xxx ministeriön julkaisusarja 2020:xx

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)

Suositus ja kriteeristö

Lautakunnat

Valtiovarainministeriön julkaisuja - 2022

Valtiovarainministeriö Helsinki 2022

Sisältö

VNK TÄYTTÄÄ, MINISTERIÖN JULKAISUSARJAN NIMI JA JULKAISUN VUOSI : SARJANUMERO.

1 Johdanto

Tämä on tiedonhallintalautakunnan suositus julkisen hallinnon arviointikriteeristöstä, jäljempänä *Julkri,* ja sen käytöstä. Julkri tukee koko julkishallinnon tietoturvallisuuden kehittämisen ja arvioinnin tarpeita. Sitä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä.

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019), jäljempänä *TihL* tai *tiedonhallintalaki*) on säädetty tietoturvallisuustoimenpiteisiin liittyviä vastuita julkisen hallinnon tiedonhallintayksiköille ja viranomaisille sekä yksityisille henkilöille ja yhteisöille taikka muille kuin viranomaisena toimiville julkisoikeudellisille yhteisöille, siltä osin kuin ne hoitavat julkista hallintotehtävää. Jäljempänä näistä tietoturvallisuussäänTelyn kohteista käytetään termiä *organisaatio*. Lisäksi laissa säädetään tietoturvallisuustoimenpiteiden vähimmäistasosta sekä velvoitteesta seurata toimintaympäristönsä tietoturvallisuuden tilaa ja varmistua tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta koko niiden elinkaaren ajan. Organisaation on tunnistettava olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Hankintojen osalta organisaation tulee varmistaa, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Suosituksen laadinnassa on huomioitu Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jäljempänä *TLA tai turvallisuusluokitteluasetus*, laki viranomaisen toiminnan julkisuudesta (621/1999), jäljempänä *julkisuuslaki*, EU:n yleinen tietosuoja-asetus ((EU) 2016/679), jäljempänä *tietosuoja-asetus* ja tietosuojalaki (1050/2018). Lisäksi on huomioitu Tietoturvallisuuden auditointityökalu viranomaisille (Katakri) ja pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) yhdenmukaisuuden varmistamiseksi.

Viranomaisen tietojärjestelmien turvallisuutta voidaan arvioida viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011), jäljempänä *arviointilaki*, mukaisilla arvioinneilla. Lisätietoja arviointi- ja hyväksymisprosessista löytyy ohjeesta ”Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit”.

Organisaatiot voivat käyttää tietosuoja-asetuksen mukaisia tietosuojaa koskevia sertifikaatteja yhtenä keinona sen osoittamiseksi, että rekisterinpitäjälle tai käsittelijälle säädettyjä velvollisuuksia noudatetaan. Yleisen tietosuoja-asetuksen 42 artiklan mukainen sertifiointi ei vähennä rekisterinpitäjän tai henkilötietojen käsittelijän vastuuta tietosuoja-asetuksen noudattamisesta eikä se rajoita tietosuojavaltuutetun toimiston tehtäviä ja valtuuksia. Henkilötietojen käsittelyä koskevasta osoitusvelvollisuudesta on

saatavissa lisätietoja Tietosuojavaltuutetun ohjeesta ”Osoita noudattavasi tietosuoja-säännöksiä”.

Viranomaiselle palveluja tarjoavan luotettavuuden arvioinnissa voidaan hyödyntää turvallisuusselvityslain (726/2014) mukaista yritysturvallisuusselvitystä, joka kohdistetaan Suomesta tuotettuun tai tulevaisuudessa tuotettavaan palveluun ja sen tarjoajaan. Lisätietoa on saatavissa Suojelupoliisin ohjeesta ”Yritysturvallisuusselvitys. Yritysturvallisuusselvitys luotaa yrityksen luotettavuutta ja tietoturvaa”.

Kansainvälisten tietoturvallisuusvelvoitteiden alaisten tietojärjestelmien arvioinnit toteutetaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) mukaisilla menettelyillä. Ulkoasiainministeriö toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa Suomen kansallisena turvallisuusviranomaisena. Lisätietoa on saatavissa Kansallisen turvallisuusviranomaisen ohjeistuksista.

2 Kriteeristö

Tässä suosituksessa ja sen liitteissä kuvataan julkisen hallinnon arviointikriteeristö, *Julkri,* ja suositus sen käyttöön. Suositus sisältää seuraavat liitteet:

- liite 1A Julkri-kriteerit,
- liite 1B Tietosuojakriteerit,
- liite 2 Julkri-työkalu (Excel),
- liite 3 Julkri-työkalun käyttöohje ja
- liite 4 Termistö.

Kriteeristö sisältää luottamuksellisuuden, saatavuuden ja eheyden perusteella eri tasoille luokiteltuja kriteereitä, joista työkalu poimii olennaiset ja valinnaiset kriteerit arvioitavan kohteen turvallisuusvaatimusten ja valitun käyttötapauksen perusteella. Lähtökohtaisesti olennaiset kriteerit tulisi sisällyttää arviointiin. Organisaatio voi riskiarvioinnin sekä tapauskohtaisen harkinnan perusteella sisällyttää arviointiin myös valinnaisia kriteerejä ja päättää, mitkä valinnaiset kriteerit sisällytetään arviointiin.

Kriteeristöä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä. Kriteeristö on suositus ja lainsäädännön vaatimukset voidaan täyttää myös muulla kuin kriteereissä kuvatulla tavalla.

2.1 Tarkoitus ja hyödyt

Kriteeristön käyttö tukee organisaatioita tietoturvallisuuden ja henkilötietojen suojaamisen suunnittelussa, toteuttamisessa ja arvioinnissa. Sitä voi hyödyntää lainmukaisuuden arvioinnissa ja osana tietosuoja-asetuksen mukaista osoitusvelvollisuutta. Organisaatio voi käyttää Julkria esimerkiksi seuraavissa tilanteissa:

- **Palvelun suunnittelussa ja vaatimusmäärittelyssä** ennen hankintaa tavoitteenaan tunnistaa palvelulle asetettavat vaatimukset.

- **Toimittajan arvioinnissa** tavoitteenaan tunnistaa vaatimukset toimittajalle kilpailutuksessa tai osana palvelusopimusta sekä varmistaa vaatimusten toteutuminen toimittajan toiminnassa.

- **Palvelun arvioinnissa** suhteessa hankinnan ja palvelusopimuksen vaatimuksiin.

- **Tietosuojaa koskevien vaatimusten toteutumisen arvioinnissa.**

Kriteeristö tukee organisaation riskilähtöistä turvallisuusjohtamista. Ennalta määritellyt käyttötapaukset helpottavat kriteeristön tilannekohtaista soveltamista. Lisäksi Julkrissa on mahdollista määritellä myös organisaatiokohtaisia käyttötapauksia usein toistuviin arviointitilanteisiin. Käyttötapauksia käsitellään Julkri-työkalun käyttöohjeessa (liite 3).

Kriteeristöä voidaan käyttää salassa pidettävän tiedon, henkilötiedon ja turvallisuusluokitellun tiedon käsittelyn arvioinnissa. Turvallisuusluokka I (TL I – ERITTÄIN SALAINEN) osalta organisaation tulee lisäksi huomioida tapauskohtaiset käsittelyn vaatimukset.

2.2 Rajaukset

Julkrissa on hallinnollisessa ja teknisessä osa-alueessa mainittu saavutettavuus yleisenä kriteerinä. Yksityiskohtaisempia saavutettavuuskriteerejä kriteeristö ei sisällä, joten organisaation tulee huomioida saavutettavuuteen liittyvät vaatimukset erikseen. (Laki digitaalisten palvelujen tarjoamisesta 306/2019).

Julkri ei sisällä kansainvälisen turvallisuusluokitellun tiedon tietoturvallisuuden arviointia (588/2004). Siihen liittyvästä ohjeistuksesta ja arviointikriteeristöstä vastaa ulkoministeriön alainen kansallinen turvallisuusviranomainen NSA.

Valmiuslain (1552/2011) piiriin kuuluvat toiminnan jatkuvuutta poikkeusoloissa koskevat toimenpiteet on rajattu kriteeristön ulkopuolelle. Kriteeristön varautumista koskeva tiedonhallintalakiin perustuva osio (VAR) kuitenkin osaltaan tukee organisaatiota myös poikkeusoloihin varautumista koskevien vaatimusten täyttämisessä.

Julkrissa ei ole huomioitu toimialakohtaisen lainsäädännön, kuten sosiaali- ja terveydenhuollon tai finanssialan vaatimuksia, eikä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018) mukaisia vaatimuksia.

3 Kriteeristön rakenne ja osa-alueet

Kriteerit on ryhmitelty viiteen **osa-alueeseen**. Jokaisella osa-alueella on yksilöivä osa-alueen nimi, johon perustuu myös osa-alueeseen kuuluvien kriteerien tunnisteen alkuosa. Kriteeristön osa-alueet ja niiden lyhenteet ovat:

- hallinnollinen turvallisuus (HAL),
- fyysinen turvallisuus (FYY),
- tekninen turvallisuus (TEK),
- varautuminen ja jatkuvuudenhallinta (VAR).
- tietosuoja (TSU).

Osa-alue koostuu **pääkriteereistä** ja niitä täydentävistä **alikriteereistä**. Kriteerejä on yhteensä yli kaksi sataa. Pääkriteeri – alikriteeri rakennetta on hyödynnetty esimerkiksi sellaisissa tapauksissa, joissa samaan aihealueeseen liittyvät vaatimukset tiukentuvat siirryttäessä korkeammille turvallisuuden tasoille. Esimerkiksi salassa pidettäviä tietoja koskevaa pääkriteeriä voidaan täydentää TL IV luokkaan kuuluvia tietoja koskevan vaatimuksen toteutustapaa tarkentavalla alikriteerillä.

Kukin kriteeri on luokiteltu eri tasoille luottamuksellisuuden, eheyden, saatavuuden ja tietosuojan näkökulmista. Kriteeristä riippuen se voi liittyä yhteen tai useampaan näkökulmaan. Esimerkiksi sama käyttöoikeuksia koskeva kriteeri voi liittyä sekä luottamuksellisuuteen, eheyteen että tietosuojaan.

Kriteeristön eri osa-alueiden yleiskuvaukset on kuvattu seuraavissa luvuissa. Yksittäiset kriteerit ovat liitteissä 1A ja 1B.

3.1 Hallinnollinen turvallisuus

Hallinnollisen turvallisuuden osa-alueessa käsitellään niitä menetelmiä, joilla tietoturvallisuuden hallinta jalkautetaan osaksi koko organisaation toimintaa. Osa-alue kattaa yleisiä hallinnollisen turvallisuuden, henkilöstöturvallisuuden, tietojärjestelmien ja niiden hankinnan sekä käyttöturvallisuuden kriteereitä. Hallinnollisen turvallisuuden kriteereillä pyritään siihen, että organisaatiolla on riittävän hyvin toimiva tietoturvallisuuden hallintajärjestelmä sekä menettelyt sen varmistamiseksi, että tietoja käsittelevä henkilöstö toimii asianmukaisesti.

Monet hallinnollisen turvallisuuden osa-alueen kriteerit toimivat perustana muiden osa-alueiden kriteereille. Esimerkiksi suojattavien kohteiden tunnistamiseen, riskienhallintaan ja dokumentointiin liittyvät kriteerit ovat yleisiä, ja niitä tulee oletusarvoisesti hyödyntää muiden osa-alueiden kriteerien soveltamisen yhteydessä.

Hallinnolliseen turvallisuuteen liittyviä prosesseja tulee käsitellä kokonaisuuksina. Tietoturvallisuuden hallintamenettelyt tulee suhteuttaa riskienarvioinnin perusteella suojattavaan tietoon ja organisaation toimintaan.

Osa-alueen tarkoituksenmukainen käyttö edellyttää arvioinnin kohdentamista siihen osaan organisaatiosta, jolla on vaikutus arvioinnin kohteena olevaan tietojen käsittelyyn. Tarkoituksenmukainen kohdennus voi olla esimerkiksi tietojenkäsittely-ympäristöä hallinnoiva organisaation osa.

Mikäli organisaatiossa käsitellään eri tasoille luokiteltuja tietoja erillisissä ympäristöissä ja prosesseissa, voi olla tarkoituksenmukaista jakaa arviointi erillisiin loogisiin kokonaisuuksiin. Erityisesti henkilöstöturvallisuuden arvioinnissa tulee huomioida, että toteutustapa voi vaihdella kohdekohtaisesti. Esimerkiksi korkeammille tasoille turvallisuusluokiteltujen tietojen käsittely-ympäristön henkilöstön ohjeistuksen sisältö eroaa yleensä merkittävästi koko organisaatiota koskevista yleisistä ohjeistuksista.

Organisaation tulee varmistaa, että tietojen käsittelyä koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta.

Hyvään riskienhallintaan kuuluu menettelytapojen ja erityisesti riskien arvioinnin dokumentointi. Tietoturvallisuuden hallintaan liittyvät suunnitelmat ja ohjeet sekä arvioinnin tulokset ja johtopäätökset tulisi esittää kirjallisena. Dokumentteihin tulee täydentää tiedot toimenpiteiden toteutumisesta. Dokumentoinnilla tässä tarkoitetaan laajasti erilaisia kirjalliseen muotoon saatettavissa olevia tallenteita, kuten Intranet-sivuja ja toiminnanohjausjärjestelmän työmääräyksiä.

3.2 Fyysinen turvallisuus

Fyysinen turvallisuus (FYY) sisältää luvattoman tietoihin pääsyn estäviä ja rajoittavia toimitiloihin ja säilytysratkaisuihin liittyviä kriteereitä. Lisäksi osa-alueella on kuvattu tietojen käsittelyyn, säilyttämiseen, siirtämiseen, kuljettamiseen ja tuhoamiseen liittyviä kriteereitä. Fyysisen turvallisuuden osa-aluetta on mahdollista käyttää arvioitaessa tiedon suojaamiseksi toteutettuja fyysisen turvallisuuden toimenpiteitä.

Osa-alueen sisältö perustuu Katakri-kriteeristöön. Erityisesti turvallisuusluokitellun tiedon käsittelyä koskevien kriteerien sisältö on pyritty säilyttämään yhdenmukaisena Katakrin kanssa. Selkeimpiä eroja suhteessa Katakriin ovat kansainvälisiin tietoturvallisuusvelvoitteisiin perustuvien kriteerien jättäminen pois osa-alueelta sekä tiettyjen kriteerien luokittelu sovellettavaksi myös muille kuin turvallisuusluokitelluille tiedoille.

Osa-alueen rakenne on suunniteltu siten, että eri tasoisia turvallisuusalueita koskevat yhteiset kriteerit, vain hallinnollisia alueita koskevat kriteerit sekä vain turva-alueita koskevat kriteerit on koottu kukin omaan alalukuunsa. Tämä rakenne poikkeaa Katakrin rakenteesta, jossa osa kriteereistä on toistettu saman sisältöisinä eri tasoisilla turvallisuusalueilla.

Viranomaisten tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia (tiedonhallintalaki 15 § 2 mom). Turvallisuusluokiteltujen tietojen fyysiseksi suojaamiseksi, turvallisuusluokitteluasetuksessa on säädetty kahdentyyppisistä fyysisesti suojatuista turvallisuusalueita: hallinnollisista alueista ja turva-alueista. Julkrissa käytetään hallinnollisen alueen ja turva-alueen käsitteitä.

Salassa pidettäviä tietoja sisältävät tietovarannot sekä niiden käsittelyyn käytetyt tietojärjestelmät suositellaan sijoitettavaksi viranomaisen tähän tarkoitukseen määrittelemälle suojatulle-alueelle, jollainen on esimerkiksi turvallisuusluokitteluasetuksessa ja tässä suosituksessa ja sen liitteenä olevassa kriteeristössä kuvattu hallinnollinen alue.

Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten turvatoimien toteuttamista siten, että estetään luvaton pääsy tietoihin:

a) varmistamalla, että tietoja käsitellään ja säilytetään asianmukaisesti,
b) mahdollistamalla pääsy tietoihin tiedonsaantitarpeen ja tarvittaessa turvallisuusselvitysten perusteella,
c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet ja
d) estämällä oikeudetta tapahtuva tunkeutuminen tai viivyttämällä sitä.

Työskentely on mahdollista järjestää myös eri organisaatioille yhteisissä toimitiloissa. Tällöin yhteisissä toimitiloissa tulee noudattaa yhteisiä toimitilaturvallisuuteen liittyviä periaatteita, jotka mahdollistavat salassa pidettävän tiedon asianmukaisen käsittelyn ja säilyttämisen. Kunkin tietoja käsittelevän organisaation tulee lisäksi varmistaa, että yhteisten toimitilojen tarjoama turvallisuus on riittävä suhteessa organisaatioon kohdistettuihin fyysisen turvallisuuden vaatimuksiin.

3.3 Tekninen turvallisuus

Tekninen osa-alue kattaa tietojärjestelmien ja tietoliikenneyhteyksien teknisiin ominaisuuksiin, turvalliseen käyttöön ja toimintamalleihin liittyvät kriteerit. Kriteerien tavoitteena on varmistaa, että tietojärjestelmät ja niiden käyttö toteuttavat yleiset teknisen tietoturvallisuuden, ja tarvittaessa myös tietosuojan, vaatimukset. Huomioitavaa kuitenkin on, että teknisen osa-alueen kriteerien toteuttaminen ei yksinään takaa yksittäisen tietojärjestelmän turvallisuutta, vaan myös muiden osa-alueiden kriteerit tulee huomioida.

Arvioinnin kohteena voi olla joko yksittäinen tietojärjestelmä tai tietojenkäsittely-ympäristö tai laajempi kokonaisuus tietojärjestelmiä. Arvioitaessa useista tietojärjestelmistä koostuvaa kokonaisuutta, tulee huomioida vaatimusten toteutuminen kaikissa yksittäisissä järjestelmissä.

Tekninen osa-alue ottaa huomioon myös järjestelmien sijoittumisen turvallisuusalueille ja niiden etäkäytön turvallisuusalueiden ulkopuolella. Tarkemmat vaatimukset hallinnolliselle alueelle ja turva-alueelle on määritelty fyysisen turvallisuuden osa-alueella.

Kriteeristössä viitataan usean kriteerin osalta, että salausratkaisun tulee olla riittävän turvallinen kyseiseen käyttötapaukseen. Salausratkaisun turvallisuuden arvioinnissa voi käyttää hyväksi esimerkiksi Kyberturvallisuuskeskuksen NCSA-toiminnon kansainvälisen turvallisuusluokitellun tiedon suojaamiseksi myöntämiä hyväksyntöjä. Lisätietoja on saatavilla Kyberturvallisuuskeskuksen verkkosivuilta.

3.4 Varautuminen ja jatkuvuudenhallinta

Osa-alueelle on koottu normaaliolojen varautumista ja jatkuvuudenhallintaa koskevia kriteereitä. Kriteerit perustuvat tiedonhallintalain (muun muassa 4 §:n 2 mom 2 k, 13 §:n 1, 2 ja 4 mom sekä 15 §) ja yleisiin vaatimuksiin laadittavista ohjeista ja tietoturvallisuustoimenpiteistä sekä standardissa ISO/IEC 27002 kuvattuihin tietoturvallisuuden jatkuvuutta kuvaaviin hallintakeinoihin. Valmiuslain piiriin kuuluvat toiminnan jatkuvuutta poikkeusoloissa koskevat toimenpiteet on rajattu kriteeristön ulkopuolelle. Kriteeristö kuitenkin osaltaan tukee organisaatiota myös poikkeusoloihin varautumista koskevien vaatimusten täyttämisessä.

Osa-alueen kriteerit koskevat pääasiassa saatavuudeltaan tärkeiksi tai kriittisiksi luokiteltuja kohteita. Saatavuuden tasot on kuvattu luvussa 4.2 Luokittelutasot. Riskiperusteisesti kriteereitä voidaan soveltaa myös matalampiin saatavuusluokkiin kuuluvissa kohteissa. Jatkuvuusvaatimusten sekä niiden taustalla olevan lainsäädännön selvittäminen koskee kuitenkin lähtökohtaisesti kaikkia organisaatioita.

Keskeisiä kriteereitä osa-alueella ovat varautumistoimenpiteet erilaisiin vakaviin häiriötilanteisiin, toiminnan jatkuvuussuunnitelmat sekä tietojärjestelmien toipumissuunnitelmat ja niiden harjoittelu. Jatkuvuudenhallinta liittyy läheisesti häiriöiden ja poikkeamatilanteiden hallintaprosesseihin, joihin liittyvät kriteerit on kuvattu HAL- ja TEK-osa-alueilla.

3.5 Tietosuoja

Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella.

Henkilötietojen käsittelyssä on noudatettava tietosuoja-asetuksen vaatimuksia, kun käsittely on kokonaan tai osittain automaattista tai tiedot muodostavat rekisterin osan. Tietosuoja-asetus suojaa henkilötietoja riippumatta siitä, mitä tekniikkaa tietojenkäsittelyssä käytetään. Tietojen säilytystavalla ei myöskään ole merkitystä. Tietoja voidaan säilyttää esimerkiksi tietojärjestelmässä, videovalvontajärjestelmässä tai paperiarkistossa.

Tietosuoja-osa-alueelle on koottu yksinomaan henkilötietojen käsittelyä koskevia kriteereitä, joita ovat esimerkiksi käsittelyn lainmukaisuutta, tietosuojaperiaatteita sekä rekisteröidyn oikeuksia koskevat kriteerit. Lisäksi henkilötietojen käsittelyyn sovelletaan Julkrissa muilla osa-alueilla olevia tietoturvakriteereistä. Henkilötietojen käsittelyssä sovellettavat tietoturvakriteerit ovat Julkrissa valtaosin yhteisiä muiden tietojen turvaamisessa käytettyjen kriteerien kanssa. Jokainen muilla osa-alueilla oleva kriteeri on luokiteltu sen mukaan, sovelletaanko sitä myös henkilötietojen käsittelyssä ja jos sovelletaan, koskeeko kriteeri kaikkia henkilötietoja vai ainoastaan erityisiä henkilötietoryhmiä. Muilla osa-alueilla olevia henkilötietojen käsittelyä koskevia kriteereitä on joissakin yksittäisissä tapauksissa tarkennettu tietosuoja-osa-alueella olevalla tarkentavalla kriteerillä.

4 Kriteerien tiedot

Arviointikriteeri koostuu tunnisteesta, luokitteluista, (luottamuksellisuus, eheys, saatavuus, henkilötieto), sisällöistä (nimi, vaatimus, yleiskuvaus ja toteutusesimerkki) sekä viittauksista eri lähteisiin.

Tunniste	**HAL-06, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto,**
Nimi	**Riskienhallinta**
Vaatimus	Organisaatio toteuttaa tietoturvallisuusriskien hallintaa ja on arvioinut olennaiset tietoihin kohdistuvat riskit sekä mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.
Yleiskuvaus	Tietoturvallisuusriskien hallintaprosessi koostuu toimintaympäristön määrittämisestä, riskien arvioinnista (tunnistaminen, analysointi, merkityksen arviointi), riskien käsittelystä, riskien hyväksynnästä, riskejä koskevasta viestinnästä ja tiedonvaihdosta sekä riskien seurannasta ja katselmoinnista. Tietoturvallisuusriskien hallinta on osa organisaation toimintaa ja muuta riskienhallintaa. Tietoturvallisuusriskien hallinnan avulla varmistetaan tietoturvallisuustoimenpiteiden riittävyys tietojen luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi. Riskienhallinta vaikuttaa muihin tietoturvallisuuden hallinnan eri osa-alueisiin. Riskienhallinta tulee suunnitella ja ohjeistaa siten, että siinä käsitellään systemaattisesti ja suunnitelmallisesti erilaisia tietoturvallisuuteen liittyviä riskejä kuten tietosisällön virheellisyyksistä johtuvia riskejä, organisaation toiminnan keskeytyksiin liittyviä riskejä sekä henkilötietojen tietoturvaloukkauksiin liittyviä riskejä.
Toteutusesimerkki	- Tietoturvallisuusriskien arvioinnissa ja analysoinnissa käytetään yleisesti hyväksyttyä menetelmää. - Tietoturvallisuusriskien arvioinneista laaditaan aikataulutettu ja vastuutettu vuosisuunnitelma. - Tietoturvallisuusriskien hallintaan osallistuu riittävästi asiantuntijoita. - Tietoturvallisuusriskien hallinnassa on otettu huomioon sidosryhmistä ja toimitusketjuista aiheutuvat riskit. - Tietoturvallisuusriskien arviointia hyödynnetään muissa tietoturvallisuuden hallinnan prosesseissa.
Lainsäädäntö	TiHL 13 § 1 mom; TLA 6 §, 7 §
Viitteet	FYY-01, TEK-01, TEK-13, TEK-15
Muita lisätietoja	SFS-EN ISO/IEC 27001:2017 6.1 ja 8-10, SFS-EN ISO/IEC 27005:2018 luku 6, SFS ISO 31000:2018, PiTuKri TJ-03; Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5 luku 5.2; Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2021:65 luku 6

Yllä on kuvattu esimerkkinä hallinnollisen osa-alueen kriteeri Riskienhallinta. Kriteerin tunniste on HAL-06. Tässä tapauksessa luottamuksellisuuden (L) taso on julkinen, eheys (E) on vähäinen, saatavuus (S) on vähäinen ja kyseistä kriteeriä voi hyödyntää myös henkilötietojen käsittelyn arvioimisessa (TS). Luvuissa 4.1.-4.4 on kuvattu tarkemmin kriteerien tunnisteet ja niiden tasot.

4.1 Tunniste

Kriteerillä on yksilöivä tunniste, joka koostuu osa-alueen nimen lyhenteestä, pääkriteerin juoksevasta numerosta sekä alikriteerin juoksevasta numerosta. Yksilöivien tunnisteiden lyhenteet ovat hallinnollinen (HAL), tekninen (TEK), varautuminen (VAR) ja fyysinen (FYY) ja tietosuoja (TSU). Pääkriteerit on numeroitu osa-alueittain ja alikriteerit pääkriteereittäin. Esimerkiksi teknisen tietoturvallisuuden osa-alueella on pääkriteeri TEK-14 ja sillä alikriteerit TEK-14.1, TEK-14.2.

4.2 Luokittelutasot

Kriteerit on luokiteltu luottamuksellisuuden, eheyden ja saatavuuden näkökulmista. Jos kriteeri koskee myös henkilötietojen käsittelyä, on se luokiteltu lisäksi tietosuojan näkökulmasta. Täydentävät tietoturvallisuuden näkökulmat, kuten tiedon kiistämättömyys tai autenttisuus, on huomioitu kriteerien sisällöissä.

Kriteeri voi liittyä yhteen tai useampaan tietoturvallisuuden näkökulmaan ja se valikoituu mukaan arviointiin, jos se on olennainen yhdestäkin näkökulmasta. Esimerkiksi kriteeri voi olla merkitty eheyden näkökulmasta tasolle Normaali, mikä tarkoittaa, että kriteeri on olennainen kaikille niille tiedoille, jotka on luokiteltu eheyden näkökulmasta tasolle Normaali.

Monet kriteerit ovat luonteeltaan yleisiä ja liittyvät laajasti tietoturvallisuuden hallintaan. Tällaisia ovat esimerkiksi tehtävien ja vastuiden määrittelyyn, riskien hallintaan ja dokumentointiin liittyvät kriteerit.

4.2.1 Luottamuksellisuuden tasot

Luottamuksellisuus on tiedon ominaisuus, joka ilmentää sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä eikä se paljastu sivullisille. Tässä suosituksessa

luottamuksellisuuden tasot on kuvattu asteikolla julkinen, salassa pidettävä, turvallisuusluokka IV, turvallisuusluokka III, turvallisuusluokka II ja turvallisuusluokka I. Taulukossa on kuvattu nämä tasot ja esimerkkejä. Tiedonhallintalautakunnan suositus (2021:5) sisältää suosituksia turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä sekä turvallisuusluokiteltujen asiakirjojen käsittelyä koskevista tietoturvallisuustoimenpiteistä.

Taso	Kuvaus	Esimerkki
Julkinen	Viranomaisen asiakirjat ovat julkisia, jollei laissa erikseen toisin säädetä. (julkisuuslaki 1 §)	Kunnanvaltuuston pöytäkirjat, organisaation julkiset internet-sivut.
Salassa pidettävä	Viranomaisen asiakirja on pidettävä salassa, jos se laissa on säädetty salassa pidettäväksi tai jos viranomainen lain nojalla on määrännyt sen salassa pidettäväksi taikka jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus. (julkisuuslaki 22 §)	Potilasasiakirjat, tiedot sosiaalihuollon asiakkaasta, psykologiset testit ja soveltuvuuskokeet.
Turvallisuusluokka IV (TL IV)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **lievää** vahinkoa suojattavalle edulle.	Olennaisen tietojärjestelmän turvajärjestelyiden dokumentaatio, jonka paljastuminen ei keskeytä toimintaa, mutta saattaa edellyttää muutoksia paljastuneissa suunnitelmissa.
Turvallisuusluokka III (TL III)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **vahinkoa** suojattavalle edulle.	Elintärkeiden toimintojen turvajärjestelyiden dokumentaatio, jonka paljastumisen vuoksi toiminta joudutaan keskeyttämään.
Turvallisuusluokka II (TL II)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **merkittävää vahinkoa** suojattavalle edulle.	Elintärkeiden toimintojen turvajärjestelyiden dokumentaatio, jonka paljastumisen vuoksi laajan ihmisjoukon turvallisuutta ei voida taata ja jonka seurauksena toiminta joudutaan keskeyttämään pitkähköksi ajaksi.
Turvallisuusluokka I (TL I)	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **erityisen suurta vahinkoa** suojattavalle edulle.	Yhteiskunnan toimintakyvyn kannalta keskeisiin toimintoihin, kuten kriittiseen infrastruktuuriin tai elintärkeään toimintaan liittyvän tiedon paljastuminen, jonka seurauksena viranomaisen toiminta todennäköisesti estyy ja vahinko on laajamittaista.

Kriteerejä ei ole luokiteltu luottamuksellisuuden näkökulmasta erikseen tasolle Harkinnanvaraisesti annettava. Organisaation on riskien perusteella harkittava, sisällytetäänkö harkinnanvaraisesti annettavien tietojen arviointiin salassa pidettävien tietojen kriteereitä. Tämä onnistuu määrittelemällä arvioinnin esiehdoissa luottamuksellisuus

tasolle Julkinen, jolloin Julkri-työkalu tarjoaa salassa pidettäviä tietoja koskevat kriteerit valinnaisiksi.

4.2.2 Saatavuuden tasot

Saatavuus tarkoittaa sitä, miten tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla. Julkrissa saatavuuden tasot ovat vähäinen, normaali, tärkeä ja kriittinen. Taulukossa on kuvattu ja annettu esimerkkejä eri saatavuuden tasoista.

Taso	Kuvaus	Esimerkki
Vähäinen	Tiedon saatavuuden osalta pystytään hyväksymään useiden viikkojen mittaisia häiriöitä.	Henkilöstön pysäköintipaikkojen rekisteri, puiston penkkien vikarekisteri
Normaali	Tiedon saatavuuden osalta pystytään hyväksymään enintään päivien mittaisia häiriöitä.	Arkistojärjestelmä
Tärkeä	Tiedon saatavuuden osalta pystytään hyväksymään enintään tuntien mittaisia häiriöitä.	Potilastietojärjestelmä
Kriittinen	Tiedon saatavuuden osalta pystytään hyväksymään enintään minuuttien mittaisia häiriöitä.	Keskitetyt käyttäjän tunnistamispalvelut

4.2.3 Eheyden tasot

Eheys on tiedon ominaisuus, joka tarkoittaa sitä, että tietoa ei ole muutettu luvatta tai että se ei ole muuttunut vahingossa ja että mahdolliset muutokset voidaan todentaa. Taulukossa on kuvattu Julkrissa käytössä olevat eheydet tasot vähäinen, normaali ja tärkeä sekä annettu tasoihin joitakin esimerkkejä.

Taso	Kuvaus	Esimerkki
Vähäinen	Tiedon häviämisestä tai muuttumisesta ei aiheudu olennaista haittaa.	Toimisto-ohjelmistot, järjestelmien virhelokit.
Normaali	Tiedon häviäminen tai muuttuminen aiheuttaa kohtuullista haittaa, mutta se voidaan havaita ja siitä voidaan toipua.	Henkilöstöhallinnon järjestelmät.
Tärkeä	Tiedon häviäminen tai muuttuminen aiheuttaa merkittävää haittaa tai mainevahinkoa ja sen havaitseminen voi olla vaikeaa.	Laboratoriotuloksia välittävät integraatioalustat, joissa yksittäisten mittausten virheiden havainnointi voi olla vaikeaa. Henkilötietojen käsittelyyn liittyvät lokitiedot.

Kriittinen	Tiedon häviäminen tai muuttumista ei voida hyväksyä missään tilanteessa.	Yhteiskunnan toimivuuden kannalta keskeiset maksuliikennejärjestelmät tai raideliikenteen ohjausjärjestelmä

4.3 Sisällöt

Kriteerien sisältö koostuu nimestä, vaatimuksesta, yleiskuvauksesta ja toteutusesimerkistä.

- **Nimi** kuvaa otsikkotasolla mihin asiaan kriteeri kohdistuu. Nimi on yksi tai muutama kriteerin aihepiiriä kuvaileva sana. Alikriteerien nimi koostuu pääkriteerin nimestä sekä väliviivalla erotetusta tarkenteesta. Esimerkiksi Käyttöoikeudet – ajantasaisuus, joka on käyttöoikeudet -pääkriteeriä täsmentävä ajantasaisuutta koskeva alikriteeri.
- **Vaatimus** kuvaa tavoitteen, joka organisaation tulee täyttää. Vaatimus on lyhyehkö lause tai lyhyt kappale. Vaatimukset voidaan täyttää useilla eri toteutustavoilla. Vaatimukset ovat yksilöityjä, eli samaan vaatimukseen ei sisälly useita eri vaatimuksia. Mikäli alikriteeri ei sisällä erillistä vaatimusta, alikriteeri tarkentaa pääkriteeriä joko yleiskuvauksen tai toteutusesimerkin osalta.
- **Yleiskuvaus** sisältää kriteeriä taustoittavaa ja perustelevaa lisätietoa. Se ei ole vaatimus vaan peruste kriteerille. Yleiskuvauksessa voidaan esimerkiksi kuvata uhkia, joita kriteerin mukaisten hallintakeinojen avulla torjutaan. Mikäli samaan kokonaisuuteen liittyy useita alikriteereitä, laaditaan eri kriteereille yhteinen yleiskuvaus vain kertaalleen pääkriteerin yhteyteen.
- **Toteutusesimerkki** kuvaa miten organisaatio voi toteuttaa vaatimuksen. Toteutusesimerkki ei ole vaatimus, mutta se voi toimia suuntaa antavana ohjeena siitä tasosta, miten vaatimuksen voi täyttää.

4.4 Viittaukset

Kriteeri voi sisältää viittauksia lainsäädäntöön, ohjeisiin ja standardeihin sekä viittauksia Katakri- ja PiTuKri-arviointikriteereihin sekä muihin Julkri-kriteeristön kriteereihin. Viittaukset on pyritty yksilöimään siten, että vastaava kohta on löydettävissä nopeasti viiteaineistosta.

- **Lainsäädäntö** kuvaa mihin lainsäädäntöön kriteeri perustuu.
- **Muita lisätietoja** sisältävät viittauksia kriteeriin liittyviin tiedonhallintalautakunnan suosituksiin, PiTuKri-arviointikriteeristöön ja standardeihin.

- **Julkri-viite** sisältää viittauksen yhteen tai useampaan muuhun Julkri-kriteeristön kriteeriin, mikäli kriteeri muodostaa sovellettavan kokonaisuuden yhdessä jonkun toisen kriteerin kanssa.
- **Katakri-viite** sisältää viittauksen vastaavaan kriteeriin Katakri-arviointi-kriteeristössä, jos sellainen on olemassa.

5 Kriteeristön käyttö

Kriteeristöä voidaan soveltaa koko organisaation toimintaan, jonkun osa-alueen toimintaan tai hankittavan palvelun arviointiin. Tiedon eri tasoille tarkoitetut käsittely-ympäristöt suositellaan arvioitavaksi erikseen, jotta matalamman tason kohteisiin ei sovelleta liian korkeita kriteereitä eikä siten lisätä tarpeettomasti monimutkaisuutta ja kustannuksia.

Arvioinnin kohteen täsmällinen määrittely ja rajaus on yksi kriteeristön käytön tärkeimmistä vaiheista. Arviointi voi kohdistua yksittäiseen järjestelmään, mutta lisäksi tulee varmistaa, että eri arvioinnit yhdessä kattavat koko organisaation toiminnan.

Organisaatiossa käsitellään kriittisyydeltään ja luottamuksellisuudeltaan moniin eri luokkiin kuuluvia tietoja ja käsittelyssä käytetään monia eri tietojärjestelmiä sekä palveluita. Lisäksi eri tietojärjestelmien yhteydessä usein hyödynnetään yhteisiä alustapalveluita. Näistä seikoista johtuen organisaation kannattaa suunnitella arvioitavat kohteet loogisiksi kokonaisuuksiksi sekä hyödyntää jo aiemmin tehtyjä arviointeja.

Esimerkiksi jos hankitaan uusi tietojärjestelmä, jota tullaan operoimaan yhteisellä alustalla, jonka turvallisuus on jo aiemmin arvioitu, voidaan uuden tietojärjestelmän arvioinnista jättää pois aiemmin arvioidut yhteisen alustan vastuulla olevat kriteerit.

Käyttötapausten avulla organisaatio voi määritellä ennakolta eri tilanteisiin soveltuvia kriteereitä ja siten helpottaa kriteeristön käyttöä samankaltaisena toistuvissa tilanteissa. Käyttötapausten hyödyntämistä on kuvattu tarkemmin erillisessä liitteessä 2 Työkalun käyttöohje.

Ennen kriteeristön käyttöä organisaation tulee määritellä arvioinnin kohteesta seuraavat asiat:

- arvioitavalta kohteelta edellytettävä luottamuksellisuus, eheys ja saatavuus,
- sisältyykö arvioinnin kohteeseen henkilötietoja sekä kuuluvatko nämä tiedot erityisiin henkilötietoryhmiin,
- mahdollisesti arvioinnista poisjätettävät osa-alueet,
- käyttötapaus, jos arviointiin soveltuva käyttötapaus on olemassa.

Arvioinnin kohteen luokittelun perusteella kriteerit ovat olennaisia, valinnaisia tai jätetään arvioinnin ulkopuolelle. Organisaation on suositeltavaa sisällyttää olennaiset kriteerit arviointiin. Valinnaisten kriteerien osalta organisaatio päättää riskiarvion sekä tilannekohtaisen harkinnan perusteella kunkin kriteerin sisällyttämisestä arviointiin.

Hyödynnettäessä Julkri-kriteeristöä organisaation tietoturvallisuuden arvioinnissa, on lähtökohtaisesti täytettävä arviointiin sisältyvien kriteerien vaatimukset. Organisaatio voi kuitenkin jättää arviointiin sisältyvän kriteerin vaatimuksen täyttämättä, jos organisaatio voi osoittaa, että riskiä ei ole tai riski on hyväksyttävällä tasolla kriteerin vaatimuksen täyttämättä jättämisestä huolimatta. Esimerkiksi riskejä on pienennetty riittävästi muilla keinoilla hyödyntäen kompensoivia kontrolleja.

Jos organisaatio tarvitsee todistuksen Julkri-kriteeristöön perustuvasta vaatimuksenmukaisuudesta, niin kaikkien arviointiin sisältyvien kriteeriteerien tulee toteutua arvioinnin kohteessa. Jos kriteerin toteuttaminen ei kuitenkaan ole mahdollista, on yksilöitävä ja perusteltava kompensoivat menettelyt, joilla varmistetaan, että riski on hyväksyttävällä tasolla kriteerin toteuttamatta jättämisestä huolimatta.

Kriteeristöä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä. Kriteeristö on suositus ja lainsäädännön vaatimukset voidaan täyttää myös muulla kuin kriteereissä kuvatulla tavalla.

5.1 Arviointia edeltävät toimenpiteet

Ennen arvioinnin käynnistymistä suositellaan hankintojen turvallisuuden varmistamista, lainsäädäntöjohdannaisten riskien selvittämistä sekä sopimusehtojen soveltuvuus käyttötarkoitukseen. Tämä koskee ensisijaisesti tietojärjestelmille tai palveluille tehtäviä arviointeja. Tässä voidaan hyödyntää hallinnollisen turvallisuuden osa-alueen riskienhallintaan liittyviä kriteerejä HAL-06 ja HAL-06.1 sekä hankintojen turvallisuuteen liittyviä kriteerejä HAL-16 ja HAL-16.1. Mainittuja edeltäviä toimenpiteitä on kuvattu lyhyesti seuraavissa kappaleissa.

Tietoturvallisen tietojenkäsittelyn järjestäminen

Organisaation tulee varmistaa hankinnoissaan, että käytettävien tietojärjestelmien ja palveluiden osalta on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. Organisaation on ennakolta varmistuttava siitä, että tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti.

Lainsäädäntöjohdannaiset riskit

Organisaatio tulee tunnistaa lainsäädäntöjohdannaiset riskit, joilla viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa palveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy palvelun tai järjestelmän asiakkaiden salassa pidettäviin tietoihin.

Järjestelmä- ja palvelusopimukset

Palvelun tai järjestelmän palveluntarjoajan sopimusehdoista tulee varmistaa, että ne eivät rajoita kyseisen palvelun tai järjestelmän soveltuvuutta kyseiseen käyttötapaukseen koko niiden elinkaaren ajan.

6 Säädökset

Asevelvollisuuslaki (1438/2007). https://www.finlex.fi/fi/laki/ajantasa/2007/20071438

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI

Laki digitaalisten palvelujen tarjoamisesta (306/2019). https://www.finlex.fi/fi/laki/ajantasa/2019/20190306

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018). https://www.finlex.fi/fi/laki/ajantasa/2018/20181054

Laki julkisen hallinnon tiedonhallinnasta (906/2019). https://finlex.fi/fi/laki/ajantasa/2019/20190906

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). https://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011). https://www.finlex.fi/fi/laki/ajantasa/2011/20111406

Laki viranomaisten toiminnan julkisuudesta (621/1999). https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Tietosuojalaki (1050/2018). https://www.finlex.fi/fi/laki/ajantasa/2018/20181050?search%5Btype%5D=pika&search%5Bpika%5D=tietosuojalaki

Turvallisuusselvityslaki (726/2014). https://www.finlex.fi/fi/laki/ajantasa/2014/20140726

Työaikalaki (872/2019). https://www.finlex.fi/fi/laki/ajantasa/2019/20190872

Valtion virkaehtosopimuslaki (664/1970). https://www.finlex.fi/fi/laki/ajantasa/1970/19700664

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). https://www.finlex.fi/fi/laki/alkup/2019/20191101

Valmiuslaki (1552/2011). https://www.finlex.fi/fi/laki/ajantasa/2011/20111552

7 Ohjeet ja muut materiaalit

BSI IT-Grundschutz-Compendium 2021. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf

CIS Critical Security Controls. https://www.cisecurity.org/controls

Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

NIST SP 800 -sarja. https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information https://csrc.nist.gov/publications/sp800

Kansallinen turvallisuusviranomainen. https://um.fi/kansallinen-turvallisuusviranomainen

NIST SP 800 -sarja. https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information https://csrc.nist.gov/publications/sp800. Erityisesti 800-53 (tietoturvallisuuden ja tietosuojan hallintakeinot), 800-37 (riskienhallinta), 800-63B (käyttäjän tunnistaminen ja elinkaaren hallinta)

PiTuKri 2020 Pilvipalveluiden turvallisuuden arviointikriteeristö. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Suojelupoliisi Yritysturvallisuusselvitys. Yritysturvallisuusselvitys luotaa yrityksen luotettavuutta ja tietoturvaa. https://supo.fi/yritysturvallisuusselvitys

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö 2021:65. Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. http://urn.fi/URN:ISBN:978-952-367-897-2

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö 2021:5. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. http://urn.fi/URN:ISBN:978-952-367-500-1

Tietosuojavaltuutetun toimisto. Osoita noudattavasi tietosuojasäännöksiä. https://tietosuoja.fi/osoitusvelvollisuus

Turvallisuuskomitea (2017). Yhteiskunnan turvallisuusstrategia. https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/

Traficom 2021. Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit. Tilaajaorganisaation näkökulma. ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf (kyberturvallisuuskeskus.fi)

Traficom 2021. Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat-salausratkaisut

Valtiovarainministeriö (2020:73). Pilvipalvelujen soveltamisohje - Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille. http://urn.fi/URN:ISBN:978-952-367-503-2

Yleisiä tarkastusluetteloita ja kovennusohjeita

NIST - National Checklist Program Repository. https://ncp.nist.gov/repository

CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

DISA Security Technical Implementation Guides (STIGs). https://public.cyber.mil/stigs/