Arkkitehtuurikilta

30.3.2026

Digitaalinen turvallisuus

Sisällys

Arkkitehtuurikilta

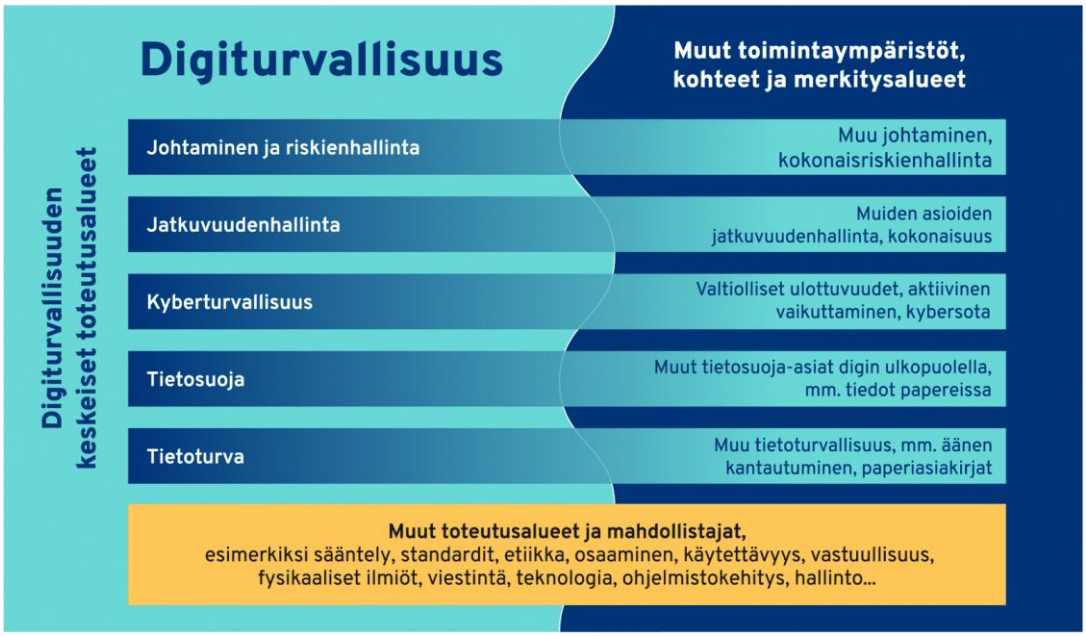
30.3.2026

1 Mitä on digiturva

Digitaalisella turvallisuudella eli digiturvalla pyritään varmistamaan, että digitaalinen toimintaympäristö on luotettava, turvallinen ja saatavilla. Tämä edellyttää, että eri toimijat osaavat varautua digitaaliseen toimintaympäristöön kohdistuviin uhkiin, kestävät häiriötilanteita ja pystyvät palautumaan niistä mahdollisimman hyvin ja nopeasti. Arkistenkin toimintojen turvaaminen vaatii laaja-alaista yhteistyötä, jaettuja toimintamalleja sekä halua kehittää niitä.

Digitaalisen turvallisuuden toteutusalueet ulottuvat myös digitaalisen maailman ulkopuolelle. Digitaalinen turvallisuus ei siis ole organisaation tai yhteiskunnan muusta toiminnasta erillinen kokonaisuus vaan olennainen osa niiden kaikkea toimintaa.

Julkisen hallinnon digitaalisella turvallisuudella on viisi painopistettä, jotka ovat kaikille toimijoille yhteisiä ja välttämättömiä hallitun digitaalisen turvallisuuden tuottamiseksi. Nämä painopisteet ovat johtaminen ja riskienhallinta, jatkuvuudenhallinta, tietoturva, tietosuoja ja kyberturvallisuus.[1]



1.1 Digitaalisen turvallisuuden arkkitehtuuri

Digitaalisen turvallisuuden arkkitehtuuri on ensisijaisesti suunnittelutyötä helpottava työväline, jolla digitaalista turvallisuutta voidaan kehittää ja jäsentää. Arkkitehtuuri muodostaa käsityksen organisaation suojattavasta omaisuudesta ja toimintaympäristöstä sekä niihin kohdistuvista uhista ja riskeistä. Lisäksi se kattaa ymmärryksen organisaatioon kohdistuvista vaatimuksista ja strategisista linjauksista sekä niitä toteuttavista digitaalisen turvallisuuden rakennusosista.

[1] Mitä on digiturva? | Digi- ja väestötietovirasto (dvv.fi)

Digitaalisen turvallisuuden arkkitehtuurilla siis pyritään suunnittelemaan ja hahmottamaan digitaalista turvallisuutta, joka on laaja ja jatkuvasti muutoksessa oleva kokonaisuus, kiinnittäen huomion erityisesti siihen, miten muuttuva ympäristö ja sen asettamat vaatimukset vaikuttavat tehtyihin digitaalisen turvallisuuden valintoihin ja ratkaisuihin.

Digitaalisen turvallisuuden arkkitehtuurilla pyritään saavuttamaan muun muassa seuraavia tavoitteita:

- Ymmärretään organisaation toiminnan tarpeet ja asetetaan niiden perusteella tavoitteet digitaalisen turvallisuuden toimintatavoille ja teknisille ratkaisuille.
- Laaditaan kuvaus organisaation digitaalisen turvallisuuden rakenteista osana organisaation kokonaisarkkitehtuuria.
- Sovitetaan digitaalisen turvallisuuden ratkaisut organisaation muuhun toimintaan esimerkiksi huomioimalla ne organisaation kokonaisarkkitehtuurissa.
- Asetetaan digitaaliselle turvallisuudelle tavoitetila, johon pyritään määrätietoisella kehittämisellä.

Viitekehys ei siis ole sellaisenaan kriteeristö tai katalogi turvallisuuskontrolleista, mutta se sisältää konkreettisia toimenpiteitä ja esimerkkejä digitaalisen turvallisuuden parantamiseksi.

Kenelle?

Viitekehys on tarkoitettu kaikille julkisen hallinnon toimijoille digitaalisen turvallisuuden kokonaisuuden suunnittelun ja hahmottamisen työvälineeksi.

Viitekehyksessä ei oteta kantaa siihen, millä välineellä tai työkalulla organisaatiossa tulisi kuvata tai dokumentoida digitaalista turvallisuutta, sillä sellainen kuvaustapa mikä toimii yhdessä organisaatiossa, ei välttämättä toimi lainkaan toisessa. Organisaation tulisikin hyödyntää viitekehystä parhaaksi katsomallaan tavalla. Visuaalisten ja rakenteellisten kuvausten tekeminen helpottaa kuitenkin huomattavasti laajojen kokonaisuuksien hahmottamista.

2 Viitekehys

Digitaalisen turvallisuuden arkkitehtuurin viitekehys pohjautuu yhdysvaltalaisen National Institute of Standards and Technologyn (NIST) laatimaan ja kansainvälisesti laajasti tunnettuun Cybersecurity Framework -kehykseen. Viitekehys kokoaa käytäntöjä useasta eri standardista ja se koostuu viidestä avaintoiminnosta: hallinnointi, tunnistaminen, suojaaminen, havainnointi, reagointi ja palautuminen.

Viitekehys mahdollistaa järjestelmällisen digitaaliseen turvallisuuteen liittyvien vaatimusten, periaatteiden ja näitä palvelevien kyvykkyyksien suunnittelun ja dokumentoinnin organisaation tavoitteiden mukaisesti. Viitekehyksen avaintoiminnot ja niiden tavoitteet on kuvattu lyhyesti tässä dokumentissa. Varsinaiset toimenpiteet on jaoteltu viiden avaintoiminnon alle kategorioihin, jotka muodostavat viitekehyksen rakenteen.

Cybersecurity Framework

Arkkitehtuurikilta 30.3.2026

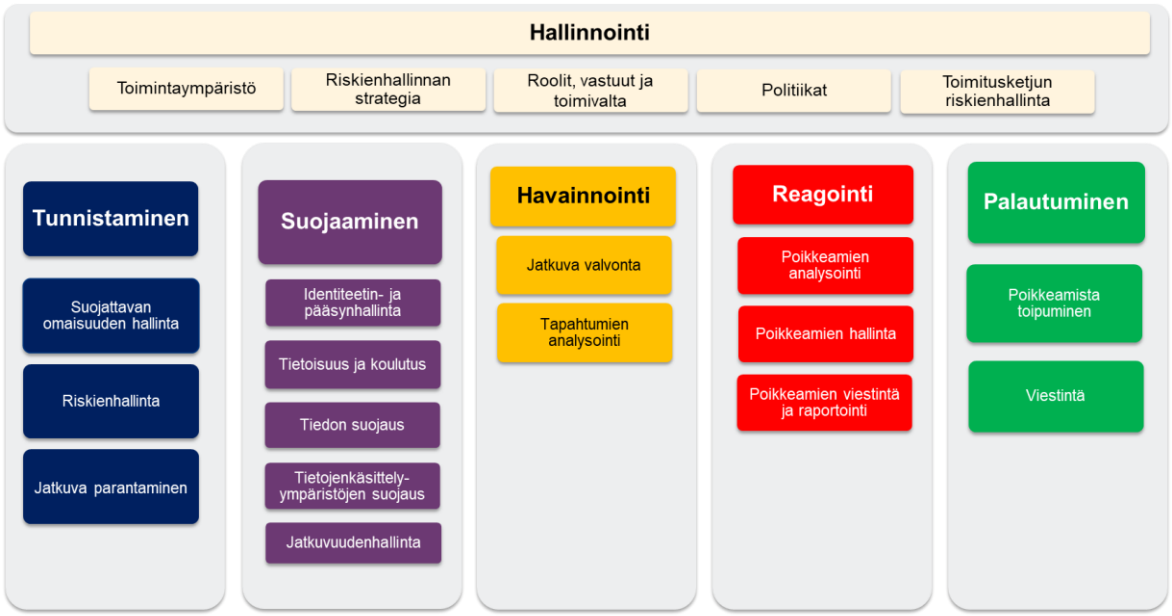
Digitaalisen turvallisuuden arkkitehtuurin viitekehys pohjautuu yhdysvaltalaisen *National Institute of Standards and Technologyn (NIST)* laatimaan ja kansainvälisesti laajasti tunnettuun *Cybersecurity Framework* -kehykseen. Viitekehys kokoaa käytäntöjä useasta eri standardista ja se koostuu kuudesta avaintoiminnosta: **hallinnointi, tunnistaminen**, **suojaaminen**, **havainnointi**, **reagointi** ja **palautuminen**. Toiminnot jakautuvat viitekehyksessä useampaan alikategoriaan sekä näiden yksityiskohtaisempiin toimenpiteisiin ja niiden muodostamiin **kyvykkyyksiin.**

Cybersecurity Framework | NIST

The NIST Cybersecurity Framework (CSF) 2.0

Viitekehyksen esittely

Digitaalisen turvallisuuden arkkitehtuurin laatiminen aloitetaan tunnistamalla omaan toimintaympäristöön liittyvät tekijät, kuten suojattavat digitaaliset kohteet, infrastruktuuri, säädökset ja muut vaatimukset. Kun digitaaliseen turvallisuuteen liittyvät tekijät ja vaatimukset on tunnistettu, voidaan suojautumiseen ja havainnointiin käytetyt ratkaisut suunnitella käyttäen hyödyksi tätä tietoa. Ohjeistuksen päävaiheiden tarkoituksena on lisäksi auttaa rakentamaan kattavat rakenteet poikkeamatilanteisiin reagointiin, niistä palautumiseen sekä kertyneiden oppien ja kokemusten hyödyntämiseen jatkokehittämisessä.



2.1 Hallinnointi - Miten hallitsemme digitaalista turvallisuutta

Hallinnoinnin tavoitteena on, että organisaatiolla on hallintorakenteet ja prosessit digitaalisen turvallisuuden hallintaan.

Lopputuloksena on, että seuraavat organisaation digitaaliseen turvallisuuteen liittyvät asiat ovat linjassa organisaation toiminnan kanssa ja niitä kehitetään säännönmukaisesti.

- Strategiat
- Käytännöt
- Prosessit
- Resurssit

Näin ohjataan organisaatiota siinä, mitä sen tulisi tehdä saavuttaakseen ja priorisoidakseen muiden viitekehyksen viiden avaintoiminnon tavoitteet ja odotukset. Johtamiseen liittyvät toiminnot ovat keskeisiä kyber- ja digitaalisen turvallisuuden sisällyttämisessä osaksi organisaation laajempaa kokonaisvaltaista riskienhallintastrategiaa.

Hallinnointi kattaa organisaation toiminnan ymmärtämisen; kyberturvallisuusstrategian ja toimitusketjun riskienhallinnan määrittelyn; roolien, vastuiden ja valtuuksien asettamisen; politiikan luomisen; sekä toimitusketjujen hallinnan.

Oleellista on, että organisaation kyber- ja digitaalisen turvallisuuden riskienhallintastrategia, odotukset ja politiikka määritellään, viestitään ja että niitä seurataan.

2.2 Tunnistaminen - Mitä suojattavaa meillä on

Tunnistamisvaiheen tavoitteena on, että organisaatio on tunnistanut oman toimintaympäristönsä sekä toiminnan mahdollistavat ja toiminnan jatkuvuuteen liittyvät kriittiset suojattavat kohteet ja omaisuuden. Lisäksi organisaatio tunnistanut näihin kohdistuvat uhat ja riskit sekä niiden mahdollisen vaikutuksen toimintaansa.

Oman toimintaympäristön ja suojattavien kohteiden tunnistaminen on ensimmäinen osa digitaalisen turvallisuuden arkkitehtuurin muodostamista. Toimenpiteet, kuten kohteiden suojaus tai poikkeamien havainnointi voidaan tehdä vain, mikäli oma ympäristö tunnetaan riittävän hyvin.

Tunnistamisen lopputuloksena muodostuu kuvaus oman organisaation digitaalisesta ympäristöstä, kuten

- Järjestelmistä, tietovarannoista, laitteista ja niiden sisältämästä tiedosta
- Toimintaympäristöstä ja toimintaa ohjaavista tekijöistä kuten lainsäädännöstä
- Digitaalisen turvallisuuden hallintamallista, kuten käytännöistä ja suunnitelmista
- Digitaalisen ympäristön uhkista, riskeistä ja niiden hallintakeinoista

Oleellista digitaalisen turvallisuuden arkkitehtuurin kannalta on, että tunnistamisvaiheessa erityisiä suojaamisen, havainnoinnin, reagoinnin tai palautumisen toimenpiteitä vaativat kohteet kyetään määrittämään.

2.3 Suojaaminen - Miten suojaudumme uhilta

Suojautumisvaiheen tavoitteena on, että organisaatio suojaa tunnistetut kohteet, kuten tietojärjestelmät, tietovarannot ja tiedot riskienhallinnan keinoin tunnistetuilta uhilta ja riskeiltä. Käytännössä tämä tarkoittaa muun muassa identiteetin- ja pääsynhallinnan, tietoverkkojen turvallisuuden, tietoturvallisuuden, tietoturvateknologian suunnittelua ja toteuttamista suhteessa tunnistettuihin riskeihin sekä näiden toimenpiteiden dokumentointia ja kuvaamista.

Suojaamisen kannalta olennaista on ottaa huomioon erilaiset vaatimukset ja tietoturvaratkaisut tietojärjestelmien, palveluiden ja näitä tukevan infrastruktuurin elinkaaren kaikissa vaiheissa aina kehityksestä ylläpitoon ja päättämiseen.

Koska suojattavien kohteiden tietoturva- ja tietosuojavaatimukset vaihtelevat käsiteltävän tiedon ja toimintaympäristön mukaisesti, on erityisen tärkeätä tunnistaa oman organisaation toimintaan ja tietoon kohdistuvat vaatimukset kohdassa viitekehyksen kohdassa Tunnistaminen.

Viitekehyksessä esitellyt suojaustoimenpiteet ovat kansainvälisistä tietoturvallisuuden, kyberturvallisuuden ja digitaalisen turvallisuuden standardeista johdettuja toimenpiteitä, joiden avulla organisaation on mahdollista rakentaa suojaustaan kokonaisuutena erillisten ratkaisujen sijaan.

2.4 Havainnointi - Miten havaitsemme poikkeamat

Havainnointivaiheen tavoitteena on, että organisaatio kehittää digitaaliseen turvallisuuteen vaikuttavien häiriöiden havainnointikyvykkyyttä. Käytännössä tämä tarkoittaa poikkeamanhallintaprosessin määrittelyä ja toteuttamista siten, että organisaatio on määritellyt digitaalisen turvallisuuden perustason ja ottanut käyttöön prosessin ja menetelmät, joilla digitaalisen turvallisuuteen vaikuttavia tapahtumia havaitaan ja havainnointikyvykkyyttä saadaan parannettua.

On tärkeä huomata, että digitaalisen turvallisuuden kannalta pelkkä suojautuminen tunnistettuja riskejä ja uhkia vastaan ei riitä. Tarvitaan lisäksi käsitys siitä, mikä on normaalia toimintaa ja mikä on normaalista poikkeavaa toimintaa digitaalisissa ympäristöissä. Poikkeavan toiminnan havainnointia voidaan toteuttaa tehokkaasti, mikäli suojattavat kohteet ja näiden käyttötarkoitus ja toimintaympäristö tunnetaan riittävän hyvin.

Havainnointikyvyn toteuttamiseksi on olemassa useita erilaisia teknisiä ratkaisuja, mutta pelkästään teknisiin ratkaisuihin tukeutuminen ei riitä, vaan prosessit ja toimintamallit havaittujen poikkeamien käsittelyyn ja korjaamiseen on oltava olemassa.

Digitaalisen turvallisuuden havainnoinnin tukena toimii myös käyttäjien tekemät ilmoitukset. Siksi onkin oleellista, että organisaatiossa on toimintamalli ilmoitusten raportointiin ja vastaanottamiseen.

Seuraavat kohdat opastavat rakentamaan havainnointikykyä suunnitelmallisesti siten, että toimintamallit ja valitut tekniset ratkaisut tukisivat toisiaan mahdollisimman hyvin.

2.5 Reagointi - Kuinka hallitsemme poikkeamia

Reagointivaiheen tavoitteena on, että organisaatiolla on kyvykkyys reagoida havaittuihin digitaalisen turvallisuuden poikkeamiin mahdollisimman nopeasti poikkeamanhallintaprosessin mukaisesti. Käytännössä tämä tarkoittaa poikkeamahallintaprosessin toteuttamista siten, että henkilökunta ja sidosryhmät tietävät tehtävänsä ja roolinsa reagointitoimenpiteissä, viestintä-, koordinaatio- ja raportointikäytännöt on määritelty ja digitaalisen turvallisuuden häiriötapahtumia hallitaan ja niiden vaikutusta lievennetään.

Reagointi digitaalisen turvallisuuden poikkeamatilanteisiin tapahtuu useimmiten joko teknisin välinein havaitun tai käyttäjien ilmoittamien poikkeamien seurauksena.

Reagoinnin osalta on tärkeää, että mahdollisia poikkeamatilanteita on pohdittu jo etukäteen ja niihin liittyvät suunnitelmat viestinnästä, palautumisesta ja jatkuvuudesta on ajan tasalla sekä tarpeellisten henkilöiden tiedossa.

Yhtenä osana poikkeamatilanteisiin reagointia on tilanteen analysointi ja poikkeamaan johtaneiden syiden selvittäminen sekä tarvittavien korjaustoimenpiteiden tekeminen.

Poikkeamatilanteisiin reagointia on suositeltavaa harjoitella säännöllisin väliajoin joko järjestämällä sisäisiä ja kohdennettuja harjoituksia tai osallistumalla ulkopuolisen tahon järjestämään harjoitukseen.

2.6 Palautuminen - Kuinka pystymme jatkamaan toimintaamme

Palautumisvaiheen tavoitteena on, että organisaatiolla on kyvykkyys toipua digitaalisen turvallisuuden aiheuttamista häiriöstä takaisin normaaliin toimintatilaan. Käytännössä tämä tarkoittaa kriittisten suojattavien järjestelmien toipumissuunnitelmien luontia ja kehittämistä häiriötilanteista toipumisesta saatujen kokemusten perusteella sekä suunnitelmien tekoa mahdollisten digitaalisen turvallisuuden häiriöstä aiheutuvien mainehaittojen korjaamiseksi.

Toiminnalliseen palautumiseen liittyvät toimenpiteet toimivat lisäksi syötteenä jatkuvalle parantamiselle, eli uusien vaatimusten, tarpeiden ja kyvykkyyksien **tunnistamiselle** (vaihe 1).

3 Digitaalisen turvallisuuden arviointi

3.1 Tietoturva-auditointimenetelmät

Tämä dokumentti kokoaa yhteen yleisimmät tietoturva-auditoinnin viitekehykset ja menetelmät sekä antaa käytännön ohjeet, miten valita sopiva yhdistelmä hallinnollisen ja teknisen tietoturvan varmentamiseen. Painotus on auditointikäytännöissä: mitä oikeasti tarkastetaan, millä todisteilla ja millä työkaluilla.

Mitä tietoturva-auditointi käytännössä tarkoittaa

Auditointi voi tarkoittaa hyvin eri asioita. Käytännössä se jakautuu kolmeen kysymykseen:

1) Onko vaadittu johtamis- ja ohjausjärjestelmä olemassa? (hallinnollinen tietoturva)

2) Toteutuvatko kontrollit arjessa ja ovatko ne mitattavasti toimivia? (operatiivinen toiminta)

3) Onko tekninen toteutus ja konfiguraatio linjassa vaatimusten kanssa? (tekninen tietoturva)

Hyvä auditointi yhdistää sekä hallinnollisen että teknisen tietoturvan (mm. konfiguraatiot, lokit, testitulokset, haavoittuvuudet, kooditarkastukset).

Hallinnollinen vs. tekninen tietoturva

Hallinnollinen tietoturva tarkoittaa:

- Johtaminen, eri politiikat, vastuut, riskienhallinta, poikkeamien käsittely, jatkuvuus, toimittajahallinta, roolitukset, ohjeet, pöytäkirjat, toimittajasopimukset, jatkuvuussuunnitelmat, auditointiraportit

Tekninen tietoturva tarkoittaa:

- Konfiguraatiot, haavoittuvuuksien hallinta, identiteettien hallinta, verkkoratkaisu ja -segmentointi, lokitus, riittävät kovennukset, sovellusturva, varmistukset, haavoittuvuusskannaukset, penetraatio testaus -raportit

3.2 Viitekehykset ja standardit – mihin ne sopivat

Alla on kuvattuna keskeiset auditointimenetelmät ja missä roolissa niitä yleensä käytetään. Paras lopputulos syntyy lähes aina yhdistämällä johtamisjärjestelmä (esim. ISO 27001) ja tekninen kontrollikatalogi (esim. CIS Controls) sekä sovellusturvan vaatimuslista (OWASP ASVS).

ISO 27001

ISO 27001 on johtamisjärjestelmä ja se vaatii prosessit riskiperusteiseen tietoturvan hallintaan. Sopii erinomaisesti ulkoiseen sertifiointiin ja osoittaa, että tietoturvaa johdetaan hallitusti ja kun organisaatio haluaa systemaattisen hallintamallin (roolit, riskit, parantaminen) ja/tai sertifioinnin.

ISO/IEC 27002 on liite ISO 27001 -standardiin ja sen avulla voidaan tarkistaa, että tietoturvakontrollit (organisatoriset, henkilöstö, fyysiset, teknologiset) ovat riittävät ja se soveltuu erityisesti auditointikriteeriksi.

CIS (Critical Security Controls)

CIS on priorisoitu tekninen kontrollikatalogi käytännön kyberpuolustukseen (18 kontrollia) ja se soveltuu tilanteeseen, kun halutaan varmistaa, että ”onko konfiguraatio oikein ?” Se sisältää toteutus- ja toimenpidelistan tekniseen perusturvaan ja se sisältää myös konfiguraatiokovennusstandardit (käyttöjärjestelmä, pilvipalvelut, tietokannat, verkkolaitteet).

OWASP ASVS (Application Security Verification Standard)

OWASP ASVS on sovellusturvan vaatimus- ja auditointistandardi, joka määrittelee mitattavat ja todennettavat turvallisuusvaatimukset sovelluksille niiden kriittisyyden mukaan (tasot L1–L3).

Sitä käytetään käytännössä kehityksen, testauksen ja auditoinnin yhteisenä kriteeristönä, esimerkiksi hankintavaatimuksena, penetraatiotestauksen pohjana ja DevSecOps hyväksymiskriteeristönä.

NIST SP 800-53

NIST SP 800-53 on laaja ja yksityiskohtainen tietoturva- ja tietosuojakontrollien viitekehys, joka kattaa hallinnolliset, tekniset ja operatiiviset kontrollit erityisesti korkean varmuuden ja viranomaisympäristöihin.

Sitä käytetään käytännössä järjestelmien turvallisuusvaatimusten määrittelyyn, auditointiin ja jatkuvaan valvontaan, usein yhdessä riskiluokituksen ja baseline-ajattelun kanssa.

4 Lisätietoja

Mikäli haluat tutustua tarkemmin digitaalisen turvallisuuden arkkitehtuurin viitekehykseen, tutustuthan sekä Digi- ja väestötietoviraston laatimaan julkiseen Confluence -työtilaan ja eOppiva-kurssiin digitaalisen turvallisuuden arkkitehtuurista ja sen hyödyntämisestä organisaatiossa.

Arkkitehtuurikilta 30.3.2026

Työtila: Digitaalisen turvallisuuden arkkitehtuuri - Digitaalisen turvallisuuden arkkitehtuurin julkinen dokumentaatio - DVV external Confluence

Löydät kurssiin eOppivasta: Mitä on digitaalisen turvallisuuden arkkitehtuuri? - Digitaalinen turvallisuus järjestykseen arkkitehtuurin avulla (eoppiva.fi)