

# KATAKRI kehittyä. Miten se on muuttunut?

## Kansallinen turvallisuusauditointikriteeristö (KATAKRI) on saanut ensimmäisen päivityksensä. Mitä siihen sisältyy? Entä miten kriteeristön ajatellaan kehittyvän jatkossa?

Vuoden 2009 aikana mittavalla henkilötöyöpanoksella aikaansaatu, security-turvallisuuden vaatimuksia omalta osaltaan linjaava auditointikriteeristö on kokenut ensimmäisen uudistuksensa. Päivityskierros toteutettiin sisäministeriön johdolla ja edelleen osana hallituksen sisäisen turvallisuuden ohjelmaa. Kriteeristön ensimmäinen versio laadittiin aikanaan viranomaisjohtoisesti, mutta tiiviissä yhteistyössä yritysten, järjestöjen ja opetuslaitosten kanssa. Päivityskierroksella noudatettiin samaa kaavaa, tosin rajatummalla kokoonpanolla. Päivityksen pääsisällöksi oli etukäteen asetettu ensimmäisestä versiosta löytyneiden epäkohtien korjaaminen. Toiseksi tavoitteeksi oli asetettu safety-osion liittäminen kriteeristöön. Miten näiden osalta kävi?

### Sisällön taustaa

Elinkeinoelämälle annettaviin tiedon turvaamisen suosituksiin ja viranomaisten asettamiin vaatimuksiin ja niiden tarkastamiseen pureutuva KATAKRI jakautuu neljään osioon: hallinnollinen turvallisuus/turvallisuusjohtaminen, henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Kunkin osion sisällön suhteen on esitetty kolmiportainen, valtionhallinnon tietoturvaluustasojen mukainen vaatimusjaottelu:

- perustaso
- korotettu taso
- korkea taso.

Käytettäessä KATAKRIa kansainvälisen turvallisuusluokitellun tiedon suojaamisvaatimusten todentamisen välineenä edellä mainitut tasot vastaavat turvallisuusluokitusmerkintöjä KÄYTTÖ RAJOITETTU (RESTRICTED), LUOTTAMUKSELLINEN (CONFIDENTIAL) ja SALAINEN (SECRET).

### KATAKRI:n käyttötarkoitus

Kansallinen turvallisuusauditointikriteeristö toimii viranomaisten työkaluna silloin, kun näiden on johonkin kansalliseen tai kansainväliseen hankkeeseen liittyen varmistettava yrityksen tai muun yhteisön kyky huolehtia tiedon turvallisuudesta sen mukaisesti, mille turvallisuustasolle kulloinenkin hanke on määritetty.

KATAKRI toimii myös elinkeinoelämän turvallisuustoiminnan eräänä ohjenuorana. Kriteeristöön on koottu oma suositusosionsa, jonka avulla yritys voi kohdistaa vapaaehtoiset turvallisuustoimensa sellaisiksi, että niistä on suoranaista hyötyä siinä tapauksessa, että yritykseltä edellytetään jossakin vaiheessa viranomaisvaatimusten täyttämistä. Nämä otsikon ”elinkeinoelämän suositukset” alla KATAKRI:n toisessa versiossa kulkevat ohjeet on laadittu ”jalat maassa” siten, että turvallisuustoiminnan parantamiseen käytetyt eurot eivät ohjautuisi väärin. Jotkin kriteeristön suosituksista saattavat olla mittavampia kuin perustason viranomaisvaatimukset, mutta tämä ei muodosta silti ristiriitaa; perustasolla ei kaikissa

tapauksissa vaadita kovinkaan paljon, sen sijaan turvallisuustasoaan parantavalle yritykselle on hyvä näissäkin tapauksissa osoittaa oikea suunta kyseisen osa-alueen suosituksilla.

Kolmas käyttötarkoitus kansalliselle turvallisuusauditointikriteeristölle ovat yritysten keskinäiset turvallisuusauditoinnit silloin, kun liiketoiminnan tuoksinassa on syytä varmistua bisneskumppanin kyvystä pitää salassa liikesalaisuudet ja muu ns. sensitiivinen tieto.

### **Hallinnollinen turvallisuus ja turvallisuusjohtaminen**

Turvallisuusauditointikriteeristö sisältää mittavan kontrollityökalun tiedon turvallisen hallinnan ja turvallisuusjohtamisen osalta. Auditointikysymykset ja niihin liittyvät vaatimukset esitetään seuraaville alakokonaisuuksille:

- Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt
- Turvallisuuden vuotuinen toimintaohjelma
- Turvallisuuden tavoitteiden määrittely
- Riskien tunnistus, arviointi ja kontrollit
- Turvallisuusorganisaatio ja vastuut
- Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet
- Turvallisuusdokumentaatio ja sen hallinta
- Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen
- Raportointi ja johdon katselmukset.

Hallinnollisen turvallisuuden osio on kasvanut toisessa julkaisuversiossa yhdellätoista aikaisemmin tietoturvallisuusosioon kuuluneella kysymyksellä ja yhdellä kokonaan uudella, käsittely-ympäristöihin liittyvällä kysymyksellä.

### **Henkilöstöturvallisuus**

Henkilöstöturvallisuudella tarkoitetaan KATAKRI:ssa lähinnä henkilön työyhteisön tietoturvallisuudelle muodostamaa uhkaa, vaikka normaalisti se kattaakin terminä myös henkilöön kohdistuvilta uhkilta suojautumisen. Turvallisuusauditointikriteeristön käsittelymalli pohjautuu pitkälti valtionhallinnon tietoturvallisuuden johtoryhmän vuonna 2008 julkaisemassa henkilöstöprosessikuvauksessa esitettyihin virstanpylväisiin (VAHTI 2/2008). Osion sisältö jakautuu seuraaviin kokonaisuuksiin:

- Tekninen kriteeristö (henkilöstön hallinnointi)
- Riittävän osaamisen varmistaminen
- Henkilön muu soveltuvuus tehtävään
- Rekrytointipäätöksen jälkeiset toimet
- Toimenpiteet työsuhteen solmimisen yhteydessä

- Toimenpiteet työsuhteen aikana.

KATAKRI:n kakkosversiossa henkilöstöturvallisuusosioon on siirretty kaksi aiemmin tietoturvallisuusosioon kuulunutta kysymystä ja poistettu viranomaisten osalta henkilöluottotietojen tarkistusvaatimus.

### **Fyysinen turvallisuus**

Fyysisen turvallisuuden käsite kattaa KATAKRI:ssa sekä toimitilaturvallisuuden, että sitä tukevat muut järjestelyt, kuten vartiointi- ja hälytyspalvelut. Fyysisen turvallisuuden osio on jaettu yksinkertaisesti kolmeen osa-alueeseen:

- Alueen turvallisuus
- Rakenteellinen turvallisuus
- Turvallisuustekniset järjestelmät.

KATAKRI II:n fyysisen turvallisuuden osioon on siirretty viisi aiemmin tietoturvallisuusosioon kuulunutta kysymystä. Ikkunakalvovaatimus on poistettu perustasolta, samoin vaatimus kassakaappien standardinmukaisuudesta. Sen sijaan perustasolle on lisätty äänieristysvaatimus kyseisen tason tiedoista keskusteltaessa.

### **Tietoturvallisuus**

Tietoturvallisuuden osa-alue on muokkautunut KATAKRI:n ensimmäisestä versiosta eniten. Ensimmäisessä versiossa mukana olleet, teknisen tietoturvallisuuden näkökulmasta esitetyt hallinnollisen turvallisuuden, henkilöstöturvallisuuden ja fyysisen turvallisuuden alaan liittyvät vaatimukset on siirretty kaikki edellä mainittujen osioiden sisälle. Näin ollen tietoturvallisuusosioon ovat jääneet seuraavat osa-alueet:

- Tietoliikenneturvallisuus
- Tietojärjestelmäturvallisuus
- Tietoaineistoturvallisuus
- Käyttöturvallisuus.

Tietoturvallisuusosiota päivitettäessä pyrittiin entistä suurempaan yhteensopivuuteen KATAKRI I:n käyttöönoton jälkeen valmistuneisiin ohjaaviin aineistoihin nähden. Tällaisia ovat erityisesti vuonna 2010 voimaan tullut valtionhallinnon tietoturva-asetus sitä täydentävine ohjeineen ja EU:n 2011 käyttöön otettu uusi turvallisuusohjeisto. Tietoturvallisuusosion lähdeviitteistöä on myös laajennettu ja kriteeristön loppuun on koottu oma liitteensä lisäinformaation antamiseksi joidenkin vaatimusten osalta. Kokonaan uusia kysymyksiä on tässä osiossa kolme kappaletta.

### **Safety-osuus**

Päivitystyön ohjausryhmä asetti tavoitteeksi tuoda KATAKRI:n kakkosversioon mukaan myös safety-turvallisuuden alaan kuuluva osio, joka kulki työnimellä ”Omatoiminen varautuminen ja pelastustoiminta”. Työ toteutettiin SPEK:n ansiokkaassa ohjauksessa. Koska pelastusalalla ja erityisesti sen suurilla alueellisilla toimijoilla on kehitteillä kovin läheisesti valmistunutta työtä sivuavia hankkeita, päätti

kansallinen ohjausryhmä ottaa asian tiimoilta aikalisän näiden rinnakkaishankkeiden koordinoimiseksi keskenään. Jatkovalmistelua ohjaa sisäasiainministeriön pelastusosasto.

### **Tulevaisuus**

Kansallisen turvallisuusauditointikriteeristön seuraavaa päivitysvuotta ei ole sovittu. Päivitystarpeita tulevat kuitenkin asettamaan mm. kehittyvä turvallisuusselvityslainsäädäntö sekä fyysisen turvallisuuden osa-alueella menossa oleva käytännön tutkimustyö. Paitsi pelastusturvallisuusosion, myös kuljetusturvallisuusosion mukaan ottamisesta ja valmisteleminen keskustellaan paraikaa. Ajatuksena olisi yhteen sovittaa amerikkalaisperäiset vaatimukset ja EU-vaatimukset suomalaiskansallisiksi vaatimuksiksi, joita sovellettaisiin tarpeen mukaan resurssipooli-idealla.

Onko kaikki, eri turvallisuuden osa-alueisiin pureutuvat vaatimukset syytä sisällyttää samaan KATAKRI:iin, vai olisiko syytä pitää jo syntynyt työ omana kokonaisuutenaan ja laatia samalle formaatille viranomaishyväksynnän saamia liitännäiskriteeristöjä? Ratkaisu tähänkin saataneen alkavana talvena.

### **Kuvan kainaloteksti:**

Artikkelin kirjoittaja, Matti Kesäläinen, on entinen puolustushallinnon apulaisturvallisuusjohtaja, joka vetää nykyisin organisaatio- ja yritysturvallisuuden eri osa-alueisiin keskittyvää KESEC Consulting –yritystä.