päämäärien saavuttamiseksi on olennainen osa tietojärjestelmätarkastajan työkenttää.

VÄHEMMÄN PUUTTEITA, ENEMMÄN TARPEELLISIA KONTROLLEJA

Tarkastajan päämääränä on todellinen, konkreettinen muutos puutteellisessa tai riskialttiissa toiminnassa.

Tarkastaja raportoi havaitsemiaan puutteita ja tekee korjaus ehdotuksia. Tämän lisäksi on tärkeää, että tarkastaja pyrkii lisäämään organisaation vastuuhenkilöiden, linjajohdon ja työntekijöiden ammattitaitoa siten että tarpeelliset kontrollit kuvataan ja toteutetaan jo järjestelmiä rakennettaessa tai toimintoja organisoitaessa. Tällöin tarkastettavat ymmärtävät ja hyväksyvät kontrollien merkityksen ja tärkeyden sekä korjaavat mahdollisia, itse havaitsemiaan kontrollipuutteita oma-aloitteisesti.

Organisaation kontrolleja koskevan ammattitaidon lisääminen eli asioihin vaikuttaminen etukäteen vaatii tarkastajalta myyntitaitoa ja uskottavuutta.

TIETOJÄRJESTELMÄ-TARKASTUKSEN ARVOSTUS

Varsinkin sisäisellä tietojärjestelmätarkastuksella on haasteena tulla miellettyksi ja hyväksytyksi osaksi johdon valvontatointia ja toisaalta aidoksi yhteistyökumppaniksi muun organisaation kanssa. Valitettavan usein tarkastus koetaan välttämättömäksi pahaksi, joka etsii virheitä ja raportoi ne yrityksen johdolle. Tämän käsityksen pystyy muuttamaan vain tarkastus itse tekemällä työtään niin hyvin, että sen merkitys ymmärretään. Tietojärjestelmätarkastajan on ymmärrettävä tietotekniikkaa niin paljon, että hän pystyy asettamaan reaalimaailman teoreettisen kirjaviisauden tilalle. Riippumattomuus säilyttäen on käytettävä niitä työ menetelmiä, jotka johtavat tuloksiin.

*Esko Nuutila , CISA,
Tarkastuspäällikkö, PSP
Puheenjohtaja, Tietojärjestelmien
tarkastus ja valvonta ry,
esko.nuutila@psp.fi*

KEVÄTKOKOUSKUTSU 98

Sytyke ry:n sääntömääräinen kevätkokous pidetään

Perjantaina 27.3. klo 17 alkaen

Helsingin liikelouden ammattikorkeakoulussa (HELIA),

ATK-instituutti, Rautatieläisenkatu 5, Itä-Pasilassa.

Asialistalla normaalit sääntömääräiset asiat kuten vuoden 1997 toimintakertomus, tilinpäätös ja vastuuvapaudet vuoden 1997 toimihenkilöille.