VALTIOVARAINMINISTERIÖ

Selvitys digitaalisen turvallisuuden kansainvälisestä arviointilainsäädännöstä

3.9.2021

Sisällys

TIIVISTELMÄ

Tässä digitaalisen turvallisuuden kansainvälisen arviointilainsäädännön selvityksessä on koottu yhteen tietoa digitaalisen turvallisuuden tarkastusjärjestelyistä, akkreditointikäytännöistä, lainsäädännöstä ja standardeista valituissa maissa.

Digitaalinen turvallisuus kattaa tässä asiayhteydessä riskienhallinnan, jatkuvuudenhallinnan ja varautumisen, tietoturvallisuuden, kyberturvallisuuden ja tietosuojan. Verrokkivaltioksi valittiin Tanska, Ruotsi, Viro, Saksa, Alankomaat ja Singapore. Tietoa digitaalisen turvallisuuden arviointilainsäädännöstä, toiminnan organisoinnista ja arviointikriteeristöistä kerättiin verrokkivaltioiden julkisista dokumenteista ja muista lähteistä. Selvityksen on laatinut työryhmä, johon kuuluivat erityisasiantuntija Niko Mäkilä ja tietohallintoneuvos Tuija Kuusisto ja valtiovarainministeriöstä sekä KPMG:n konsultteja.

Digitaalisen turvallisuuden varmistamiseksi EU-valtioissa on yhteisiä käytäntöjä, kuten yleinen tietosuoja-asetus (GDPR[1], General Data Protection Regulation), verkko- ja tietoturvadirektiivi (NIS[2], Directive on security of network and information systems sekä sen uudistettu ehdotus NIS 2[3]), akkreditointi- ja markkina-valvonta-asetus (NLF[4], New Legislative Framework) sekä kyberturvallisuus-asetus[5]. Yleisessä tietosuoja-asetuksessa asetetaan yrityksille ja organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat tarkat vaatimukset. NIS 2-direktiiviehdotuksella otetaan käyttöön tiukempia valvontatoimenpiteitä kansallisille viranomaisille sekä säädetään tiukemmista toimeenpanovaatimuksista julkishallinnolle. NLF-asetuksella on säädetty akkreditointitoiminnasta ja markkinavalvonnan vaatimuksista Euroopan unionin tasolla, mukaan lukien kansallisten akkreditointielimien velvollisuudet tehtävissään. NLF-asetusta ei sovelleta kansallisen turvallisuuden piiriin kuuluviin asioihin, kuten esimerkiksi turvallisuusluokiteltua tietoa käsittelevien kohteiden arviointiin. EU:n kyberturvallisuusasetuksella luodaan uusi EU:n laajuinen tieto- ja viestintähyödykkeiden sertifiointijärjestelmä ja tuodaan käyttöön yhteiset kyberturvallisuusvaatimukset ja arviointiperusteet.

Tämä selvitys on toteutettu tutkien verrokkivaltioiden julkisia lähteitä ja keskittyen pääosin tietoturvallisuuden hallintajärjestelmien arviointiin. Hallinnollisen tietoturvan osalta verrokkivaltioiden digitaalisen turvallisuuden arviointilainsäädäntö ei ole kovin yhtenäinen. Valtion virastojen ja kriittisen infrastruktuurin toimijoiden tietoturvallisuuden säännöllistä tarkastamista suositellaan kaikissa verrokkimaissa, mutta tarkastuksen toteutuskäytäntö vaihtelee. Säännöllistä auditointia edellytetään määrävälein Virossa, Saksassa ja Singaporessa, kun taas Tanskassa, Ruotsissa ja Alankomaissa määrävälein toteutettuja auditointeja ei edellytetä.

Verrokkimaissa käytetään kansainvälisiä digitaalisen turvallisuuden standardeja. ISO 27001 -standardia käytetään tietoturvan hallintajärjestelmien toteuttamisessa ja ISO 17021-1 -standardi asettaa vaatimuksia tietoturvallisuuden arviointilaitosten akkreditointiprosessiin. Joissakin maissa on myös

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1614339830925
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823
[4] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32008R0765
[5] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A52017PC0477R%2801%29

kehitetty omia standardeja digitaalisen turvallisuuden varmistamiseksi. Saksassa on kehitetty tietoturvan hallintajärjestelmänä BSI IT-Grundschutz, joka kattaa tekniset ja organisatoriset sekä infrastruktuuriin ja henkilöstöön liittyvät näkökulmat. Viro on ottanut mallia Saksan IT-Grundschutzista ja se on laatinut oman ISKE-tietoturvastandardinsa. Lisäksi Singaporessa on kehitetty monitasoinen pilviturvallisuusstandardi, MTCS, jossa määritetään kolme erilaista tietoturvasertifikaatin tasoa pilvipalvelujen pääryhmille.

Hallinnollisen tietoturvan näkökulmasta kaikille valtioille yhteisiä menettelyjä on vähän eikä ole sellaista yleistä menettelyä, jota kansainvälisesti noudatettaisiin. Digitaalisen turvallisuuden merkitys on kuitenkin laajasti tunnistettu kaikissa verrokkivaltioissa, ja näin ollen kaikilla olisi opittavaa toisiltaan. Kun arviointilaitoksen hyväksyntäprosessissa edellytetään arviointilaitoksen henkilöstöltä ammattitaitoa ja luotettavuutta, henkilösertifiointi voisi tässä olla yksi tapa osoittaa hallinnollisen tietoturvan todennusosaamista. Myös Suomessa tietoturvallisuuden arvioinnissa tulisi hyödyntää olemassa olevia kansallisia standardeja täydentämällä kansainvälisillä standardeilla. Koska tällä hetkellä Suomessa kansallisten tietojärjestelmien ja tietoliikenneratkaisujen arviointi perustuu enimmäkseen vapaaehtoisuuteen, digitaalisen toimintaympäristön turvallisuuden takaamiseksi arviointikäytäntöä pitäisi parantaa vastaamaan kansainvälistä tasoa. Arviointia siis tulisi tehdä säännöllisesti, esimerkiksi vuosittain.

Teknisen tietoturvan arvioinnista ei löytynyt materiaalia eikä verrokkivaltioiden tilanteita voi verrata Suomeen. Yleisiä teknisen tietoturvan viitekehyksiä ei ole tunnistettu tässä selvityksessä. On kuitenkin tiedossa, että eri toimijat ovat asettaneet vaatimuksia ja arviointimenettelyjä omaan toimintaansa liittyvien tietojärjestelmien teknisen tietoturvallisuuden toteuttamiseen ja arviointiin.

1 VERROKKIVALTIOIDEN ANALYYSI

Teknisen tietoturvan arviointiin liittyvistä käytännöistä saatiin tietoja vain rajoitetusti, minkä takia selvityksen näkökulma painottuu hallinnollisen tietoturvan arviointiin. Kansainvälisen turvallisuusluokitellun tiedon suojausten arvioinnista on esimerkiksi EU:lla ja Natolla omaa sääntelyään, joka koskee näiden yhteisöjen jäseniä. Tässä selvityksessä ei ole keskitytty kansainvälisen turvallisuusluokitellun tiedon suojausten arviointiin.

1.1 EU-lainsäädäntö

Yleisessä tietosuoja-asetuksessa asetetaan yrityksille ja organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat tarkat vaatimukset. GDPR koskee kaikkia EU:n alueella toimivia organisaatioita sekä kaikkia EU:n ulkopuolella toimivia organisaatioita, jotka tarjoavat tavaroita tai palveluja asiakkaille tai yrityksille EU:ssa. Asetuksen mukaan organisaation on nimettävä tietosuojavastaava, kun se kerää tai käsittelee henkilötietoja säännöllisesti. Tietosuojavastaavalla on vastuu varmistaa tämän asetuksen ja muiden tietosuojalainsäädäntöjen tai henkilötietojen käsittelijän toimintamenettelyjen noudattamista.

EU:n yhteisen korkean kyberturvatason varmistamiseksi on ehdotettu NIS 2 -direktiivi joulukuussa 2020. Ehdotuksella mm. uudistetaan verkko- ja tietojärjestelmien turvallisuutta koskevia sääntöjä, otetaan käyttöön tiukempia valvontatoimenpiteitä kansallisille viranomaisille ja tiukennetaan toimeenpanovaatimuksia kaikissa jäsenvaltioissa. Lisäksi ehdotetulla direktiivillä laajennetaan kriittisiä infrastruktuureja koskevan direktiivin soveltamisalaa, johon kuuluu uutena myös julkishallinto. Julkishallinto kuuluu soveltamisalan keskeisiin sektoreihin ja se voi tarkoittaa seuraavia:

— keskushallintojen julkiset toimijat

— asetuksen (EY) 1059/200327 liitteessä I lueteltujen NUTS 1 -tason (Nomenclature of Territorial Units for Statistics) alueiden julkishallinnon toimijat

— asetuksen (EY) 1059/200327 liitteessä I lueteltujen NUTS 2 -tason alueiden julkishallinnon toimijat

— asetuksen (EY) 1059/2003 liitteiden II ja III mukaan Suomessa luokitustasoihin kuuluisivat valtionhallinto ja sen alaiset valtakunnalliset virastot ja laitokset sekä maakunnat, hyvinvointialueet ja kunnat

Uuden ehdotuksen nojalla jäsenvaltioiden on nimettävä yksi tai useampi kyberturvallisuuden alalla toimivaltainen kansallinen viranomainen direktiivin mukaisia valvontatehtäviä varten sekä kyberturvallisuuden kansallinen keskitetty yhteyspiste, joka vastaa koordinoinnista jäsenvaltioiden rajat ylittävän viranomaisyhteistyön ja viestinnän varmistamiseksi. Lisäksi ehdotuksen mukaan jäsenvaltioiden tulee laatia kansalliset kyberturvallisuusstrategiat sekä vahvistaa valvontaviranomaisten tehtäviä ottaen käyttöön ehdotuksessa esitettyjä riskienhallintatoimia.

Ehdotuksessa säädetään kansallisten viranomaisten tiukemmista valvontatoimenpiteistä ja keskeisten toimijoiden tiukemmista toimeenpanovaatimuksista. Kyseisillä viranomaisilla tulee olla valtuudet kohdistaa asianomaiset toimijat säännöllisiin kohdennettuihin tarkastuksiin, paikan päällä tehtäviin tarkastuksiin ja toimipaikkojen ulkopuoliseen jälkikäteiseen valvontaan, mukaan lukien satunnaiset tarkastukset sekä tietojen, asiakirjojen tai minkä tahansa valvontatehtäviensä kannalta välttämättömien tietojen hankkimiseen. Ehdotuksessa myös esitetään hallinnollisia sanktioita toimijan velvoitteiden laiminlyönnistä.

Ehdotus edellyttää haavoittavuuksien systemaattista tunnistamista, jolloin toimijan haavoittuvuuksista tulee ilmoittaa CSIRT-toimijalle (Computer Security Incident Response Teams). Riskienhallintatoimen kehittämiseksi ja viestintäverkon turvallisuuden varmistamiseksi ehdotus korostaa päästä päähän salauksen kehitystä. Lisäksi ehdotus on yhdenmukainen myös joulukuussa 2020 ehdotetun CER-direktiivin (Critical Entities Resilience) kanssa, jonka tarkoituksena on parantaa Euroopan unionin kannalta välttämättömien palvelujen häiriönsietokykyä sekä ylläpitää yhteiskunnan kriittisiä ja taloudellisia toimintoja. Kaikkiin CER-direktiiviehdotuksen nojalla yksilöityihin kriittisiin yhteisöihin sovelletaan kyberresilienssin velvoitteita NIS 2 -direktiiviehdotuksen mukaisesti.

NLF-asetuksella (akkreditointi ja markkinavalvonta-asetus (EY) N:o 765/2008) on säädetty akkreditointitoiminnasta ja markkinavalvonnan vaatimuksista Euroopan unioin tasolla. Asetuksen nojalla jäsenvaltioilla tulisi olla vain yksi kansallinen akkreditointielin ja niiden olisi huolehdittava kyseisen elimen toiminnan objektiivisuudesta ja puolueettomuudesta. Kansallisten akkreditointielinten toiminnan riippumattomuuden varmistamiseksi asetuksessa on säädetty, että jäsenvaltiot ovat velvollisia varmistamaan sen, että kansallinen akkreditointielin katsotaan julkiseksi viranomaiseksi sen juridisesta asemasta riippumatta. Asetusta ei kuitenkaan sovelleta kansallisen turvallisuuden piiriin liittyviin asioihin, kuten turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien arviointitoimintaan.

Asetuksen 5 artiklan 1 kohdan mukaan kansallisen akkreditointielimen on annettava arvio vaatimustenmukaisuuden arviointilaitoksen pätevyydestä tietyn vaatimustenmukaisuuden arviointitehtävän suorittamiseen. Päteväksi osoitetulle laitokselle myönnetään akkreditointitodistus ja asetuksen 5 artiklan 3 kohdan mukaan kansallisten akkreditointielinten on myös valvottava kaikkia niitä vaatimustenmukaisuuden arviointilaitoksia, joille akkreditointitodistus on myönnetty.

Vuonna 2019 voimaantullut EU:n kyberturvallisuusasetus vahvistaa Euroopan verkko- ja tietoturvaviraston (ENISA, European Union Agency for Cybersecurity) roolia EU:n laajuisen kyberturvallisuuden kehittämisessä sekä luo uuden EU:n laajuisen tieto- ja viestintähyödykkeiden sertifiointijärjestelmän. Sertifiointijärjestelmä tunnistetaan kaikissa jäsenvaltioissa ja sen avulla varmistetaan hyödykkeiden vaatimusten täyttäminen esimerkiksi liittyen tiedon, toiminnon tai palvelun saatavuuteen, eheyteen ja luottamuksellisuuteen. ENISA toimii EU-tason toimivaltaisena elimenä ja täten sillä on tärkeä rooli sertifiointijärjestelmän koordinointityössä. Sertifiointijärjestelmän avulla hyödykkeiden valmistajat tai tarjoajat voivat hakea sertifiointia vaatimustenmukaisuuden arviointilaitoksen kautta. Asetuksen mukaan arviointilaitos voi esimerkiksi olla juridisesti riippumaton yksityinen yritys, ja sen hyväksyy kansallinen akkreditointielin NLF-asetukseen nojaten.

Kyberturvallisuusasetuksen avulla myös tuodaan käyttöön yhteiset kyberturvallisuusvaatimukset ja arviointiperusteet ja siten vältetään sertifiointijärjestelmien ja niihin liittyvien turvallisuusvaatimuksien ja arviointiperusteiden hajanaisuutta jäsenvaltioissa ja eri kriittisten infrastruktuurien aloilla. Asetuksen mukaan jäsenvaltioiden on nimettävä yksi valvontaviranomainen, joka valvoo vaatimustenmukaisuuden arviointilaitosten ja niiden myöntämien sertifikaattien vaatimustenmukaisuutta kyberturvallisuusasetuksen sekä EU:n sertifiointijärjestelmien nojalla. Suomessa Traficom on sekä toimivaltainen viranomainen että valvontaviranomainen. Asetusta ei varsinaisesti tarvitse erikseen implementoida osaksi kansallista lainsäädäntöä. Suomessa asetusta ei ole pantu vielä kansallisesti täytäntöön.

1.2 Maakohtaiset analyysit

1.2.1 Tanska

Datatilsynetillä eli Tanskan tietosuojaviranomaisella on valtuudet auditoida viranomaisia ja yksityisiä yrityksiä sekä suorittaa tutkimuksia rekisterinpitäjän tai -käsittelijän tietosuojalainsäädännön noudattamisesta. Tanskan digitalisaatioviraston (Digitaliseringsstyrelsen) kyber- ja tietoturvallisuusosasto vastaa mm. julkisen sektorin tietoturvaan liittyvien oikeudellisten vaatimusten, standardien, sekä GDPR- ja eIDAS-säädösten (electronic identification, authentication and trust services eli sähköisen tunnistatutumisen palvelut) noudattamiseen liittyvistä kysymyksistä. Lisäksi Tanskan valtiontalouden tarkastusvirasto (Rigsrevisionen) tarkastaa valtion viranomaisten tietoturvajärjestelmiä. Esimerkiksi, vuonna 2016 tarkastusvirasto on arvioinut, miten Tanskan viranomaiset ovat hallinneet ulkopuolisille toimittajille ulkoistettuja tietoturvajärjestelmiä ja antanut arvioinnin perustella suosituksia asian hallitsemiseen. Myös tarkastusviraston vuonna 2017 tekemässä auditoinnissa tarkastettiin, oliko valituilla keskeisillä valtion laitoksilla tyydyttävä suoja kiristyshaittaohjelmia (ransomware) vastaan.

Tanskassa valtionvarainministeriön tarkastus- ja valvontatoimisto (Kontor for Revision og Tilsyn) arvioi IT:n valvonnan avulla, hoidetaanko ministeriön tietoturvallisuuden hallintaa asianmukaisesti. Toimisto suorittaa myös IT:n valvontaa valtion IT-palveluiden viraston kanssa virastojen asiakkaiden puolesta. Lisäksi toimisto neuvoo Tanskan valtiontalouden tarkastusviraston tarkastettavina olevia yksiköitä, jolloin se myös vastaa viestintä- ja koordinointitehtävästä tarkastusviraston kanssa. Toimisto laatii vuosikertomuksen ja antaa tietoa meneillään olevista tietoturvan valvontatoimista. Lisäksi se julkaisee vuosittain IT-valvontakertomuksen valtion IT-palveluiden virastosta. Tanskan kansallisena tietoturvaviranomaisena toimii kyberturvallisuuskeskus (The Danish Centre for Cybersecurity).

Den Danske Akkrediteringsfond (DANAK) toimii Tanskan akkreditointielimenä ja sillä on sopimus Tanskan turvallisuustekniikan viranomaisen (Sikkerhedsstyrelsen) kanssa akkreditointitehtävien suorittamisesta. Tanskassa akkreditointi perustuu EU:n asetukseen ja se myönnetään yleensä neljäksi vuodeksi. Akkreditointivaatimukset tietoturvan hallintajärjestelmien (ISMS, Information Security Management System) sertifiointiin on määritetty seuraavissa standardeissa:

— DS/EN ISO/IEC 17021-1:2015, ’Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements’ 4th edition 2015-07-30,

— DS/ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems.

Hallinnollisesta näkökulmasta Tanskassa ei ole lainsäädäntöä, joka vaatisi vuosittaista tietoturvallisuuden tarkastamista. Kyberturvallisuuskeskuksen tehtäviin kuuluu kyberturvallisuuden käytäntöjen noudattamisen seuranta, mutta vuotuista tarkastusta ei kuitenkaan vaadita erikseen. Tietoturvastandardin osalta on säädetty niin, että, kaikkien valtion viranomaisten on noudatettava ISO/IEC 27001-standardia tammikuusta 2014 lähtien. Tietoturvallisuutta koskevan yhteistyön tukemiseksi valtion IT-neuvosto on perustanut tietoturvafoorumin (GISF, Government Information Security Forum), johon osallistuu noin kolmekymmentä valtion laitosta. Foorumi kokoontuu neljästä kuuteen kertaa vuodessa.

NIS-direktiivin mukainen keskitetty kansallinen yhteyspiste Tanskassa on kyberturvallisuuskeskus. Toimivaltaisina kansallisina viranomaisina toimivat Tanskan yritysviranomainen, Tanskan energiavirasto, Tanskan liikenne-, rakennus- ja asuntovirasto, Tanskan merenkulkuviranomainen, Tanskan finanssivalvontaviranomainen, Tanskan terveystietovirasto sekä ympäristö- ja elintarvikeministeriö.

1.2.2 Ruotsi

Ruotsin keskeiset viranomaiset, joille on määrätty digitaaliseen turvallisuuteen liittyviä vastuita, ovat varautumisesta ja kriisinhallinnasta vastaava turvallisuusvirasto Myndigheten för samhällsskydd och beredskap (MSB), tietosuojaviranomainen Datainspektionen ja valtionhallinnon digitalisointia koordinoiva Myndigheten för digital förvaltning (DIGG). MSB:n tietoturvaosasto vastaa kansalliseen tietoturvaan liittyvän työn tukemisesta ja koordinoinnista. Ruotsissakaan ei teknisen tietoturvan arviointilainsäädännöstä ei löytynyt tietoa mutta yksittäisillä toimijoilla voi olla omia tietoteknisiä ratkaisuja koskevia ohjeita, esimerkiksi Ruotsin puolustusvoimien (Försvarsmakten) tietoturvallisuutta koskeva ohje (Krav på IT-säkerhetsförmågor hos IT-system, KSF[6]).

Ruotsin akkreditointielimenä toimiva Styrelsen för ackreditering och teknisk kontroll (SWEDAC) koordinoi markkinavalvontaa Ruotsissa ja sen toimintaa säätelevät hallituksen antamat ohjeet sekä lainsäädäntö ja kansainväliset sopimukset. Yleiset akkreditointivaatimukset tietoturvan hallintajärjestelmien sertifiointiin on määritetty standardissa ISO/IEC 17021-1:2015.

MSB:n vuoden 2009 määräykset[7] valtion virastojen tietoturvasta tukevat häiriöiden torjuntatoimenpiteiden säännöllistä tarkastusta ja seurantaa. Tarkastusta ei kuitenkaan tarvitse suorittaa tietyn aikataulun mukaisesti. Julkisissa ja yksityisissä hankintaprosesseissa tunnustetaan kansainväliset tietoturvasertifikaatit. Vaikka joitain kansallisia tietoturvallisuusohjeita on kehitetty, ne eivät vaadi ylimääräistä kansallista sertifikaattia tai akkreditointia.

[6] http://isd.fmv.se/Documents/krav-pa-godkanda-sakerhetsfunktioner-version-3-1.pdf
[7] https://rib.msb.se/filer/pdf/25357.pdf

Turvallisuuteen liittyvien arkaluonteisten toimintojen suojelemiseksi Ruotsissa on kehitetty turvasuojelulaki (Säkerhetsskyddslag (2018:585)[8], Protective Security Act, (PSA)) ja -asetus (Säkerhetsskyddsförordning (2018:658)[9], Protective Security Regulation (PSR)), jotka tulivat voimaan huhtikuussa 2019. Turvallisuuteen liittyvä toiminta on tässä asiayhteydessä toimintaa, jolla on merkitystä Ruotsin valtion turvallisuudelle tai johon sisältyy valtiota sitova kansainvälinen turvasitoumus. Lainsäädäntöä sovelletaan sekä julkisiin että yksityisiin organisaatioihin, myös ei-ruotsalaisiin organisaatioihin.

PSA:lla pyritään estämään vakoilua, sabotaasia, terrorismia ja muita kansalliseen turvallisuuteen kohdistuvia rikoksia. Tämän lain noudattamiseksi organisaatioiden tulee mm. suorittaa analyysi turvasuojelusta, toteuttaa tämän analyysin pohjalta suojausmenetelmät, jotka kattavat tietoturvan ja fyysisen turvallisuuden, sekä suorittaa henkilöstöturvallisuusarviointi ennen turvatoimesta vastaavan henkilön palkkaamista. PSA luokittelee turvallisuudelle arkaluontoiset toimet seuraavasti:

- Luokiteltu (erittäin salainen): Sisältää poikkeuksellisen vakavien vahinkojen riskin,
- Salainen: Sisältää vakavien vahinkojen riskin,
- Luottamuksellinen: Sisältää merkittävien vahinkojen riskin,
- Rajoitettu: Sisältää pienten vahinkojen riskin.

Lisäksi asetus kriisivalmiudesta ja valvonnasta vastaavien viranomaisten toimenpiteistä lisääntyneen varautumisen yhteydessä (Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap[10]) sisältää valtion viranomaisiin sovellettavia tietoturvan säännöksiä, esimerkiksi turvatoimia sekä tapahtumista ilmoittamista MSB:lle. Jokainen viranomainen on vastuussa omien turvatoimiensa toteuttamisesta. Ruotsissa kiristettiin myös verkkoturvallisuutta koskevaa lainsäädäntöä vuoden 2020 alusta vastaamaan kriittisen infrastruktuurin, erityisesti 5G-verkon turvallisuusvaatimuksia.

Ruotsin valtiontalouden tarkastusviraston (Riksrevisionen) vuonna 2019 tekemässä auditoinnissa tarkasteltiin vanhentuneita IT-järjestelmiä tehokkaan digitalisoinnin toteuttamisen näkökulmasta. Tarkastuksen tarkoituksena oli tutkia vanhentuneiden IT-järjestelmien vaikutusta valtionhallinnossa ja arvioida olivatko viranomaiset, ja hallitus toteuttaneet sopivia toimenpiteitä varmistaakseen, etteivät nämä järjestelmät muodostu tehokkaan digitalisoinnin esteiksi. Lisätietoja muista julkishallinnon digitaalisen turvallisuuden arviointiorganisaatioista ei ole löytynyt.

Ruotsissa MSB toimii NIS-direktiivin mukaisena keskitettynä kansallisena yhteyspisteenä. Toimivaltaisina kansallisina viranomaisina toimivat Posti- ja televiestintäviranomainen (Post- och telestyrelsen, PTS), Energiavirasto (Energimyndigheten, STEM), Liikennevirasto (Transportstyrelsen, TS), Finanssivalvontaviranomainen (Finansinspektionen, FI), Terveyden ja sosiaalihuollon tarkastuslaitos (Inspektionen för vårdochomsorg, IVO) sekä Elintarvikevirasto (Livsmedelsverket, SLV).

[8] http://rkrattsbaser.gov.se/sfst?bet=2018:585
[9] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddsforordning-2018658_sfs-2018-658
[10] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20151052-om-krisberedskap-och_sfs-2015-1052#:~:text=I%20f%C3%B6rordningen%20(2015%3A1053),som%20d%C3%A5%20omedelbart%20ska%20till%C3%A4mpas.

1.2.3 Viro

Talous- ja viestintäministeriöön kuuluvalla tietohallintotoimistolla (Government CIO Office) (entinen valtion tietojärjestelmäosasto, RISO) on tärkeä rooli Viron tietoyhteiskuntapolitiikan suunnittelussa. Se kehittää tietoyhteiskunnan toimintaa ja valmistelee lakiluonnoksia IT-alalla. Valtion tietohallintotoimiston strategisiin tehtäviin kuuluu valtion tietoturvan hallintajärjestelmien tehtävien ja kehittämissuunnitelmien koordinointi IT-politiikan mukaisesti. Lisäksi tehtäviin kuuluvat: IT-budjetointi, lainsäädäntö, projektit, arvioinnit, standardointi, hankintamenettelyt sekä kansainvälinen yhteistyö. Vuonna 2018, luotiin Government Cloud -alusta julkishallinnon IT-palveluiden hallitsemiseksi ja tarkastamiseksi.

Viron akkreditointielimenä toimii Eesti Standardimis- ja Akrediteerimiskeskus (EVS). Yleiset akreditointivaatimukset tietoturvan hallintajärjestelmien sertifiointiin on määritetty standardissa ISO/IEC 17021-1:2015.

Viro on ottanut mallia Saksan IT-Grundschutzista, kun se on laatinut oman ISKE-tietoturvastandardinsa. ISKE-tietoturvastandardin toteutuksen tavoitteena on varmistaa julkisen sektorin tietojärjestelmissä käsiteltävien tietojen riittävä tietoturvataso. Standardissa luokitellaan kolmea suojaustasoa (H, M, L) kolmen tekijän perusteella: tietojen saatavuus, eheys ja luottamuksellisuus. Tarkastuksista on säädetty, että ministeriöt, virastot sekä valtion tietoturvaan liittyvät rekisterinpitäjät ovat velvollisia suorittamaan tarkastuksen seuraavasti:

- H-taso: 2 vuoden välein,
- M-taso: 3 vuoden välein,
- L-taso: 4 vuoden välein,
- paikallishallinnon tarkastuksia tehdään epäsäännöllisesti.

Uusi Estonian Information Security Standard (E-ITS) korvaa ISKEn vuoden 2022 aikana[11]. ISKE on käytössä vuoden 2023 loppuun asti.

Vuonna 2008 voimaan tullut asetus[12] tietojärjestelmien turvatoimenpiteiden järjestämisestä yllä mainitut standardit edellyttävät, että valtion turvallisuuden hallintajärjestelmän pääarvioijalla (lead auditor) tulee olla voimassa oleva tietoturvallisuuden tarkastuksen sertifikaatti, riittävä osaaminen sekä tarkastuskokemusta. Uuden E-ITS-tietoturvastandardin mukaan hyväksyttyjä sertifikaatteja ovat ISACA-yhdistyksen myöntämä Certified Information Systems Auditor (CISA) sekä ISO 27001 Lead Auditor Certificate, jonka on myöntänyt joko IRCA (International Register of Certificated Auditors) tai PECB (Professional Evaluation and Certification Board). Auditointien teknisiltä arvioijilta edellytetään vähintään kahden vuoden kokemusta IT-auditoinneista, järjestelmänhallinnasta tai tietoturvallisuudesta. Teknisen tietoturvan tarkastamiseen liittyvästä osaamisesta ei ole annettu yksityiskohtaisia vaatimuksia[13].

[11] https://www.ria.ee/en/cyber-security/estonian-information-security-standard.html
[12] https://www.ria.ee/sites/default/files/content-editors/ISKE/regulation-the-system-of-security-measures-for-information-systems-2007-12-20.pdf
[13] https://eits.ria.ee/et/versioon/2020vers1/standardi-dokumendid/auditeerimisjuhend-kavand/#8noudedeitsaudiitorile8

Viron valtiontalouden tarkastusviraston (Riigikontroll) vuonna 2018 suorittamassa auditoinnissa tarkastettiin, kuinka valtio oli määrittänyt, mitkä tiedot ja tietokannat olivat kriittisiä kansallisen turvallisuuden takaamiseksi. Näiden tietojen ja tietokantojen turvallisuuden ja jatkuvuuden suojaamista myös tarkastettiin, mukaan lukien yleiskatsaus suojauksessa käytetyistä työkaluista. Lisätietoja muista julkishallinnon digitaalisen turvallisuuden arviointiorganisaatioista ei ole löytynyt.

Tietojärjestelmäviranomainen Riigi Infosüsteemi Amet (RIA) toimii NIS-direktiivin mukaisena keskitettynä kansallisena yhteyspisteenä sekä toimivaltaisena kansallisena viranomaisena.

1.2.4 Saksa

Kyberturvallisuus on monesta muusta viranomaistoiminnasta poiketen keskitetty Saksassa liittovaltion eikä osavaltioiden viranomaisille. Liittovaltion tietotekniikkavirasto (Bundesamt für Sicherheit in der Informationstechnik, BSI). BSI vastaa kriittisen infrastruktuurin operaattoreita ja digitaalisten palvelujen tarjoajia koskevien säännösten täytäntöönpanosta.

Henkilötietojen käsittelyn turvallisuusvaatimusten valvontaa tekevät Saksassa useat viranomaiset, joilla on erilaisia pätevyyksiä. Saksassa jokaisen osavaltion valvontaviranomainen (Landesbeauftragter für den Datenschutz, LfD) on yhdessä liittovaltion viranomaisen (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI) kanssa ensisijaisesti vastuussa GDPR:n vaatimusten täytäntöönpanosta.

Saksassa on BSI:n johdolla kehitetty viranomaisten ja yritysten tietoturvan hallintamenettely IT-Grundschutz, joka kattaa tekniset ja organisatoriset sekä infrastruktuuriin ja henkilöstöön liittyvät näkökulmat. IT-Grundschutz tarjoaa järjestelmällisen lähestymistavan tietoturvaan. IT-Grundschutz-menettelyn mukainen sertifiointi perustuu BSI-standardeihin, jotka puolestaan ovat yhteensopivat kansainvälisten ISO-standardien kanssa. BSI:n sertifioimana tietoturvapalvelujen tarjoajana toimii mm. TÜV Informationstechnik GmbH (TÜViT). Se tukee yrityksiä ja viranomaisia tietoturvan hallintajärjestelmän suunnittelussa, toteuttamisessa, seurannassa sekä jatkuvassa parantamisessa ISO/IEC 27001 ja BSI-standardien mukaisesti.

Saksassa organisaatioiden tulee tarkistaa tietoturvaohjelmansa säännöllisesti, varsinkin silloin, kun liiketoimintakäytännöissä, tietojärjestelmissä tai niiden uhkaavissa riskeissä tapahtuu merkittäviä muutoksia. BSI-lain (BSI Act of 2009 / BSI-Gesetz[14]) mukaan kriittisen infrastruktuurin toimijat, jotka toimivat esimerkiksi energia- tai liikennealalla, ovat velvollisia kahden vuoden välein osoittamaan tarkastuslaitokselle (BSI) auditointien, tutkimusten tai sertifikaattien avulla, että palvelut täyttävät Saksan tietoturva-asetuksen (IT-SiG[15]) vaatimukset.

Tällä hetkellä Saksassa ei ole velvoitetta hyväksyä kansainvälisiä standardeja, kuten ISO 27001:2013. Nämä standardit ovat kuitenkin laajalti tunnustettuja ja käytännössä hyväksyttyjä. BSI noteeraa ne

[14] https://www.bsi.bund.de/EN/TheBSI/BSIAct/bsiact_node.html
[15] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/it_sig_node.html

yleisiksi IT-turvallisuuden standardeiksi, ja vuonna 2017 päivitetyt BSI-standardit ovat sopusoinnussa ISO/IEC 27001-standardin kanssa. Arvioitaessa toimijan vaatimustenmukaisuutta BSI-standardien mukaan, BSI tarjoaakin mahdollisuutta sertifioitua myös kansainvälisten standardien mukaisesti.

Näiden standardien lisäksi useat lait säätelevät tietoturvaa ja asettavat niihin liittyviä standardeja Saksassa, mukaan lukien:

— Liittovaltion tietosuojalaki (Bundesdatenschutzgesetz, BDSG), joka suojaa henkilötietoja. Saksa päivitti lain vuonna 2017 vastaamaan EU:n yleistä tietosuoja-asetusta (asetus (EU) 2016/679) (GDPR).

— Tietoturvalaki (IT-Sicherheitsgesetz/ IT-SiG), joka vaikuttaa telepalveluihin, mukaan lukien verkkosivustot, sosiaalinen media ja muut verkkopalvelut, televiestintä ja muut kriittiset infrastruktuurialat, joita ovat esimerkiksi energia-ala, liikenneala, terveydenhuoltoala, vesihuoltoala, elintarvikeala, rahoitus ja vakuutusala. Keväällä 2021 tietoturvalakiin tehtiin merkittävä päivitys, joka lisää BSI:n valtuuksia, parantaa digitaalista kuluttajansuojaa, kasvattaa kriittisen infrastruktuurin operaattorien vastuuta ja vahvistaa valtion suojausroolia kriittisten komponenttien käytössä, sisältäen mahdollisuuden kieltää kriittiseksi määriteltyjen komponenttien käyttö Saksan tietoverkoissa tekniseen ja turvallisuuspoliittiseen riskiarvioon perustuen.

— Muut oikeudelliset järjestelmät, jotka suojaavat riskitietoja.

Saksan kansallisessa strategiassa kriittisen infrastruktuurin suojaamiseksi (2009) kriittiseen infrastruktuuriin on määritelty kuuluvan 1. energiahuolto, 2. tieto- ja viestintätekniikka, 3. liikenne, 4. juomavesi- ja jätevesihuolto, 5. terveydenhuolto, ravitsemus- ja elintarvikehuolto, 6. hätä- ja pelastuspalvelut sekä katastrofeihin varautuminen, 7. parlamentti, liittohallitus, hallinto, oikeuslaitos, 8. rahoitus- ja vakuutustoiminta sekä 9. media (joukkoviestimet) ja kulttuuriperintö. Kriittisen infrastruktuurin palvelujen turvaamiseksi Saksassa on perustettu julkisen ja yksityisen sektorin kumppanuushanke UP KRITIS, joka kokoaa yhteen kriittisen infrastruktuurin operaattorit ja järjestöt sekä vastuuviranomaiset. BSI on NIS-direktiivin mukainen keskitetty kansallinen yhteyspiste sekä toimivaltainen kansallinen viranomainen.

1.2.5 Alankomaat

Laki avoimesta hallituksesta (Wet Open Overheid) on Alankomaiden tiedonvapauslaki, joka säätelee hallitusta koskevien tiedustelupyyntöjen aktiivista julkaisemista ja käsittelyä. Jopa turvaluokitellut tiedot ovat avoimia pyynnöille, mutta tietojen salassapidon tarve punnitaan avoimuuden tarpeeseen nähden. Digitaalisen hallinnon laki (Wet Digitale Overheid) sisältää perusteet, jotka ovat välttämättömiä Alankomaiden eIDAS-järjestelmän kansallisen täytäntöönpanon kannalta, ja myös perustan julkisten IT-standardien hallitusten laajuiselle hyväksymiselle. Alankomaissa kaikilla sähköisen tunnistautumis- (Electronic Identification, eID) ja todentamisvälineiden tarjoajilla sekä teknisen infrastruktuurin välittäjillä tulee olla tietoturvan hallintajärjestelmä, joka kattaa sähköisen tunnistamisen

luottamuskehystä[16] koskevat vaatimukset ja sen on oltava määritetty ISO/IEC 27001 -standardin mukaisesti. Myös sertifioidulla organisaatiolla tai em. palveluntarjoajien hallinto-organisaatiolla on oltava kolmannen osapuolen lausunto, jolla on vastaava vaatimustenmukaisuustodistus riippumattomalta rekisteröidyltä sähköisen tietojenkäsittelyn tarkastajalta (Electronic Data Processing Auditor, EDP). Lisäksi valtioneuvoston päätös tietoturvasta (Special Information vuodelta 2013[17]) edellyttää jokaisen tietojärjestelmän suorittavan säännöllisiä tarkastuksia, mutta pakollista aikataulua ei kuitenkaan ole asetettu.

Baseline Informatiebeveiliging Overheid (BIO) sisältää tietoturvavaatimukset kaikille valtion elimille, sekä keskushallinnolle että paikallisille, ja perustuu vahvasti ISO 27000 -standardeihin. Keskushallinnossa VIR-asetus (Voorschrift Informatiebeveiliging Rijksdienst) keskushallinnon tietosuojasta antaa tietosuojavaatimukset ja VIRBI-asetus (Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie) keskushallinnon tietosuojasta asettaa turvallisuusluokiteltujen tietojen suojaamista koskevat vaatimukset. Kaikki tietoprosessit ovat luottamuksellisuuden, eheyden ja saatavuuden kattamia. Keskushallinnon yksiköt vastaavat riskienhallinnastaan, akkreditoinnista ja sisäisen valvonnan koordinoinnista.

Norea on Alankomaiden IT-tilintarkastajien ammattiliitto. Norea osallistuu moniin kansallisiin IT-asioita käsitteleviin komiteoihin, määrittelee käytännön tarkastusstandardeja sekä järjestää konferensseja ja työpajoja. Turvatarkastus ei kuitenkaan rajoitu Norean jäseniin tai rekisteröityihin EDP-tarkastajiin. Rekisteröityjä tilintarkastajia ei myöskään välttämättä tarkisteta ennakkoon. Joissakin virallisissa tehtävissä rekisteröityjen EDP-tilintarkastajien käyttö on pakollista, mutta useimmissa tapauksessa se ei ole.

Vuosina 2018-2020 Alankomaiden tilintarkastustuomioistuin (Algemene Rekenkamer) tarkasti kriittisten vesihuoltorakenteiden ja rajavalvonnan kyberturvallisuuden varmistamista ja toteuttamista. Lisätietoja muista julkishallinnon digitaalisen turvallisuuden arviointiorganisaatioista ei ole löytynyt.

NIS-direktiivin mukainen keskitetty kansallinen yhteyspiste Alankomaissa on Kansallinen kyberturvallisuuskeskus (NCSC, National Cyber Security Centre). Toimivaltaisina kansallisina viranomaisina toimivat Radio Communications Agency, Agentschap Telecom, De Nederlandsche Bank (DNB), Inspectorate Healthcare and Youth, Ministry of Infrastructure and Water Management sekä Directorate-General Water and Soil. Verkko- ja tietoturvatoimintaa koordinoi kansallinen terrorismin ja turvallisuuden koordinaattori (Dutch National Coordinator of Counterterrorism and Security, NCTV).

1.2.6 Singapore

Singaporessa kyberturvallisuusvirasto (the Cyber Security Agency of Singapore) ja Infocomm Media Development Agency (IDA) toimivat hallintoeliminä, jotka säätelevät ICT-alaa ja asettavat vaatimustenmukaisuuden arviointia koskevia erityisvaatimuksia. Singaporen valtiontalouden tarkastusvirasto (Auditor-General's Office Singapore) tarkastaa ministeriöt, valtioelimet ja muut viranomaiset,

[16] https://ec.europa.eu/cefdigital/wiki/download/attachments/74091935/Notification_Form_Dutch_Trust_Framework_for_Electronic_Identification%20with%20IDPs.pdf
[17] https://wetten.overheid.nl/BWBR0033507/2013-06-01

ja sillä on oma IT-auditointiosasto. CREST on voittoa tavoittelematon kansainvälinen organisaatio, joka akkreditoi ja myöntää sertifioinnin tietoturva-alan palveluntarjoajille. Tietoturva-alan ammattilaisten liitto (AISP) perusti CREST Singaporen vuonna 2016 Singaporen kyberturvallisuusviraston (CSA) tuella. Aloite kehitettiin yhteistyössä Singaporen rahaviranomaisen (MAS), Singaporen pankkiyhdistyksen (ABS) ja Singaporen Infocomm Media Development Agency (IDA) kanssa.

ISO 27001 -standardi soveltuu tietoturvan hallintajärjestelmiin. Lisäksi Singaporessa on kehitetty monitasoinen pilviturvallisuusstandardi (MTCS, Multi-Tier Cloud Security). Siinä määritetään kolme erilaista tietoturvasertifikaatin tasoa pilvipalvelujen kolmelle pääryhmälle, joita ovat infrastruktuuri palveluna (Infrastructure as a Service, IaaS), sovellusalusta palveluna (Platform as a Service, PaaS) sekä ohjelmisto palveluna (Software as a Service, SaaS). Singaporessa henkilötietosuojalaki (PDPA, Personal Data Protection Act) määrittelee valvontavaatimukset henkilötiedoille sekä täydentää mm. pankkilakia ja vakuutuslakia. PDPA sisältää määräykset henkilötietojen keräämisestä, käytöstä ja luovuttamisesta Singaporessa. Siinä säädetään myös kansallisen Do Not Call (DNC) -rekisterin perustamisesta, jonka mukaan henkilöt voivat rekisteröidä Singaporen puhelinnumeronsa DNC-rekisteriin, jotta he eivät saa organisaatioilta ei-toivottuja yhteydenottoja.

Singaporen valtiontalouden tarkastusviraston viimeisimmässä vuosikertomuksessa[18] (julkaistu syyskuussa 2020) havaittiin heikkouksia ja aukkoja useiden julkisyhteisöjen, kuten puolustusministeriön ja valtiovarainministeriön, IT-valvonnassa. Vuosikertomuksessa kävi ilmi, että kolmansien osapuolten käyttöoikeudet olivat löyhät ja pääkäyttäjätilien (ne, joilla on laajat käyttöoikeudet, kuten mahdollisuus tehdä muutoksia toimintalokeihin, käyttöoikeuksiin ja suojausasetuksiin) kirjaus- ja tarkastustoiminnot olivat riittämättömiä.

Vuoden 2018 kyberturvallisuuslain[19] mukaan kriittisen tietoinfrastruktuurin toimijan on suoritettava kyberturvallisuusauditointi, jolla se osoittaa, että lain ja sovellettavien käytäntöjen vaatimukset toteutuvat. Tietoturvallisuusauditointi on suoritettava myös tämän kyberturvallisuuslain mukaisesti vähintään kerran kahdessa vuodessa ja sen tekee kyberturvallisuusasiamiehen hyväksymä tai nimeämä tilintarkastaja. Tilintarkastajan on sovellettava sekä vaatimustenmukaisuuden arviointimenettelyä että riskiperusteista lähestymistapaa kriittisen tietoinfrastruktuurin kyberturvallisuustarkastuksessa.

1.2.7 Suomi

Yleisesti ottaen viranomaisilla ei ole velvoitetta teettää tietoturvallisuuden arviointeja kolmansilla osapuolilla, vaan arviontien tekeminen perustuu vapaaehtoisuuteen. Viranomaiset voivat tehdä tietoturvallisuuden arviointia itse tai tilata tietoturvallisuuden arvioinnin Traficomilta tai sen hyväksymältä tietoturvallisuuden arviointilaitokselta (1406/2011). Traficomin tehtävät viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden kansallisissa arvioinneissa on kirjattu lakiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011). Tietoturvallisuuden arviointilaitokset hyväksytään arviointilaitoksista annetun lain mukaisessa menettelyssä (1405/2011). Prosessissa ovat mukana Suomen kansallinen akkreditointiyk-

[18] https://www.ago.gov.sg/docs/default-source/report/871d5a31-829c-4682-9716-8c61cf742c49.pdf
[19] https://sso.agc.gov.sg/Acts-Supp/9-2018/#pr4-

sikkö FINAS sekä Traficom, jonka asiantuntijat arvioivat FINASin lukuun arviointilaitosten pätevyysalueiden teknistä osuutta. FINAS järjestää koulutusta teknisille arvioijille arviointiprosessiin liittyvää koulutusta. Hyväksytyn arviointilaitoksen henkilöstöltä edellytetään luotettavuutta ja osaamista, mutta henkilösertifiointia ei vaadita.

Tiedonhallintalaissa edellytetään tiedonhallintayksiköiden seuraavan ja varmistavan tietojärjestelmien ja tietoaineistojen tietoturvallisuus koko niiden elinkaaren ajan. Laki ei kuitenkaan velvoita säännöllisiin ulkopuolisen toimijan tekemiin arviointeihin, vaan toteutus on tiedonhallintayksikön vastuulla. Tiedonhallintalautakunnan tehtävänä on edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tiedonhallintalain vaatimusten toteuttamista sekä valvoa valtion virastojen ja laitosten sekä kuntien ja kuntayhtymien tiedonhallintalain noudattamista arvioimalla[20]. Arviointilaki (1406/2011) antaa mahdollisuuden käyttää arvioinneissa useita erilaisia viitekehyksiä, mutta arviointilaitoksille myönnettyjä pätevyysalueita ovat ainoastaan Katakri, VAHTI ja ISO 27001.

Sosiaali- ja terveysalan järjestelmien arviointia säädellään asiakastietolaissa (159/2007) ja toisiolaissa (552/2019). Sosiaali- ja terveysalan järjestelmien tietoturvallisuuden arviointeja voivat tehdä hyväksytyt tietoturvallisuuden arviointilaitokset (ks. edellä). Tietoturvallisuuden osalta toimivaltaisia viranomaisia ovat Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira), Kansaneläkelaitos (Kela) sekä Terveyden ja hyvinvoinnin laitos (THL). Hyväksytystä arvioinnista annettava todistus on voimassa enintään viisi vuotta ja vaatimustenmukaisuuden valvonnasta vastaa Valvira.

Kansallinen turvallisuusviranomainen (National Security Authority, NSA) toimii erillisenä yksikkönä ulkoministeriössä. Sen tehtävänä on ohjata ja valvoa, että Suomelle toimitettu kansainvälinen turvallisuusluokiteltu tieto suojataan ja sitä käsitellään kansainvälisen tietoturvallisuusvelvoitelain (588/2004) mukaisesti. NSA koordinoi määrättyjen kansallisten turvallisuusviranomaisten toimintaa ja työskentelee yhteistyössä niiden kanssa. Määrättyjä turvallisuusviranomaisia ovat puolustusministeriö, pääesikunta ja suojelupoliisi. Traficom toimii määrättynä tietoliikenneturvallisuusviranomaisena (National Communication Security Authority, NCSA) niissä tapauksissa, joissa on kyse teknisestä tietoturvallisuudesta ja tietoliikenteen turvallisuudesta.[21]

[20] https://vm.fi/tiedonhallintalautakunnan-tehtavat
[21] https://um.fi/kansallinen-turvallisuusviranomainen

EU:n yleisen tietosuoja-asetuksen kansallinen viranomainen on tietosuojavaltuutetun toimisto, jonka tehtävänä on mm. hyväksyä tietosuojan arviointilaitokset. Tällaisia laitoksia ei toistaiseksi ole. NIS-direktiivin mukaisena yhteyspisteenä ja kansainvälistä tiedonvaihtoverkon kontaktina toimii Liikenne- ja viestintäviraston (Traficom) Kyberturvallisuuskeskus, joka toimii myös digitaalisten palvelujen ja digitaalisen infrastruktuurin valvontaviranomaisena. Yhteiskunnan kriittisen infrastruktuurin tietoturvavelvollisuuksista ja tietoturvahäiriöiden ilmoittamisesta säädetään erityislainsäädännössä sektorikohtaisesti. Toimijoita valvovat sektorikohtaiset valvontaviranomaiset, joille huoltovarmuuskriittiset toimijat raportoivat tietoturvauhkista ja -loukkauksista. Sektorikohtaiset valvontaviranomaiset ovat Energiavirasto (sähkönjakelu, kantaverkko, maakaasun siirtoverkko), Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira (sosiaali- ja terveyspalvelut, lääkinnälliset laitteet ja sote-tietojärjestelmien valmistajat), Finanssivalvonta (pankit ja niiden keskusyksiköt, EU-pankkien sivuliikkeet sekä pörssi), Traficom (ilmailu, merenkulku, rautatie- ja maantieliikenne) sekä maa- ja metsätalousministeriö ja ELY-keskukset (vesilaitokset).

2 KANSAINVÄLISEN VERTAILUN YHTEENVETO

Tässä selvityksessä ei ole keskitytty kansainvälisten turvallisuusluokiteltujen tietojen suojausten arviointiin, vaan selvityksen näkökulmana on julkisesti saatavilla olevaan arviointilainsäädäntö, joka puolestaan painottuu kansallisten tietojen hallinnollisen tietoturvan arviointiin.

Hallinnollisen tietoturvan näkökulmasta verrokkivaltioiden digitaalisen turvallisuuden osa-alueita koskeva arviointilainsäädäntö ei yleisesti ottaen ole kovin yhtenäinen. Voi kuitenkin todeta, että kyberrikollisuuteen, kriittisen infrastruktuurin suojaamiseen ja tietoliikenteen toimivuuteen otetaan kantaa, ja digitaalisen turvallisuuden merkitys on laajasti tunnistettu kaikissa verrokkivaltioissa. Lainsäädäntö on siis vaihtelevaa, mutta EU-maiden tietosuoja-asetus (GDPR), tarkistettu tietoverkkodirektiivi (NIS 2), akkreditointi ja markkinavalvonta-asetus (NLF) sekä kyberturvallisuusasetus yhtenäistävät käytäntöjä.

Valtion virastojen ja kriittisen infrastruktuurin toimijoiden tietoturvallisuuden säännöllistä tarkastamista suositellaan kaikissa verrokkimaissa, mutta tarkastuksen toteutuskäytäntö vaihtelee. Tanskassa, Ruotsissa ja Alankomaissa ei vaadita erityistä aikataulua arvioinnin suorittamiseen. Virossa ministeriöt, virastot sekä valtion tietoturvaan liittyvät rekisterinpitäjät ovat velvollisia suorittamaan arvioinnin ISKE-tietoturvastandardin suojausluokituksen mukaisesti kahden, kolmen tai neljän vuoden välein. Saksassa on säädetty, että kriittisen infrastruktuurin toimijoiden tulee kahden vuoden välein osoittaa palvelunsa täyttävän tietoturva-asetuksen (IT-SiG) vaatimukset auditointien, tutkimusten tai sertifikaattien avulla. Myös Singaporessa kyberturvallisuuslaki edellyttää kriittisen infrastruktuurin toimijoita suorittamaan tietoturvallisuusauditointia vähintään kerran vuodessa. Suomessa viranomaisten tietoturvallisuuden arviointien hakeminen on vapaaehtoista, eikä laki velvoita säännöllisiin ulkopuolisen toimijan tekemiin arviointeihin.

Yleisesti ottaen verrokkimaissa tunnustetaan ja hyväksytään kansainväliset digitaalisen turvallisuuden osa-alueiden standardit. ISO 27001 -standardi on tunnustettu tietoturvan hallintajärjestelmien toteuttamisessa ja ISO 17021-1 -standardi asettaa vaatimuksia tietoturvallisuuden arviointilaitosten akkreditointiprosessiin. Tanskassa on erityisesti säädetty, että kaikkien valtion viranomaisten on noudettava ISO 27001 -standardia vuodesta 2014 lähtien. Joissakin maissa on myös kehitetty omia standardeja digitaalisen turvallisuuden varmistamiseksi. Saksassa on kehitetty tietoturvan hallintajärjestelmänä BSI IT-Grundschutz, joka kattaa tekniset ja organisatoriset sekä infrastruktuuriin ja henkilöstöön liittyvät näkökulmat. Viro on ottanut mallia Saksan IT-Grundschutzista ja se on laatinut oman ISKE-tietoturvastandardinsa. Singaporessa on kehitetty monitasoinen pilviturvallisuusstandardi, MTCS, jossa määritetään kolme erilaista tietoturvasertifikaatin tasoa pilvipalvelujen pääasiallisille tuotantomalleille. Suomessa arviointilaki (1406/2011) antaa mahdollisuuden käyttää arvioinneissa useita erialisia viitekehyksiä, mutta ainoastaan Katakri, VAHTI ja ISO 27001 ovat arviointilaitoksille myönnettyjä pätevyysalueita.

Suomessa hyväksytyn arviointilaitoksen henkilöstöltä edellytetään luotettavuutta ja osaamista, mutta henkilösertifiointia ei vaadita. Virossa asetus tietojärjestelmien turvatoimenpiteiden järjestelmästä ISKE ja uusi E-ITS-standardit edellyttävät, että valtion turvallisuuden hallintajärjestelmän pääarvioijalla (lead auditor) tulee olla voimassa oleva tietoturvallisuuden tarkastuksen sertifikaatti, riittävä

osaaminen sekä tarkastuskokemusta. Uuden E-ITS-tietoturvastandardin mukaan hyväksyttyjä sertifikaatteja ovat ISACA-yhdistyksen myöntämä Certified Information Systems Auditor (CISA) sekä ISO 27001 Lead Auditor Certificate, jonka on myöntänyt joko IRCA (International Register of Certificated Auditors) tai PECB (Professional Evaluation and Certification Board). Auditointien teknisiltä arvioijilta edellytetään vähintään kahden vuoden kokemusta IT-auditoinneista, järjestelmänhallinnasta tai tietoturvallisuudesta. Teknisen tietoturvan tarkastamiseen liittyvästä osaamisesta ei ole annettu yksityiskohtaisia vaatimuksia.

Suomessa viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn vaatimustenmukaisuuden arviointeja voivat teettää viranomaisten lisäksi ne, jotka tekevät hankintoja viranomaisen lukuun, tuottavat viranomaiselle tietojenkäsittely- tai tietoliikennepalveluja tai hoitavat em. palvelujen järjestämiseen liittyviä palvelutehtäviä (1406/2011 4 §). Arvioinnin voi suorittaa arviointilain mukaan Traficom tai hyväksytty arviointilaitos sille hyväksytyn pätevyysalueen mukaisesti.

Selkeää tietoa julkishallinnon digitaalisen turvallisuuden arviointilaitoksesta tai niitä koskevista lainsäädännöistä ei ole löytynyt kaikissa verrokkivaltioissa. Esimerkiksi Tanskassa tietosuojaviranomaisella (Datatilsynet) on valtuudet valtion viranomaisten tietosuoja-arviointiin, ja Saksassa viranomaisten tietoturva-arviointia tukevat kyberturvallisuusviranomaisen (BSI) sertifioimat tietoturvapalveluntarjoajat. Lisäksi voi todeta, että verrokkimaiden valtiontalouden tarkastusviraston yleiseen tehtävään myös kuuluu valtion viranomaisten tietoturvajärjestelmien hallinnollinen tarkastus.

Lainsäädännön noudattamisen ja omien standardien perustamisen lisäksi joissakin verrokkivaltioissa on kehitetty erilaisia ratkaisuja digitaalisen turvallisuuden varmistamiseksi. Esimerkiksi tietoturvallisuutta koskevan yhteistyön tukemiseksi Tanskan valtion IT-neuvosto on perustanut tietoturvafoorumin (GISF), johon osallistuu noin kolmekymmentä valtion laitosta. Foorumi kokoontuu neljästä kuuteen kertaa vuodessa. Ruotsissa on kehitetty turvasuojelulaki (PSA) turvallisuuteen liittyvien arkaluonteisten toimintojen suojelemiseksi, jonka avulla pyritään estämään kansalliseen turvallisuuteen kohdistuvia rikoksia. Virossa on vuonna 2018 luotu Goverment Cloud -alusta, joka tukee julkishallinnon IT-palveluiden hallintaa ja tarkastusta.

3 SUOSITUKSET

Koska tässä selvityksessä keskitytään pääosin tietoturvallisuuden hallintajärjestelmien arviointiin, tässä kappaleessa annetut suositukset myös pohjautuvat hallinnolliseen näkökulmaan. Kuten vertailussa on todettu, niin hallinnollisen tietoturvan osalta verrokkivaltioiden digitaalisen turvallisuuden arviointilainsäädäntö ei ole yhtenäinen. Kaikille yhteisiä menettelyjä on vähän eikä ole sellaista yleistä menettelyä, jota kansainvälisesti noudatettaisiin, Suomi mukaan lukien. EU-maiden tietosuoja-asetus (GDPR), tarkistettu tietoverkkodirektiivi (NIS 2), akkreditointi ja markkinavalvonta-asetus (NLF) sekä kyberturvallisuusasetus yhtenäistävät käytäntöjä, mutta varsinainen digitaalisen turvallisuuden arviointilainsäädännön rakenne vaihtelee. Digitaalisen turvallisuuden merkitys on kuitenkin laajasti tunnistettu kaikissa verrokkivaltioissa, ja näin ollen kaikilla olisi opittavaa toisiltaan.

Arviointilaitoksen hyväksyntäprosessissa edellytetään arviointilaitoksen henkilöstöltä ammattitaitoa ja luotettavuutta. Arvioijien hallinnollisen ja teknisen todennusosaamisen varmistamiseksi henkilösertifiointi voisi tässä olla yksi tapa osoittaa osaamista. Selvityksen perusteella vaikuttaa siltä, että henkilösertifiointia käytetään lähinnä hallinnollisen tietoturvan todennusosaamisen varmistamiseksi. Esimerkiksi Virossa valtion turvallisuuden hallintajärjestelmän toteutuksen arvioinnissa on säädetty, että pääarvioijalla (lead auditor) tulee olla voimassa oleva tietoturvallisuuden tarkastuksen sertifikaatti, riittävä osaaminen sekä tarkastuskokemusta. Uuden E-ITS-tietoturvastandardin mukaan hyväksyttyjä sertifikaatteja ovat ISACA-yhdistyksen myöntämä Certified Information Systems Auditor (CISA) sekä ISO 27001 Lead Auditor Certificate, jonka on myöntänyt joko IRCA (International Register of Certificated Auditors) tai PECB (Professional Evaluation and Certification Board). Auditointien teknisiltä arvioijilta edellytetään vähintään kahden vuoden kokemusta IT-auditoinneista, järjestelmänhallinnasta tai tietoturvallisuudesta. Teknisen tietoturvan tarkastamiseen liittyvästä osaamisesta ei ole annettu yksityiskohtaisia vaatimuksia.

Kaikissa verrokkivaltioissa tunnustetaan ja hyväksytään kansainvälistä standardia (esim. ISO 27001) tietoturvallisuuden arvioinnissa. Joissakin maissa (esim. Saksa, Viro) on myös kehitetty omia tietoturvastandardeja, jotka ovat yhteensopivia ISO 27001-standardin kanssa. Yleisesti ottaen kansalliset standardit huomioivat kansallisen lainsäädännön ja erityisriskit kansainvälisiä kehikkoja paremmin ja esimerkiksi turvallisuusluokitellun tiedon suojaamisessa niiden pohjalta tehtyjä viranomaisarviointeja ja –hyväksyntöjä tunnustetaan myös kansainvälisesti. Uuden kansallisen standardin kehittäminen kansainvälisen tason mukaisesti taas aiheuttaisi päällekkäistä työtä. Näin ollen Suomessa tietoturvallisuuden arvioinnissa tulisi enemmän hyödyntää olemassa olevia kansallisia standardeja täydentämällä kansainvälisillä standardeilla.

Useissa verrokkivaltioissa (esim. Viro, Saksa, Singapore) arviointia edellytetään säännöllisesti. Virossa ministeriöt, virastot sekä valtion tietoturvaan liittyvät rekisterinpitäjät ovat velvollisia suorittamaan arvioinnin ISKE-tietoturvastandardin suojausluokituksen mukaisesti kahden, kolmen tai neljän vuoden välein. Saksassa kriittisen infrastruktuurin toimijoiden tulee varmistaa tietoturva-asetuksen (IT-SiG) vaatimusten täyttäminen kahden vuoden välein. Singaporessa kyberturvallisuuslaki edellyttää kriittisten infrastruktuurien toimijoita suorittamaan tietoturvallisuusauditointia vähintään kerran vuodessa. Tällä hetkellä Suomessa kansallisten tietojärjestelmien ja tietoliikenneratkaisujen arviointi perustuu enimmäkseen vapaaehtoisuuteen. Suomessa digitaalisen toimintaympäristön turvallisuutta

tulisi kehittää kansainvälisen käytännön mukaisesti mm. suorittamalla arviointia säännöllisesti, esimerkiksi vuosittain.

LIITE 1 – LÄHTEITÄ

— Eduskunta, 2017. Valtioneuvoston U-kirjelmä U 58/2017 vp. Saatavilla: U 58/2017 vp (eduskunta.fi)

— Eduskunta, 2021. Valtioneuvoston U-kirjelmä U 71/2020 vp. Saatavilla: U 71/2020 vp (parliament.fi)

— Eduskunta, 2021. Valtioneuvoston U-kirjelmä U 9/2021 vp. Saatavilla: U 9/2021 vp (eduskunta.fi)

— Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS EU:n kyberturvallisuusvirastosta ENISAsta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (”kyberturvallisuusasetus”). Saatavilla: EUR-Lex - 52017PC0477R(01) - EN - EUR-Lex (europa.eu)

— Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI kriittisten toimijoiden häiriönsietokyvystä. COM/2020/829 final. Saatavilla: EUR-Lex - 52020PC0829 - EN - EUR-Lex (europa.eu)

— Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta, 2020. Virallinen lehti. Saatavilla: resource.html (europa.eu)

— Euroopan komissio, 2021. EU:n uusi kyberturvallisuusstrategia ja uudet säännöt, joilla parannetaan fyysisten ja digitaalisten kriittisten yksiköiden häiriönsietokykyä. Saatavilla: EU:n uusi kyberturvallisuusstrategia (europa.eu)

— Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (ETA:n kannalta merkityksellinen teksti). Saatavilla: EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)

— Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008, annettu 9 päivänä heinäkuuta 2008, tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta (ETA:n kannalta merkityksellinen teksti). Saatavilla: EUR-Lex - 32008R0765 - EN - EUR-Lex (europa.eu)

— Euroopan unioni. Yleinen tietosuoja-asetus. Saatavilla: Yleinen tietosuoja-asetus (GDPR) - Your Europe (europa.eu)

— LIITTEET ehdotukseen EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVIKSI toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta, 2020. Virallinen lehti. Saatavilla: resource.html (europa.eu)

Tanska

— BSA | The Software Alliance, 2015. EU Cybersecurity Dashboard - Country reports. Saatavilla: http://cybersecurity.bsa.org/countries.html

— Centre for Cyber Security, 2020. Centre for Cyber Security. Saatavilla: Centre for Cyber Security (cfcs.dk)

— Clemens Advokatfirma, 2019. How are data protection laws enforced in Denmark? Lexology. Saatavilla: How are data protection laws enforced in Denmark? - Lexology

— DANAK, 2020. About accreditation. Saatavilla: ABOUT ACCREDITATION — DANAK

— DANAK, 2020. About DANAK. Saatavilla: ABOUT DANAK — DANAK

— DANAK, 2020. Accreditation to certification of management systems for IT security. Saatavilla: ACCREDITATION TO CERTIFICATION OF MANAGEMENT SYSTEMS FOR IT SECURITY — DANAK

— Digitaliseringsstyrelsen, n.d. Organisation and responsibilities. Saatavilla: Organisation and responsibilities (digst.dk)

— Euroopan komissio, 2021. Implementation of the NIS Directive in Denmark. Saatavilla: Implementation of the NIS Directive in Denmark | Shaping Europe's digital future (europa.eu)

— Ministry of Finance, 2020. Office for Audit and Supervision. Saatavilla: Office for Audit and Supervision (fm.dk)

— Ministry of Finance, 2020. Standard for information security. Saatavilla: Standard for information security (digst.dk)

— Statsrevisorerne Rigsrevisionen, 2016. Extract from Rigsrevisionen's report on management of IT security in systems outsourced to external suppliers. Saatavilla: Report on management of IT security in systems outsourced to external suppliers (nik.gov.pl)

— The Contact Committee of the European Union's (EU) supreme audit institutions, 2020. Cybersecurity in the EU and its Member States.

Ruotsi

— Axelsson, J. n.d. Sweden. ITechLaw. Saatavilla: Sweden | ITechLaw

— BSA | The Software Alliance, 2015. EU Cybersecurity Dashboard - Country reports. Saatavilla: http://cybersecurity.bsa.org/countries.html

— Euroopan komissio, 2021. Implementation of the NIS Directive in Sweden. Saatavilla: Implementation of the NIS Directive in Sweden | Shaping Europe's digital future (europa.eu)

— Försvarsmakten, 2014. KSF Krav på IT-säkerhetsförmågor hos IT-system v3.1. Saatavilla: krav-pa-godkanda-sakerhetsfunktioner-version-3-1.pdf (fmv.se)

— MSB, 2021. About MSB. Saatavilla: About MSB

— MSB, 2009. Information security in Sweden Situational assessment 2009. Saatavilla: Information security in Sweden : situational assessment 2009 (msb.se)

— Regeringskansliet, 2021. Säkerhetsskyddslag (2018:585). Saatavilla: Regeringskansliets rättsdatabaser (gov.se)

— Robert B., 2021. Swedish Protective Security Act. *Termsfeed*. Saatavilla: Swedish Protective Security Act - TermsFeed

— Svenska kraftnät, 2020. Protective Security. Saatavilla: Protective Security | Svenska kraftnät (svk.se)

— Sveriges Riksdag, 2020. Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Saatavilla: Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap Svensk författningssamling 2015:2015:1052 t.o.m. SFS 2020:25 - Riksdagen

— Sveriges Riksdag, 2021. Säkerhetsskyddsförordning (2018:658). Saatavilla: Säkerhetsskyddsförordning (2018:658) Svensk författningssamling 2018:2018:658 t.o.m. SFS 2021:157 - Riksdagen

— SWEDAC, 2021. How accreditation works. Saatavilla: How accreditation works - Swedac

— Säkerhetspolisen, n.d. Protective security. Saatavilla: Protective security - Säkerhetspolisen (sakerhetspolisen.se)

— The Contact Committee of the European Union's (EU) supreme audit institutions, 2020. Cybersecurity in the EU and its Member States.

Viro

— Adopted on 20/12/2007 No. 252. Entry into force 01/01/2008. Saatavilla: *regulation-the-system-of-security-measures-for-information-systems-2007-12-20.pdf (ria.ee)

— Auditeerimisjuhend KAVAND. Saatavilla: https://eits.ria.ee/et/versioon/2020vers1/standardi-dokumendid/auditeerimisjuhend-kavand/

— Eesti Standardimis- ja Akrediteerimiskeskus, 2021. About the Estonian Centre for Standardisation and Accreditation. Saatavilla: About the Estonian Centre for Standardisation and Accreditation - Estonian Centre for Standardisation and Accreditation (evs.ee)

— E-estonia, 2018. Government Cloud: infrastructure as a service. Saatavilla: Government Cloud: infrastructure as a service — e-Estonia (e-estonia.com)

Estonian information security standard (2021). https://www.ria.ee/en/cyber-security/estonian-information-security-standard.html

— Euroopan komissio, 2020. Digital Public Administration factsheet 2020 Estonia. Saatavilla: Digital Public Administration factsheets - 2020 | Joinup (europa.eu)

— Euroopan komissio, 2021. Implementation of the NIS Directive in Estonia. Saatavilla: Implementation of the NIS Directive in Estonia | Shaping Europe's digital future (europa.eu)

— GOVERNMENT OF THE REPUBLIC REGULATION The system of security measures for information systems.

— Republic of Estonia Information System Authority, 2019. Three-level IT Baseline Security System ISKE. Saatavilla: Three-level IT Baseline Security System ISKE | Estonian Information System Authority (ria.ee)

— Riigikontroll, 2019. Structure of the National Audit Office. Saatavilla: Structure of the National Audit Office (riigikontroll.ee)

— The Contact Committee of the European Union's (EU) supreme audit institutions, 2020. Cybersecurity in the EU and its Member States.

Saksa

— Asetus BSI-laissa tarkoitetun kriittisen infrastruktuurin määrittelemisestä, 2016. Saatavilla: BSI-KritisV

— Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009. Act to Strengthen the Security of Federal Information Technology. BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821) last amended by Article 1 of the Act of 23 June 2017 (Federal Law Gazette I p. 1885). Saatavilla: BSI - BSI Act - BSIG (bund.de)

— Bundesamt für Sicherheit in der Informationstechnik (BSI). Cyber-Sicherheitsstragie für Deutschland (2016). Saatavilla: BSI - Cyber-Sicherheitsstragie (bund.de)

— Bundesamt für Sicherheit in der Informationstechnik (BSI). Das IT-Sicherheitsgesetz. Saatavila: BSI - IT-Sicherheitsgesetz (bund.de)

— Euroopan komissio, 2021. Implementation of the NIS Directive in Germany. Saatavilla: Implementation of the NIS Directive in Germany | Shaping Europe's digital future (europa.eu)

— Kansallinen strategia kriittisen infrastruktuurin suojaamiseksi. Saksan sisäministeriö, 2009. Saatavilla englanniksi / saksaksi.

— TÜViT, 2021. Successful ISMS rollout and certification according to ISO 27001. Saatavilla: ISO 27001 | Information Security Management | TÜViT (tuvit.de)

— Voigt, P. & Wessing, T., 2019. Information Security Considerations (Germany). Thompson Reuters. Saatavilla: Information Security Considerations (Germany) | Practical Law (thomsonreuters.com)

— von Walter, A., 2020. Cybersecurity in Germany. Lexology. Saatavilla: Cybersecurity in Germany - Lexology

Alankomaat

— Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013). Saatavilla: wetten.nl - Regeling - Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) - BWBR0033507 (overheid.nl)

— Ministry of the Interior and Kingdom Relations, 2018. Dutch Trust Framework for Electronic Identification. Notification Form.

— BSA | The Software Alliance, 2015. EU Cybersecurity Dashboard - Country reports. Saatavilla: http://cybersecurity.bsa.org/countries.html

— eIDAS Cooperation Network, 2018. Peer Review Report – NL Trust Framework for Electronic Identification “eHerkenning”.

— Euroopan komissio, 2021. Implementation of the NIS Directive in The Netherlands. Saatavilla: Implementation of the NIS Directive in The Netherlands | Shaping Europe’s digital future (europa.eu)

— NOREA De beroepsorganisatie van IT-Auditors, 2021. Saatavilla: NOREA - de beroepsorganisatie van IT-Auditors

— The Contact Committee of the European Union’s (EU) supreme audit institutions, 2020. Cybersecurity in the EU and its Member States.

Singapore

— Auditor-General's Office Singapore, 2019. Overview. Saatavilla: https://www.ago.gov.sg/who-we-are/overview

— Auditor-General's Office Singapore, 2020. Report of the Auditor-General for the financial year 2019/20. Saatavilla: https://www.ago.gov.sg/docs/default-source/report/871d5a31-829c-4682-9716-8c61cf742c49.pdf

— CREST, n.d. CREST Singapore Chapter. Saatavilla: CREST Singapore Chapter (crest-approved.org)

— Cyber Security Agency of Singapore (CSA), 2021. Frequently Asked Questions. Cybersecurity Audit for CII. Saatavilla: Cyber Security Agency of Singapore - FAQ (ifaq.gov.sg)

— CYBERSECURITY ACT 2018 (No. 9 of 2018). Saatavilla: Cybersecurity Act 2018 - Singapore Statutes Online (agc.gov.sg)

— Personal Data Protection Commission, n.d. PDPA Overview. Saatavilla: PDPC | PDPA Overview

— Phua, R., 2020. Lapses in procurement, grants disbursements and IT systems in public agencies: Auditor-General's report. CNA. Saatavilla: https://www.channelnewsasia.com/news/singapore/auditor-general-office-report-it-systems-grants-procurement-ago-13088420

— Singapore Accreditation Council, 2021. Digital / ICT. Saatavilla: Digital / ICT (sac-accreditation.gov.sg)

Suomi

— 906/2019 Laki julkisen hallinnon tiedonhallinnasta (tiedonhallintalaki)

— 920/2005 Laki vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta

— 1405/2011 Laki tietoturvallisuuden arviointilaitoksista

— 1406/2011 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista

— 552/2019 Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (toisiolaki)

— 159/2007 Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (asiakastietolaki)

— 1050/2018 Tietosuojalaki

— 588/2004 Laki kansainvälisistä tietoturvavelvoitteista

— Kyberturvallisuuskeskus (2018) NIS-direktiivi ja toimeenpano Suomessa. Saatavilla

— FINAS kotisivu

— Kyberturvallisuuskeskuksen arviointipalvelut

— Hyväksytyt tietoturvallisuuden arviointilaitokset

— Tiedonhallintalautakunta