Turun kaupunki

26.1.2012

Raportti tarkastuslautakunnalle

pwc

Tarkastuslautakunta
Turun kaupunki

Olemme suorittaneet Turun kaupungin tarkastusta ennalta laaditun tarkastusohjelman mukaisesti. Tarkastus kohdistui pääosin palkanlaskentaan ja palkkatoiminnon sisäisten kontrollien läpikäyntiin. Lisäksi on käyty läpi SAP-järjestelmän kontrolleja.

Raportissa esitämme merkittävimmät havainnot tarkastuksestamme.

Turussa 26.1.2012

PwC Julkistarkastus Oy
JHTT-yhteisö

Irma Kivilähde
JHTT

PwC Julkistarkastus Oy, JHTT-yhteisö, PL 1015 (Itämerentori 2), 00101 HELSINKI
Puh. 09 22 800, Faksi 09 174 102, www.pwc.com/fi

Yhteenveto tarkastushavainnoista

Palkkatoiminto	**1.1 Vaaralliset työyhdistelmät**	**1.2 Lokitiedot perustieto-muutoksista**	**1.3 Kontrollien dokumentointi**	**1.4 Maksu-tapahtuman hyväksyminen**
SAP-järjestelmän kontrollit	**2.1 Käyttövaltuuk-sien testaus ja vaaralliset työyhdistelmät**	**2.2 SAP-järjestelmän turvallisuus**	**2.3 SAP-järjestelmän varmuus-kopiointi ja palauttaminen**	**2.4 SAP-järjestelmän muutoshallinta**
	2.5 Käyttö-valtuuksien hallinta			

1.1 Vaaralliset työyhdistelmät

Tarkastushavainnot ja suositukset

Palkanlaskentaohjelmiston käyttöoikeudet oikeuttavat myös muutosten tekemiseen perustietorekisterissä. Täten palkanlaskentatehtäviä hoitavien henkilöiden on mahdollista perustaa uusia henkilöitä ja muuttaa perustietoja.

Sisäisen kontrollin kannalta paras vaihtoehto olisi se, että uusien henkilöiden perustaminen ja pankkitilin muuttaminen olisi rajattu mahdollisimman harvoille henkilöille, joilla ei ole muita palkkatoimintaan liittyviä tehtäviä.

Johdon kommentit

Palvelupäällikkö Sirpa Virtanen:
Organisaatiosuunnitelmassa myös palkanlaskentaan tulee oma asiakaspalveluyksikkö. Kyseiselle yksikölle tultaneen siirtämään henkilöiden perustaminen ja perustietojen ylläpito

1.2 Lokitiedot perustietomuutoksista

Tarkastushavainnot ja suositukset

Personec-järjestelmästä ei saa ajettua lokilistaa perustietojen muutoksista. Esimerkiksi pankkitilien muutokset ja uuden henkilön perustamiset on mahdollista läpikäydä vain henkilöittäin.

Mielestämme näistä muutoksista tulisi olla ajettavissa listaus, josta ilmenee muutettu/uusi tieto sekä tallentaja. Kyseinen lokitiedosto tulee ajaa säännöllisesti ja hyväksyttää asianmukaisesti.

Johdon kommentit

Palvelupäällikkö Sirpa Virtanen: Järjestelmän toimittajalle on kerrottu 11.10.11 pidetyssä Turun kaupungin ja järjestelmän toimittajan välisessä laatupalaverissa ko. listauksen puutteesta, josta tilintarkastajat ovat jo aiemminkin huomauttaneet.
Selkeää lupausta listauksen toimittamisesta emme saaneet. Otan yhteyttä järjestelmän toimittajaan ja pyydän päivämäärää, johon mennessä suunnitelma listauksen synnystä on valmiina

1.3 Kontrollien dokumentointi

Tarkastushavainnot ja suositukset

Talouspalvelukeskuksessa ajetaan palkka-ajojen yhteydessä virhe- ja seurantalistoja, esimerkiksi kaikista yli neljän tuhannen euron nettopalkoista.

Virhelistojen läpikäynnille ei ole dokumentointivaatimuksia. Kun virheet on selvitetty ja aineisto tarkastettu, kyseiset listaukset hävitetään. Siten kontrollitoimenpiteiden suorittamista ei voida jälkikäteen varmistaa.

Johdon kommentit

Palvelupäällikkö Sirpa Virtanen:
Palkanlaskennan tiimejä ohjeistetaan tulostamaan listaukset ja merkitsemään virheilmoituksen aiheuttamat toimenpiteet. Listaukset arkistoidaan 2 vuotta (tilitarkastusväli 4 vuotta)

1.4 Maksutapahtuman hyväksyminen

Tarkastushavainnot ja suositukset

Talouspalvelukeskuksen suorittaman palkanlaskentatyön jälkeen lähetetään palkkojen maksuaineiston tiedot hallintokuntaan hyväksyttäväksi. Hyväksyntä tehdään kuitenkin vain yhteissummatasolla, joten henkilöittäistä palkka-aineistoa ei hyväksytä palkanlaskijan tekemän työn jälkeen.

Mielestämme tulisi selvittää mahdollisuus henkilöittäisten palkkatietojen hyväksyttämiseen esimiehillä.

Johdon kommentit

Palvelupäällikkö Sirpa Virtanen:
Henkilöittäinen hyväksyttäminen on ollut työn alla jo pitkään. Ongelmana ovat suuret hallintokunnat, joiden massat ovat suuria ja henkilöstö vaihtuvaa. Riittävän alhaisen esimiestason listaukset ja niiden käsittely ei tällä hetkellä onnistu sähköisesti. Manuaalinen jako taas vie kohtuuttomasti aikaa, listauksien ollessa useiden tulostelaatikoiden kokoisia.

2.1 Käyttövaltuuksien testaus ja vaaralliset työyhdistelmät

Tarkastushavainnot ja suositukset

Tarkastuksessa selvitettiin käyttövaltuuksien periaatteita haastatteluin sekä tekemällä joitakin pistokokeita. Tarkastuksessa tehtiin seuraavat havainnot:

• SAP-järjestelmässä olevien käyttövaltuuksien asianmukaisuutta ei tällä hetkellä varmenneta. Tarkastuksessa havaittiin kaupungin palveluksesta poistuneen mutta uudestaan ulkoisena käyttäjänä järjestelmään luodulla henkilöllä vanhat kaupungin aikaiset valtuudet järjestelmässä.
• Sisäisten tarkastajien roolissa on kiinnitettynä tapahtumia, joiden avulla voidaan luoda tai muuttaa tapahtumia järjestelmään (mm. toimittaja- ja asiakasperustietojen luonti, maksatus, laskujen käsittely, ostotilauksen luonti).
• Ulkoisten konsulttien rooliin on kiinnitetty tapahtumia joilla voidaan luoda tai muuttaa liiketapahtumia järjestelmässä.
• Vaarallisia työyhdistelmiä ei ole systemaattisesti määritelty ja dokumentoitu. Vaarallisten työyhdistelmien määrittely aloitettiin osana käyttöönotto projektia mutta ei ole tehty loppuun asti.

Mielestämme käyttövaltuuksien asianmukaisuus tulee varmentaa järjestelmästä kattavasti.
Lisäksi suosittelemme määrittämään vaaralliset työyhdistelmät ja varmentumaan, ettei näitä ole järjestelmän käyttäjillä.

Johdon kommentit

• Asianmukaisuus varmennetaan, tavoitteena tehdä 2 kk välein, seuraavaksi helmikuussa (Valtonen). Poistuneen/uudelleen luodun henkilön tapaus on hoidettu.
• Sisäisten tarkastajien rooli: esim. FD01 näkyy käyttäjätunnuksella, mutta tapahtumaan ei silti ole oikeutta. Tarkempi ratkaisukuvaus roolista löytyy Solution Managerista Käyttäjähallinnan ratkaisukuvaus, liite 5.
• Ulkoisten konsulttien rooli: tällä hetkellä luonti- ja muutosoikeuksia on, tarvitaan ongelmatilanteiden selvittelyyn. Jatkossa on mahdollista rajata tarkemmin, mutta saattaa hidastaa ongelmatilanteiden selvittelyä, jos oikeudet ovat liian rajatut. Kuvaus konsulttirooleista olemassa Solution Managerissa Käyttäjähallinnan ratkaisukuvauksessa. Testataan ja läpikäydään konsulttitunnusten oikeudet. (Valtonen, Fujitsu)
• Vaaralliset työyhdistelmät tulisi käydä huolellisesti läpi Tapaken kanssa ja tarkistaa tilanne, koska henkilöiden tehtävät ja roolit ovat vaihtuneet. Selvitystyötä aloitetaan helmikuun lopulla (Valtonen, Helenius).

2.2 SAP-järjestelmän turvallisuus

Tarkastushavainnot ja suositukset

SAP-järjestelmän turvallisuutta testattiin pistokokein tarkastuksen aikana. Kattavaa SAP Basis turvallisuuden tarkastusta ei ole suoritettu.

Käyttäjäprofiilit
• SAP_ALL profiili on kiinnitetty pääosin teknisille tunnuksille. Lisäksi annettu 3 konsultille, joista saadun tiedon mukaan yhdellä ei ole tarvetta järjestelmään pääsyyn.
• SAP_NEW profiili on kiinnitetty pääosin teknisille tunnuksille. Lisäksi annettu 2 konsultille, joista saadun tiedon mukaan toisella ei ole tarvetta järjestelmään pääsyyn.

Salasanat
• Ratkaisukuvauksessa on määritetty salasanan minimipituudeksi 8 merkkiä, nykyasetuksilla vaaditaan 6 merkkiä pitkä salasana.
• Järjestelmää ei ole asetettu vaatimaan salasanan vaihtoa säännöllisesti. Ratkaisukuvauksessa määritetty voimassaoloaika 90 päivää.
• Salasanan kryptisyys asetuksia ei ole määritetty ratkaisukuvauksen määritysten mukaisesti.

Suosittelemme poistamaan SAP_ALL ja SAP_NEW profiilit ylimääräiseltä henkilöltä. Suosittelemme varmistamaan, että ratkaisukuvauksesta poikkeavat salasana-asetukset ovat tahtotilan mukaisia.

Johdon kommentit

ALL ja NEW profiilit: pitäisi olla tieto kenestä kysymys, jotta tunnus voidaan poistaa.

Ratkaisukuvaukseen on kirjattu tavoitteen mukainen taso, jota tavoitellaan myös verkon salasanan osalta. Nyt käytössä oleva taso vastaa verkon salasanan nykytasoa.

SAP:n salasanalla on käytännön merkitystä vain AMK:n ja tervin verkoissa, joissa suorakirjautuminen ei toimi. Muilla käytännön turvallisuustason määrittää verkon salasana.

2.3 SAP-järjestelmän varmuuskopiointi ja palauttaminen

Tarkastushavainnot ja suositukset

SAP-järjestelmän varmuuskopiointi ja palautusmenettelyissä ei havaittu olennaisia puutteita. Koko järjestelmän palauttamista on harjoiteltu ja siinä on onnistuttu kohtuullisessa ajassa. Kuitenkaan toipumissuunnitelmaa ja varmennusmenettelyitä ei ole kuvattu kirjallisesti.

Saadun tiedon mukaan varmennusnauhat viedään kerran kuukaudessa etäsäilytykseen.

Suosittelemme laatimaan onnettomuustilanteiden varalle toipumissuunnitelman ja varmentumaan suunnitelman toimivuudesta. Lisäksi suosittelemme dokumentoimaan käytössä olevat varmennusmenettelyt.

Konehuoneen onnettomuustilanteen varalta suosittelemme varmuusnauhojen etäsäilöön vientiä tiheämmin kuin kerran kuukaudessa.

Johdon kommentit

Asian selvittely on työn alla.

2.4 SAP järjestelmän muutoshallinta

Tarkastushavainnot ja suositukset

SAP-järjestelmän muutoshallinnan prosessi on kuvattuna kontrollipisteineen. Muutoshallinnan prosessia testattiin pistokokein tarkastuksen aikana ja testauksessa ei havaittu olennaisia puutteita.

Muutospyyntöjen ja tuotantoon vientien kirjausketjua varmennetaan lisäämällä muutospyynnön numero SAP tuotantoon vientiin (TA-numerointi). Suosittelemme kehittämään kirjausketjua lisäämällä myös teknisen implementointinumeron (request numero) muutospyyntöön.

Johdon kommentit

-

2.5 Käyttövaltuuksien hallinta

Tarkastushavainnot ja suositukset

Menettely SAP-järjestelmän käyttövaltuuksien anomiseen ja hyväksymiseen on pääosin asianmukainen. Uuden käyttäjän luomiseksi vaaditaan esimiehen hyväksyntä. Käyttövaltuushallinnan prosessi on kuvattu, mutta käytännön menettelyssä miten käyttövaltuuksia anotaan on eroavaisuuksia Tapake ja Haloke käyttäjien osalta. Testasimme järjestelmään luotujen käyttäjien asianmukaisuutta pistokokein emmekä havainneet olennaisia puutteita.

Saadun tiedon mukaan Turun SAP-järjestelmän käyttäjien asianmukaisuus varmennetaan nykyisellä käytännöllä 2-3 kertaa vuodessa.

Suosittelemme käyttövaltuuksien hallinnan menettelyn yhtenäistämistä kaikkien SAP ammattikäyttäjien osalta ja luomaan yhtenäisen dokumentointitavan käyttövaltuuksien anomiseen ja hyväksymiseen.

Johdon kommentit

-

Havaintojen luokittelu

Raportissa esittämämme havainnot on jaoteltu subjektiivisesti ja karkeasti kolmeen luokkaan niiden merkittävyyden perusteella. Luokat on eroteltu väreillä ja alla olevat määritelmät on tehty selventämään jaottelua. Luokittelu viittaa ensisijaisesti havainnon merkittävyyteen johdon kannalta. Punaiseksi luokiteltu havainto ei kuitenkaan aina tarkoita sitä, että tarkastuksen ja johdon näkemykset eroavat toisistaan tai että kysymys on sisäisen kontrollin puutteesta.

Punaiset havainnot vaikuttavat tai saattavat vaikuttaa olennaisesti ulkoiseen raportointiin. Ne voivat myös ilmentää merkittävää sisäisen kontrollin puutetta. Johdon tulisi kiinnittää huomiota näihin havaintoihin. Punainen saattaa lisäksi ilmentää asiaa, jolla ei ole merkittävää vaikutusta ulkoiseen raportointiin tai kontrollien puutteeseen, mutta joka johdon tulisi huomioida havainnon luonteen vuoksi (säännönmukainen poikkeaminen kirjanpidon laadinta- tai muista periaatteista, viitteet väärinkäytöksistä, tms.).

Keltaiset havainnot eivät täytä punaisen havainnon kriteereitä, mutta saattavat silti vaikuttaa ulkoiseen raportointiin tavalla, mikä mielestämme tulisi saattaa johdolle tiedoksi. Keltainen saattaa myös ilmentää huomioita sisäisistä kontrolleista. Tällöin kyse ei ole merkittävistä puutteista sisäisissä kontrolleissa vaan vähäisemmistä johdon tietoon tuotavista havainnoista.

Vihreitä ovat havainnot, jotka ennen ovat olleet punaisia tai keltaisia, mutta jotka on ratkaistu edellisen raportoinnin yhteydessä tai jälkeen. Vihreä kuvastaa lähinnä aikaisempien havaintojen kehitystä ja vihreät havainnot poistetaan listalta sen jälkeen, kun asioiden on todettu olevan kunnossa. Vihreät havainnot voivat olla lisäksi suuruusluokaltaan tai muuten merkittävyydeltään niin olennaisia, että ne halutaan tuoda johdolle tiedoksi.