TURUN KAUPPAKORKEAKOULU
Turku School of Economics

**TIIVISTELMÄ**

[X] Pro gradu -tutkielma
[ ] Lisensiaatintutkielma
[ ] Väitöskirja

| | | | |
|---|---|---|---|
| Oppiaine | Tietojärjestelmätiede | Päivämäärä | 7.3.2008 |
| Tekijä(t) | KTK Jani Leino | Matrikkelinumero | |
| | | Sivumäärä | 90 |
| Otsikko | Sarbanes-Oxley -lain vaikutus yrityksen tietoturvaan – Keskeiset tietoturvauhat ja niiltä suojautuminen Sarbanes-Oxley -lakiin sopeuduttaessa | | |
| Ohjaaja(t) | KTT Hannu Salmela | | |


Tiivistelmä

Sarbanes-Oxley -laki säädettiin palauttamaan sijoittajien luottamus Yhdysvaltain arvopaperimarkkinoihin 2000 -luvun alun kirjanpitoskandaalien jälkeen. Lain pykälä 404 vaatii U.S. Securities and Exchange Commissionissa (SEC) rekisteröityjen julkisten yhtiöiden ja niiden tilintarkastajien vuosittain tarkastavan yhtiön tilinpäätöksen, sisäiset kontrollit ja kontrollien toimivuuden. Tietojärjestelmät ovat erottamaton osa talousraportointiprosessia. Ne ovat osana kirjapitotapahtumien alulle panoa, hyväksyntää, tallennusta, käsittelyä ja raportointia. Näin ollen talousraportointiin vaikuttavat tietojärjestelmät on otettava mukaan yrityksen sisäisen kontrolliympäristön tarkastukseen. Sarbanes-Oxley -lain alaisen yrityksen tietohallinnon on pystyttävä todistamaan tiedon oikeellisuus ja tietojärjestelmien asianmukainen hallinta sekä pystyttävä selkeästi osoittamaan, että tietoon pääsyä ja muuttamista kontrolloidaan.

Tämän tutkielman tavoitteena on muodostaa käsitys, mikä vaikutus Sarbanes-Oxley -lailla on lain piirissä olevan yrityksen tietoturvaan. Kysymystä lähestytään tutkielmassa keskeisiksi tunnistettujen tietoturvauhkien kautta avustavalla kysymyksellä: Miten tietohallinnon Sarbanes-Oxley -kontrolliympäristö vastaa kirjallisuudessa esitettyjä tietoturvauhkien vastakeinoja? Tyyliltään tämä tutkielma on kvalitatiivinen case-tutkimus. Tutkielman teoriaosuus on muodostettu dokumenttianalyysin keinoin. Teoreettisena viitekehyksenä tutkielmassa toimii tietoturva. Lista keskeisistä tietoturvauhista on muodostettu valittujen auktoriteettien esittämistä malleista vertailemalla ja samankaltaisuuksia etsien. Kutakin keskeistä tietoturvauhkaa kohden on kirjallisuudesta etsitty keinot uhan torjumiseksi tai sen haittojen vähentämiseksi. Tutkielman toisen teoreettisen viitekehyksen eli IT Governance Instituten (ITGI) muodostaman ohjeellisen Sarbanes-Oxley -kontrolliympäristön kontrollien kattavuutta verrataan kirjallisuudesta löytyneisiin tietoturvauhkien vastakeinoihin. Tutkielman empiriaosassa on case- eli tapaustutkimuksen keinoin verrattu case-yrityksen Sarbanes-Oxley -kontrolliympäristön kontrollien kattavuutta edellä mainittuihin teoreettisiin viitekehyksiin.

Tutkielmassa havaittiin teoreettisen ja käytännön Sarbanes-Oxley -kontrolliympäristön kontrollien vastaavan lähes täydellisesti kirjallisuudessa mainittuja tietoturvauhkien vastakeinoja. Samalla havaittiin, että jo muutaman Sarbanes-Oxley -kontrolliympäristön avainkontrollin avulla voidaan saavuttaa perustason suoja kaikilta keskeisiltä tietoturvauhilta. Sarbanes-Oxley -lain myötä käyttöönotettu kontrolliympäristö myös formalisoi tietoturvauhkien vastakeinojen täytäntöönpanon ja seurannan. Näin ollen Sarbanes-Oxley -kontrolliympäristön käyttöönoton nähdään parantavan yrityksen tietoturvaa ja olevan merkittävä askel kohti hyvää tietohallintotapaa.



| | |
|---|---|
| Asiasanat | kontrolli, riskienhallinta, Sarbanes-Oxley, standardit, tietoturva, uhat |
| Muita tietoja | |