Tekoälyriskien hallintaa sisäisen valvonnan menetelmin

29.12.2025

Tämän syksyn aikana harvassa ovat olleet ne päivät, jolloin me opettajat emme olisi keskustelleet tekoälyn kielletyistä käyttötavoista korkeakoulussamme, esimerkiksi tekoälyn käytöstä vastoin annettua ohjeistusta kurssisuorituksen laatimisessa. Tekoälyn vääränlainen käyttö onkin noussut ongelmaksi kautta korkeakoulukentän, ja korkeakoulut ovat joutuneet pohtimaan erilaisia keinoja vääränlaisen käytön estämiseksi ja toisaalta myös vääränlaisesta käytöstä rankaisemiseksi (esimerkiksi Villa, 2025). Kuinka suuresta ongelmasta on kysymys? Tätä kysyin ChatGPT:ltä (OpenAI, 2025) ja tällaisen vastauksen sain: **Yhteenveto**

- Tekoälyä käyttää suurin osa opiskelijoista, mutta vain osa käyttää sitä väärin.
- Noin 40–55 % opiskelijoista saattaa käyttää tekoälyä tavoilla, jotka rikkovat sääntöjä tai eettisiä ohjeita.
- Viralliset huijaustapaukset ovat merkittävästi lisääntyneet viime vuosina, mutta todellinen luku on todennäköisesti suurempi kuin mitä tilastot näyttävät.

Tarkensin kysymykseni koskemaan ainoastaan Suomen tilannetta, joka ChatGPT:n (OpenAI, 2025) mukaan näyttikin valoisammalta kuin ensin mainittu maailmanlaajuinen tilanne: **Loppupäätelmä** Suomessa korkeakouluissa:

- tekoälyn käyttö on yleistä, mutta ei automaattisesti väärinkäyttöä,
- todetut huijaustapaukset tekoälyn avulla ovat vielä harvinaisempia kuin muualla maailmassa ja
- yliopistot panostavat enemmän ohjeistukseen ja opetusmenetelmien kehittämiseen kuin rangaistuksiin.

Uutisoidut tapaukset (esimerkiksi Villa, 2025) vahvistavat ChatGPT:n löytämiä mainintoja suomalaisissa korkeakouluissa tapahtuneesta tekoälyn väärinkäytöstä.

Sisäinen valvonta ratkaisemaan tekoälyväärinkäytöksiä

Tekoälyyn liittyvää väärinkäyttöongelmaa voi lähestyä sisäiseen valvontaan liittyvänä ilmiönä petosten estämisen näkökulmasta. Sisäiset tarkastajat ry (2025) määrittelee sisäisen valvonnan seuraavasti: Sisäinen valvonta voidaan kuvata prosessina, jonka avulla pyritään varmistumaan organisaation tavoitteiden saavuttamisesta. Tavoitteet liittyvät organisaation strategisiin, toiminnallisiin, raportointia koskeviin ja vaatimuksenmukaisuuteen liittyviin tavoitteisiin (Sisäiset tarkastajat ry, 2025). Sisäinen valvonta muodostuu niistä tehtävistä ja toimista, jotka varmistavat näihin tavoitteisiin pääsemisen hallitsemalla ja lieventämällä näiden tavoitteisiin pääsemiseen liittyviä riskejä sekä tukemalla organisaation päätöksentekoa ja hallintoa (COSO, 2013). Sisäinen valvonta ei kuitenkaan ole pelkästään toimintatapoja ja linjauksia, vaan kyse on myös organisaation jokaisella tasolla toimivista ihmisistä ja niistä jokapäiväisistä toimista, joilla he vaikuttavat sisäiseen valvontaan. Vaikka sisäinen valvonta esimerkiksi osakeyhtiössä jo osakeyhtiölainkin perusteella on yhtiön hallituksen vastuulla (Osakeyhtiölaki 624/2006), sisäinen valvonta ei siis ole pelkästään organisaation ylimmän johdon tai hallinnon asia. Sisäinen valvonta on koko organisaation yhdessä tekemiä toimia edellä mainittujen tavoitteiden saavuttamiseksi.

COSO-viitekehys rakentamaan sisäistä valvontaa

Usein käytetty viitekehys sisäisessä valvonnassa on ns. COSO-kuutio (COSO, 2013), joka yhdistää organisaation niin toiminnalliset kuin raportoinnin ja sääntöjen noudattamisenkin tavoitteet sisäisen valvonnan viiteen osa-alueeseen, joita ovat valvontaympäristö, riskien arviointi, valvontatoimenpiteet, tieto ja viestintä sekä seurantatoimenpiteet. COSO-viitekehystä voidaan hyödyntää myös petosten estämisessä. COSO-viitekehyksen periaatteiden pohjalta on laadittu viiden periaatteen ohjeistus petoriskien hallitsemiseksi (Fraud Risk Management Guide) (COSO, 2016). Nämä viisi periaatetta ovat seuraavat:

1. Petosten torjuntaohjelman perustaminen, jolla perustamisella osoitetaan hallituksen ja ylimmän johdon odotukset ja sitoutuminen rehellisyyteen ja eettisiin arvoihin (COSO, 2016). Erityyppisiin petoksiin liittyvän riskin hallinta on olennainen osa organisaation sisäisen valvonnan valvontaympäristöä ja organisaation hyvää hallintotapaa (COSO, 2016). Hyvällä hallintotavalla pyritään varmistamaan omistajien tavoitteiden ja oikeuksien toteutuminen organisaatiossa (kts. myös Kankaanpää, 2020).
2. Petosriskin, sen todennäköisyyden ja merkityksen arviointi sekä mahdollisten petostapojen tunnistaminen (COSO, 2016). Riskien arviointi tekoälyn väärinkäytösriskin kohdalla liittyisi laittomien toimien eli tekoälyn kielletyn käytön tunnistamiseen sekä sen pohtiminen, mikä merkitys tällä väärinkäytösriskillä on toteutuessaan.
3. Ennalta ehkäisevien ja jälkikäteen toteutettavien valvontatoimien valitseminen, kehittäminen ja käyttöönotto (COSO, 2016). Näillä toimilla pyritään lieventämään riskiä siitä, että petoksia tapahtuu tai että niitä ei havaita ajoissa. Ohjeistuksessa myös painotetaan sitä, että organisaatiossa on myös varmistettava, että suunnitellut valvontatoimenpiteet myös toteutetaan organisaation eri tasoilla ja että eri valvontatoimenpiteille on määritelty vastuuhenkilöt.
4. Viestintäprosessin suunnittelu sen varmistamiseksi, että tieto mahdollisista petoksista tulee organisaation tietoon (COSO, 2016). Samalla varmistetaan, että koko organisaatiossa käytetään yhtenäisiä menettelytapoja niin petosten tutkintaan kuin korjaaviin toimiinkin ja että petoksiin puututaan asianmukaisesti ja oikea-aikaisesti. Ohjeistuksen mukaan on huomioitava, että hyvätkään valvontatoimenpiteet eivät voi estää kaikkia petostapauksia, minkä vuoksi onkin tärkeää analysoida kaikki esiin tulleet petostapaukset valvontatoimenpiteiden parantamiseksi.

5. Jatkuva arviointi sen varmistamiseksi, että jokainen näistä petosten riskinhallinnan periaatteesta on toiminnassa (COSO, 2016). Mahdollisista puutteista olemassa olevissa toimissa ja puutteiden korjaamiseksi tarvittavista toimenpiteistä tulee viestiä oikea-aikaisesti sisäisestä valvonnasta vastaaville tahoille, mukaan lukien ylin johto ja hallitus. Nämä ohjeistuksessa mainitut jatkuvat arvioinnit voivat olla joko osa organisaation säännöllisiä liiketoimintaprosesseja tai erillisiä, ennalta laaditun suunnitelman mukaisesti toteutettavia arviointeja.

Hyvä on myös huomioida, että mikäli riski tekoälyllä tehtyyn väärinkäytökseen toteutuu, voi tällä olla vaikutuksia myös muihin osa-alueisiin organisaation toiminnassa. Väärinkäytösriski toteutuessaan voisi aiheuttaa organisaation raportointiin liittyvän riskin realisoitumisen eli riskiin siitä, että organisaation raportointi, niin taloudellinen että ei-taloudellinenkin raportointi, ei vastaakaan todellisia olosuhteita (kts. COSO, 2013). Seurauksia voisi olla myös organisaation maineelle (COSO, 2016).

Lopuksi

Tekoälyn käyttöön liittyvät riskit ovat tulleet hyvin nopeasti osaksi korkeakoulujen ja myös muiden oppilaitosten riskikenttää, mikä niiden täytyy huomioida omaa toimintaansa suunnitellessaan, jotta tekoälyn vääränlaiseen käyttöön liittyvät riskit mahdollisine negatiivisine seurauksineen eivät realisoidu. Tekoälykenttä on jatkuvassa, nopeassa muutoksessa, mikä tarkoittaa organisaatioissa jatkuvaa riskien seuraamista sekä niihin vastaamisen päivittämistä. Tässä esitelty COSO Fraud Risk Management Guide ja sen perustana oleva COSO-viitekehys yhdessä antavat organisaatioille suuntaviivoja siitä, kuinka ne voivat sekä ennakoida ja analysoida mahdollisia riskejään että suunnitella ja ottaa käyttöön toimenpiteitä, joiden avulla näitä riskejä pyritään hallitsemaan. Tekoälyn kohdalla on huomioitava kuitenkin, että riskiä eivät muodosta pelkästään tekoälyn käyttöön liittyvät väärinkäytökset ja niiden torjuminen, vaan myös se, kuinka hyvin opiskelijat saavat hankittua työelämässä tarvitsemansa tekoälyosaamisen. Esimerkiksi omassa korkeakoulussamme, Seinäjoen Ammattikorkeakoulussa, tekoälyosaaminen on yksi neljästä strategisesta tavoitteesta (Seinäjoen Ammattikorkeakoulu, i.a.), ja riskienhallintaa on myös sen varmistaminen, että osaamme ohjata opiskelijoita oikeanlaiseen tekoälyn käyttöön, jotta heillä on valmiudet tekoälyn oikeanlaiseen käyttöön niin opiskelussaan (sallituilla tavoilla) kuin sitten aikanaan työelämässäkin. Tekoälyn käyttöä ei siis voi yksiselitteisesti kieltää väärinkäytösten estämiseksi, vaan opiskelijoita tulee ohjata tekoälyn oikeanlaiseen, heidän työelämävalmiuksiaan parantavaan eettiseen käyttöön. Yhtä kaikki, sisäistä valvontaa on eettisyyskin: eettisyys on sisäisen valvonnan osa-alue, joka lähtee organisaation valvontaympäristöstä ja organisaation johdosta (COSO, 2013).

Tuulia Potka-Soininen
KTT, KLTYliopettaja
Tuulia Potka-Soininen on laskentatoimen yliopettaja, jolla on pitkä käytännön kokemus laskentatoimesta, yritysten raportoinnista sekä sisäisestä valvonnasta ja riskienhallinnasta, jotka aihealueet ovat tuttuja esimerkiksi hänen aiemmalta uraltaan tilintarkastajana.

Lähteet

COSO. (2013). *Internal Control — Integrated Framework. Executive summary.* https://www.coso.org/_files/ugd/3059fc_1df7d5dd38074006bce8fdf621a942cf.pdf COSO. (9 2016). Fraud risk management guide. Executive

summary. https://www.coso.org/_files/ugd/3059fc_02c01fde6552479196535bcfee8ea60e.pdf Kankaanpää, J. (5. 6 2020). *Omistajaohjaus, hyvä hallintotapa ja muu valvonta. Tutkimus suomalaisista osakeyhtiöistä.* Tampereen yliopiston väitöskirjat 260. [väitöskirja, Tampereen yliopisto] https://trepo.tuni.fi/bitstream/handle/10024/121896/978-952-03-1578-8.pdf?sequence=2&isAllowed=y OpenAI . (2025). ChatGPT. Osakeyhtiölaki 624/2006. (2006). https://www.finlex.fi/fi/lainsaadanto/2006/624 Seinäjoen Ammattikorkeakoulu. (i.a.). *Meidän ammattikorkeakoulu – inhimillisyyttä, laatua ja tuloksellisuutta. SEAMK strategia 2024-2028.* https://storage.googleapis.com/seamk-production/2024/09/b53c8c2d-seamk-strategia-2025-2028.pdf Sisäiset tarkastajat ry. (22. 12 2025). *Sisäinen valvonta, riskienhallinta ja organisaatiokulttuuri*. https://theiia.fi/sisainen-tarkastus/sisainen-valvonta-ja-riskien-hallinta-2/ Villa, M. (7. 11 2025). Yliopistot ovat uuden haasteen edessä – Kovat keinot käyttöön. https://www.iltalehti.fi/digiuutiset/a/a02ffae9-f89b-4153-9f29-f1db21248c72