Kybermittari

Kansallinen kyberturvallisuuden arviointimalli

Käyttöohje

Sisältö

1 Johdanto

Yhteiskunnan kannalta kriittiseen infrastruktuuriin kohdistuvat uhat ovat kehittyneet ja muuttuneet monimuotoisemmiksi. Erityisesti ovat kasvaneet kyberuhat, joilta suojautuminen on tullut olennaiseksi osaksi tietoyhteiskunnan toimivuuden ja huoltovarmuuden turvaamista. Keskenään riippuvaisten toimintojen vuoksi tulee varmistaa, että jokainen yhteiskunnan toiminnan kannalta kriittinen organisaatio on varautunut kyberuhkiin. Tämä vaatii kansallista yhteistyötä organisaatioiden, toimialojen ja yhteiskunnan kyberturvallisuuden kehittämiseksi.

Nykyisellään kyberturvallisuuden mittaamista tapahtuu erityyppisillä viitekehyksillä, jotka vaihtelevat organisaatiosta ja toimialasta riippuen. Eri viitekehyksillä saavutetut tulokset eivät useinkaan ole vertailukelpoisia, mikä vaikeuttaa tulosten vertailtavuutta ja yhtenäisten kehitystavoitteiden asettamista. Yhteisen mittariston lisäksi puuttuu keinoja jakaa luottamuksellisesti tietoa organisaation kypsyystasosta ja parhaista käytännöistä kyberturvallisuuden kehittämiseksi.

Kybermittari on Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen kehittämä kansallinen kyberturvallisuuden arviointimalli, joka luo yhtenäisen lähestymistavan kyberturvallisuuden arviointiin ja kehittämiseen. Malli on koottu kansallisista ja kansainvälisistä käytänteistä ja sen avulla voidaan arvioida kokonaisvaltaisesti yrityksen, toimialan ja yhteiskunnan kyberturvallisuuden tila ja tunnistaa potentiaaliset kehityskohteet. Kansallinen lähestymistapa mahdollistaa yritysten ja toimialojen vertailun ja tuo yhteisen kielen kyberturvallisuuden mittaamiseen ja kehittämiseen niin organisaatioiden sisällä kuin niiden välillä. Kyberturvallisuuskeskuksen rooli tukee mittarin jatkuvuutta ja luo edellytykset jakaa luottamuksellisesti tietoa parhaista käytänteistä, suosituksia ja referenssituloksia yhteistoiminnassa kriittisten organisaatioiden kanssa.

Kyberturvallisuuskeskus tarjoaa mittarin vapaasti yritysten, järjestöjen ja julkisten toimijoiden käyttöön. Lisäksi sitä voivat hyödyntää kaupalliset toimijat tai viranomaiset. Kybermittarin materiaalipaketti ja ajankohtaiset käyttöehdot ovat saatavilla osoitteessa www.kybermittari.fi suomen, ruotsin ja englannin kielellä. Mittarin pääasiallinen kohderyhmä ovat huoltovarmuuden kannalta kriittiset yritykset, mutta se soveltuu kaikkien toimijoiden käyttöön toimialasta riippumatta.

Yrityksille, järjestöille ja julkisille toimijoille Kybermittarin hyötyjä ovat mm.:

- Avoin ja vapaasti käytettävissä oleva malli kyberturvallisuuden arviointiin ja kehitystoiminnan pitkäjänteiseen ohjaamiseen;
- Kypsyystason vertailu muihin suomalaisiin toimijoihin ("benchmarking") ja parhaiden käytäntöjen jakaminen toimijoiden kesken; ja
- Yhteinen malli kyberturvallisuuden viestintään, arviointiin ja kehittämiseen organisaation sisällä ja yhdessä alihankkijoiden tai viranomaisten kanssa.

Kansallisella tasolla Kybermittari tukee kansallista kyberturvallisuusstrategiaa, jonka yhtenä strategisena toimenpiteenä on kriittisiin toimintoihin liittyvien tuotteiden ja kokonaisten ratkaisuympäristöjen toteutuksen todentamisen, testauksen, arvioinnin ja käyttösuosituksien kehittäminen. Mittarin laajamittainen käyttö tukee kansallisen tilannekuvan muodostamista, viranomaistoimintaa ja päätöksentekoa sekä auttaa kansallisten resurssien kohdentamisessa.

1.1 Kohdeyleisö

Tämä käyttöohje on tarkoitettu tukemaan Kybermittarin käyttöä ja käyttöönottoa tarjoamalla ohjeita ja neuvoja mittarin käyttöön, arvioinnin toteuttamiseen ja tulosten hyödyntämiseen. Käyttöohje on suunnattu erityisesti organisaatiojohdolle, riskienhallinnan ja kyberturvallisuuden asiantuntijoille sekä muille arviointiin osallistuville tahoille. Ohje on jaoteltu seuraaviin osiin:

- **Kappale 2** kuvaa kuinka organisaatio voi parhaiten hyödyntää Kybermittaria ja mitä sen käyttöönotto organisaatiossa vaatii;
- **Kappale 3** kuvaa Kybermittarin rakenteen ja toimintaperiaatteet;
- **Kappaleet 4 ja 5** sisältävät yksityiskohtaisia ohjeita ja suosituksia erityisesti arviointien vetäjille ja muille osallistujille; ja
- **Kappale 6** sisältää sanaston Kybermittarin ja kyberturvallisuuden termeistä.

Käyttöohje on tarkoitettu tulkittavaksi yhdessä arviointityökalun kanssa.

1.2 Alustus

Kybermittarin ovat kehittäneet yhteistyössä Kyberturvallisuuskeskus ja Huoltovarmuuskeskus vuosien 2019-2020 aikana ja sen ensimmäinen versio on julkaistu lokakuussa 2020. Mittarin ylläpidosta ja jatkokehityksestä vastaa Kyberturvallisuuskeskus.

Kehitystyössä haluttiin käyttää pohjana olemassa olevaa kansainvälisesti tunnettua viitekehystä, joka olisi aktiivisesti päivitetty ja vapaasti hyödynnettävissä. Näiden kriteerien ja laajan kartoituksen pohjalta valittiin kehitystyön pohjaksi kaksi viitekehystä, joihin Kybermittari pääosin perustuu. Nämä ovat *National Institute of Standards and Technology Cybersecurity Framework* (NIST CSF) [1] sekä *U.S. Department of Energy Cybersecurity Capability Maturity Model* (C2M2) [2] [3]. Lisäksi ohjeistusta laadittaessa hyödynnettiin muun muassa Suomen kansallista riskiarviota (2015) [4] sekä yhteiskunnan turvallisuusstrategiaa [5].

Kybermittari pohjautuu C2M2-mallin versioon 1.1 ja luonnosversioon 2.0, joiden osiot ja käytännöt on käännetty englannin kieleltä suomeksi ja ruotsiksi. Osiot ja käytännöt on samalla mukautettu soveltumaan paremmin suomalaisiin olosuhteisiin ja suomalaisten organisaatioiden käyttöön. Nämä kymmenen osiota muodostavat Kybermittarin rungon. Kyberturvallisuuskeskus on kehittänyt tämän rungon lisäksi erilliset osiot kriittisten palveluiden suojaamisesta sekä kyberturvallisuuden investoinneista. Kybermittari sisältää lisäksi Kyberturvallisuuskeskuksen kehittämän suuntaa-antavan ristiviittauksen NIST CSF -mallin kanssa, mikä mahdollistaa Kybermittarin tulosten raportoinnin myös NIST CSF -mallin mukaisella jaottelulla.

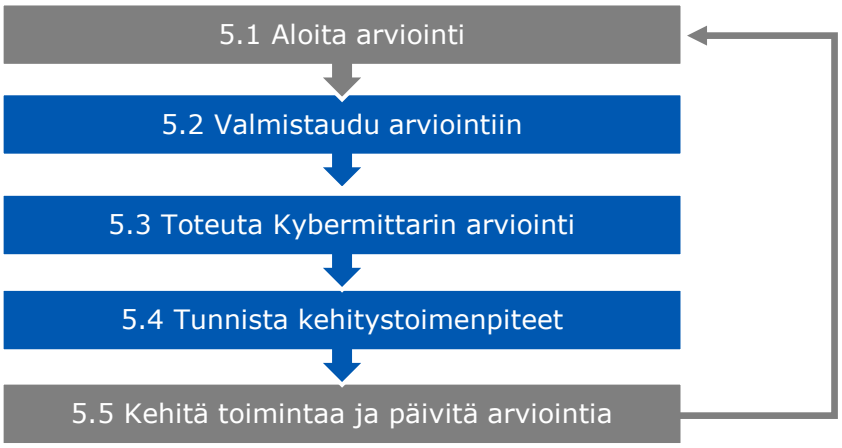
Organisaatiot voivat halutessaan jakaa Kybermittarin avulla tuottamansa arviointitulokset luottamuksellisesti Kyberturvallisuuskeskuksen kanssa. Kyberturvallisuuskeskus voi hyödyntää tuloksia lakisääteisten tehtäviensä toteuttamiseen, minkä lisäksi se voi laatia tulosten pohjalta anonymisoituja toimialojen referenssi- ja suositustasoja, joita se voi tarjota organisaatioille tukemaan Kybermittarin käyttöä ja kyberturvallisuuden kehitystä. Mahdolliset referenssi- ja suositustasot laaditaan siten, ettei niiden perusteella voida tunnistaa yksittäistä organisaatiota tai sen arviointituloksia. Tarkempia tietoja arviointitulosten jakamisesta ja referenssituloksista löytyy osoitteesta www.kybermittari.fi

2 Kybermittarin käyttö

Tämä kappale kuvaa Kyberturvallisuuskeskuksen suosittaman arviointiprosessin, joka helpottaa Kybermittarin hyödyntämistä organisaatioissa. Prosessi on laadittu pilottikartoituksista saatujen kokemusten perusteella.

Kybermittaria suositellaan käytettäväksi osana toiminnan jatkuvaa arviointi- ja kehitysprosessia. Viisivaiheinen prosessi koostuu arvioinnin käynnistämisestä ja siihen valmistautumisesta, arvioinnin toteuttamisesta sekä kehitystoimenpiteiden tunnistamisesta ja toteuttamisesta. Kehitystoimenpiteiden edetessä ja toimintaympäristön muuttuessa arviointia päivitetään tai toteutetaan uusi arviointi. Arviointiprosessi ja sen jatkuvuus on esitetty Kuvassa 1.

Kybermittarin arviointi voidaan toteuttaa kertaalleen, mutta paras hyöty mittarista saadaan, kun se tuodaan osaksi toiminnan jatkuvaa kehittämistä. Lisäksi on suositeltavaa, että arviointi sulautetaan osaksi organisaation muuta riskienhallintaa ja arvioinnin perusteella tehtävä kyberturvallisuuden kehitystyö osaksi organisaation muuta kehittämistoimintaa.



Kuva 1: Kyberturvallisuuden arvioinnin viisivaiheinen prosessi, joka helpottaa Kybermittarin hyödyntämistä organisaatioissa.

Seuraavassa kuvataan lyhyesti jokainen prosessivaihe ja kunkin vaiheen tärkeimmät osallistujat ja tehtävät. Kappaleen lopussa on tiivistettynä muistilista vaiheista ja tehtävistä. Tarkempia ohjeita Kybermittarin käyttöön löytyy kappaleesta 4.

2.1 Aloita arviointi

Osallistujat: Organisaation johtoryhmä tai muu päätöksentekoelin.

Tehtävä:

1. Päättää arvioinnin toteuttamisesta ja arvioinnin kohteesta; ja
2. Nimittää arvioinnille sponsori ja vetäjä, jotka vastaavat jatkotoimenpiteistä.

Arviointi käynnistyy päätöksellä arvioinnin toteuttamisesta määrättyyn kohteeseen ja määrätyllä laajuudella. Suositus on, että päätös tehdään organisaation johtoryhmässä tai muussa kyberturvallisuuden ja riskienhallinnan osa-alueen päätöksentekoelimessä. Näin luodaan riittävä tuki ja edellytykset arvioinnin toteuttamiselle ja kyberturvallisuuden pitkäjänteiselle kehittämiselle.

Tärkein päätös liittyy arvioitavan *toiminnan osa-alueen* valintaan. Toiminnan osa-alueella tarkoitetaan niitä organisaation tai yhteiskunnan kannalta kriittisiä palveluita tai toimintoja, joiden kyberturvallisuutta arvioinnissa tarkastellaan. Arviointi voi kattaa koko organisaation toiminnan, mutta varsinkin suuremmissa organisaatioissa suositellaan kohdistamaan arviointi kerrallaan vain yhteen kriittiseen palveluun tai toimintoon. Yhtenä kokonaisuutena käsittely edellyttää, että noudatettavat prosessit ja käytännöt ovat riittävän yhteneväiset koko arvioitavalla toiminnan osa-alueella. Mikäli halutaan arvioida useita erillisiä toiminnan osa-alueita, suositus on käynnistää jokaisesta oma arviointinsa.

Toinen tärkeä päätös on nimittää arviointia varten *arvioinnin sponsori* sekä käytännön toteutuksesta vastaava *arvioinnin vetäjä* joko organisaation sisältä tai ulkopuolelta. Myös nämä nimitykset suositellaan tehtäväksi johtoryhmässä tai muussa päätöksentekoelimessä. Arvioinnin sponsorin tulisi olla johtoryhmän jäsen tai organisaation muu toimihenkilö, mutta arvioinnin vetäjänä voidaan hyödyntää myös ulkoisen palveluntarjoajan asiantuntijaa. Arviointi on lisäksi mahdollista ulkoistaa kokonaan tai osittain palveluntarjoajan tuottamaksi.

Arvioinnin vetäjä voidaan valita organisaation sisältä tai ulkopuoliselta palveluntarjoajalta

Valintaan vaikuttavat mm. aiempi kyberosaaminen, ajankäyttö ja arvioinnin organisointi

Kun päätös arvioinnin toteuttamisesta on tehty ja arvioinnille on nimetty sponsori ja vetäjä, ottavat he vastuun arvioinnin käytännön toteuttamisesta.

2.2 Valmistaudu arviointiin

Osallistujat: Arvioinnin sponsori ja vetäjä yhdessä.

Tehtävä:

1. Rajata tarkemmin arvioitavana oleva toiminnan osa-alue ja tunnistaa osa-alueen kriittiset riippuvuudet;
2. Tunnistaa arviointiin tarvittavat asiantuntijat; ja
3. Sopia arviointitavasta ja arvioinnin aikataulusta.

Arvioinnin sponsori ja vetäjä määrittävät yksityiskohtaisemmin arvioitavana olevan toiminnan osa-alueen ja tunnistavat osa-alueen toimintavarmuuden kannalta kriittiset riippuvuudet. Kriittisillä riippuvuuksilla tarkoitetaan niitä järjestelmiä, prosesseja ja tieto-omaisuutta, joita tarvitaan valittujen palveluiden tai toimintojen toteuttamiseen. Mikäli tässä vaiheessa havaitaan haasteita esimerkiksi arvioinnin laajuuden osalta, voidaan päätös arvioitavan toiminnan osa-alueen rajauksesta käyttää vielä uudelleen johtoryhmän arvioitavana. Toiminnan osa-alueen ja sen riippuvuuksien tunnistamiseen löytyy tarkempia ohjeita kappaleesta 4.2.

Osa-alueen rajaus *kannattaa tehdä huolella, jotta arviointi voidaan toteuttaa tavoiteajassa ja tuloksia osataan tulkita myöhemmin oikein*

Työpajamuotoinen *arviointitapa on havaittu suosituimmaksi toteutustavaksi.*

Arvioitavan toiminnan osa-alueen ja sen riippuvuuksien perusteella arvioinnin sponsori ja vetäjä tunnistavat arviointiin tarvittavat organisaation asiantuntijat. Asiantuntijat tuovat omalta vastuualueeltaan arviointiin tarvittavaa osaamista esimerkiksi organisaation liiketoiminnasta, riskienhallinasta, tietohallinosta tai muista prosesseista. Sopiva osallistujamäärä vaihtelee organisaatiokohtaisesti.

Arvioinnin laajuuden, osallistujien lukumäärän ja organisaation mieltymysten perusteella arvioinnin sponsori ja vetäjä sopivat vielä arvioinnin toteutustavasta. Suositus on käyttää, joko työpaja- tai henkilövetoista arviointia. Työpajavetoisessa arvioinnissa osallistujat kutsutaan koolle yhteen tai useampaan arviointityöpajaan, joissa arviointi suoritetaan alusta loppuun. Henkilövetoisessa arvioinnissa osiot jaetaan kullekin osallistujalle erikseen täytettäväksi ja arvioinnin vetäjä koostaa vastaukset yhteen. Toteutustapojen etuja on kuvattu tarkemmin kappaleessa 4.3.

Kun kaikki edellä esitetyt asiat on määritetty, sopivat arvioinnin sponsori ja vetäjä vielä arvioinnin aikataulusta. Suositus on varata ennalta arviointiin liittyvien tapaamisten ajankohdat ja arviointiin osallistuvat asiantuntijat.

2.3 Toteuta Kybermittarin arviointi

Osallistujat: Arvioinnin vetäjä, arvioinnin sponsori ja organisaation asiantuntijat.

Tehtävä: Toteuttaa arviointi valitulla arviointitavalla Kybermittari-työkalun avulla.

Varattava aika: 1-2 työpäivää.

Arvioinnin vetäjä vastaa arvioinnin käytännön järjestelyistä ja arviointiin osallistuvien organisaation asiantuntijoiden perehdyttämisestä Kybermittarin käyttöön. Järjestelyihin kuuluvat toteutustavasta riippuen tapaamisten koollekutsuminen, materiaalien jakaminen sekä vastausten koostaminen. Perehdyttämisessä ovat avuksi Kybermittarin käyttöohje sekä muu tukimateriaali.

Arviointi suoritetaan Kybermittari-työkalun avulla. Osallistujat vastaavat kysymyksiin kyberturvallisuuden käytännöistä ja niiden toteutumisesta organisaation toiminnassa. Työkalu ohjaa arvioinnin suorittamista ja määrittää vastausten pohjalta organisaation kypsyystason arvioinnin edetessä.

2.4 Tunnista kehitystoimenpiteet

Osallistujat: Arvioinnin vetäjä, arvioinnin sponsori, organisaation asiantuntijat ja kehityssuunnitelmien omistajat.

Tehtävä:

1. Analysoida arvioinnin tulokset;
2. Määrittää mahdollinen toiminnan tavoitetaso; sekä
3. Tunnistaa ja priorisoida tärkeimmät kehitystoimenpiteet.

Arvioinnin vetäjä vastaa tulosten yhteenvedosta ja analysoinnista yhdessä arvioinnin sponsorin, organisaation asiantuntijoiden ja kehityssuunnitelmien omistajien kanssa. Kybermittari-työkalu tuottamat automaattiset raportit tukevat tulosten analysointia ja niiden avulla voidaan tunnistaa organisaation toiminnan vahvuudet ja heikkoudet usealla eri mittaristolla. Mikäli organisaatiolla on lisäksi käytössään viiteryhmien referenssi- tai suositustasoja, voidaan raportteja rikastaa tiedolla esimerkiksi toimialan keskimääräisestä kypsyystasosta.

Sopivien kehitystoimenpiteiden tunnistamiseksi suositellaan aina määrittämään organisaation tavoittelema kyberturvallisuuden tavoitetaso. Kaikilla arvioitavilla alueilla ei välttämättä ole kustannustehokasta pyrkiä korkeimmalle kypsyystasolle. Riittävä taso voidaan määrittää esimerkiksi saavutettujen tulosten, mahdollisten viiteryhmien referenssi- ja suositustasojen tai organisaation sisäisten tavoitteiden perusteella. Nämä voivat olla liiketoiminnallisia tavoitteita tai pohjautua esimerkiksi riskiarvioissa tunnistettuihin uhkiin. Niille organisaatioille, jotka toteuttavat arviointia ensimmäistä kertaa, tavoitetaso määräytyy yleensä vasta ensimmäisen arvioinnin tuloksien ja löydösten pohjalta. Yleissuosituksena voidaan pitää, että kaikki organisaatiot pyrkisivät kaikissa osioissa vähintään kypsyystasolle 1.

***Tavoitetason** määrityksessä kannattaa hyödyntää referenssi-/suositustasoja, joita voi pyytää Kyberturvallisuuskeskukselta*

Yleissuositus on pyrkiä ensin kaikessa toiminnassa tasolle 1

Arvioinnin tulosten ja tavoitetilan perusteella tunnistetaan ne kehitystoimenpiteet, joita organisaation tulisi toteuttaa toimintansa kehittämiseksi ja tavoitetilan saavuttamiseksi. Toimenpiteistä laaditaan kehityssuunnitelma, jonka tulisi sisältää toimenpiteiden priorisoinnin lisäksi ainakin toimenpidekohtainen aikataulu, vastuuhenkilö ja yksityiskohtaisempi toteutussuunnitelma. Kyberturvallisuutta ei voi kehittää irrallaan organisaation muusta toiminnasta ja tämän vuoksi kehityssuunnitelman laatimisessa tulee huomioida organisaation normaalit toiminnan suunnittelun ja budjetoinnin prosessit. Ne vaikuttavat päätöksentekoon ja suunnitelman toteuttamisen aikatauluun.

Kun kehitystoimenpiteet on valittu ja aikataulutettu, siirtyy koordinointivastuu nimetyille kehityssuunnitelmien omistajille.

2.5 Kehitä toimintaa ja päivitä arviointia

Osallistujat: Kehityssuunnitelmien omistajat, organisaation asiantuntijat sekä organisaation johtoryhmä tai muu päätöksentekoelin.

Tehtävä: Toteuttaa suunniteltuja kehitystoimenpiteitä, päivittä arviointia ja käynnistää tarvittaessa uusi arviointiprosessi.

Kybermittarin käyttäminen tulee nähdä prosessina, jossa arviointi ja kehitystoimenpiteiden toteuttaminen vuorottelevat säännöllisesti. Kyberturvallisuuden kypsyystasoa voidaan nostaa askel askeleelta päämääränä oman riskinkantokyvyn mukaisesti määritetty tavoitetaso.

Kehityssuunnitelmien omistajien keskeisenä tehtävänä on koordinoida suunnitelmien toteutusta ja ylläpitää kokonaiskuvaa toimenpiteiden etenemisestä. Tavoitteena on varmistaa päätettyjen toimenpiteiden toteutuminen ja tunnistaa oikea aika arvioinnin päivittämiselle.

***Uudelleenarviointi** kannattaa toteuttaa 1-2 vuoden välein, organisaatiosta ja arvioinnin kohteesta riippuen*

Arvioinnin päivitys tai uudelleenarviointi tulee ajankohtaiseksi, kun kehityssuunnitelmat etenevät tai organisaation toimintaympäristö muuttuu. Kybermittarin hyödyt tulevat parhaiten käyttöön, kun toimintaa arvioidaan säännöllisesti uudelleen ja kehitystoimenpiteiden vaikutukset nähdään myös raporteissa. Kybermittari-työkalu mahdollistaa aikaisempien arviointien vertailun, mikä helpottaa kehitystoimenpiteiden vaikutusten seurantaa ja raportointia.

Arviointiprosessin yhteenveto ja muistilista

Alle on koottu Kybermittarin arviointiprosessin keskeiset vaiheet ja kunkin vaiheen tärkeimmät huomioitavat asiat.

3 Kybermittarin arviointimalli

Tämä kappale kuvaa Kybermittarin arviointimallin ja sen tärkeimmät ominaisuudet. Näitä ovat erityisesti arviointimallin rakenne ja kypsyystason laskentamalli.

Kybermittari edustaa kyberturvallisuuden kyvykkyyksien arviointiin ja kehittämiseen tarkoitettua kypsyysmallia. Mallin avulla voidaan arvioida kyberturvallisuuden kyvykkyyksiä ja ohjata kehitystoimintaa neljällä eri kypsyystasolla (tasot 0-3). Tasot edustavat toiminnan järjestelmällisyyttä ja kehittyneisyyttä heikommasta parempaan. Tavoitteena on, että organisaatio määrittelee toimintansa nykytason ja etenee tasolta toiselle kohti parempaa ja tehokkaampaa toimintaa.

Taso 0 Toiminta ei täytä perustavanlaatuisia vaatimuksia;

Taso 1 Toiminta täyttää perustavanlaatuiset vaatimukset, mutta voi olla vielä ajoittaista ja toiminnan taso voi vaihdella tapauskohtaisesti;

Taso 2 Toiminta on edistyneempää ja kattavampaa kuin alemmalla tasolla, minkä lisäksi kyberturvallisuuden hallintaa kuvaavat:

- Dokumentoidut prosessit ja käytänteet;
- Riittävä resursointi ja osaaminen; sekä
- Määritetyt roolit ja vastuut.

Taso 3 Toiminta on edistynyttä ja kattavaa, minkä lisäksi kyberturvallisuuden hallintaa kuvaavat:

- Toimintaa ohjaa organisaation politiikka (tai vastaava ohjeistus);
- Toiminnalle on asetettu suoritustavoitteet, joita seurataan; sekä
- Dokumentoidut prosessit ja käytänteet ovat organisaation normien mukaisia ja niiden kehitys on jatkuvaa.

3.1 Tärkeimmät käsitteet

Kybermittarin yhteydessä käytetään käsitteitä, joiden ymmärtäminen on olennaista mittarin oikean käytön ja tulosten tulkinnan kannalta. Tässä esitellään neljä tällaista käsitettä, joiden lisäksi kappaleesta 6 löytyy laajempi sanasto Kybermittarin käsitteitä ja kyberturvallisuuden termejä.

Kyvykkyys tarkoitetaan kykyä toimia tarkoituksenmukaisella tavalla tietyllä osa-alueella ja hyödyntää osaamistaan sekä resurssejaan, jotta tavoitteet saavutetaan. Organisaatioiden kyvykkyyksien toteuttamiseen tarvitaan yleensä yhdistelmiä kolmesta osakokonaisuudesta, joita ovat toimintamallit ja prosessit, henkilöstö ja osaaminen sekä tiedot ja järjestelmät. Kybermittarin avulla pyritään arvioimaan ja kehittämään organisaation kyberturvallisuuden kyvykkyyksiä.

Kypsyysmalli tarkoittaa mallia, jossa toimintaa tarkastellaan tasoina tai askelmina, joita kiivetään ylöspäin kohti järjestelmällisempää ja kehittyneempää toimintaa. Kullekin tasolle on asetettu tavoitteita tai vaatimuksia, joita arvioinnin kohteena olevan toiminnan tulisi kyseisellä tasolla täyttää. Nämä tavoitteet ja tasot edustavat tyypillisesti parhaiksi tunnistettuja käytäntöjä ja saattavat esimerkiksi noudattaa jonkin lain tai standardin toteutusta. Lisäksi kypsyysmallille on ominaista, että toiminta jaotellaan eri osioihin, joita tarkastellaan kutakin erikseen. Kybermittarissa

organisaation kyberturvallisuuden kyvykkyyksiä arvioidaan käyttäen neljää eri kypsyystasoa ja yhtätoista arvioitavaa osiota.

Toiminnan osa-alue on Kybermittarin yhteydessä käytetty käsite, jolla tarkoitetaan niitä organisaation tai yhteiskunnan kannalta kriittisiä palveluita tai toimintoja, joiden kyberturvallisuutta arvioinnissa tarkastellaan. Palveluiden lisäksi määritelmä kattaa palveluiden tuottamisen kannalta kriittiset prosessit, järjestelmät ja tietovarannot. Toiminnan osa-alueen tunnistaminen ja selkeä määrittäminen ovat olennaisessa roolissa arvioinnin toteuttamisessa ja tulosten hyödyntämisessä.

3.2 Osiot, tavoitteet ja käytännöt

Kybermittari koostuu yhdestätoista kyberturvallisuuden *osiosta*, osioille asetetuista *tavoitteista* sekä tavoitteiden täyttymistä mittaavista *käytännöistä*. Käytännöt edustavat tyypillisiä ja hyväksi havaittuja kyberturvallisuuden menettelytapoja, joita eri toimialojen yritykset toiminnassaan noudattavat. Jokainen käytäntö edustaa tiettyä vaativuus/kypsyystasoa ja kohdistuu tiettyyn kyberturvallisuuden tavoitteeseen. Käytännöt on ryhmitelty tavoitteiden ja vaativuuden mukaisesti.

Osiot Kybermittari koostuu yhdestätoista osiosta, joita ovat:

1. Kriittisten palveluiden suojaaminen (CRITICAL);
2. Riskienhallinta (RISK);
3. Toimitusketjun ja ulkoisten riippuvuuksien hallinta (DEPENDENCIES);
4. Omaisuuden, muutoksen ja konfiguraation hallinta (ASSET);
5. Identiteetin- ja pääsynhallinta (ACCESS);
6. Uhkien ja haavoittuvuuksien hallinta (THREAT);
7. Tilannekuva (SITUATION);
8. Tapahtumien ja häiriötilanteiden hallinta (RESPONSE);
9. Henkilöstön hallinta (WORKFORCE);
10. Kyberturvallisuusarkkitehtuuri (ARCHITECTURE); ja
11. Kyberturvallisuusohjelma (PROGRAM).

Kyseinen järjestys on suositeltu arviointijärjestys, mutta osiot voidaan arvioida muussakin järjestyksessä. Suositeltavaa on, että arviointi kattaa kaikki osiot, jotta lopputuloksena muodostuu kokonaiskuva organisaation kyberturvallisuuden toiminnasta ja tunnistetaan mahdolliset piilevät heikkoudet.

Tavoitteet Kybermittari koostuu yhteensä 52 tavoitteesta, jotka jakautuvat siten, että jokainen Kybermittarin osio pitää sisällään kolmesta viiteen kyberturvallisuuden tavoitetta. Ne edustavat tyypillisiä ja hyväksi havaittuja kyberturvallisuustavoitteita.

Tavoitteet ja niiden sisältämät käytännöt edustavat joko:

- Kyberturvallisuustavoitteita, tai
- Yleisten hallintatoimien tavoitteita.

Kyberturvallisuustavoitteet edustavat tavoitteita, joita organisaation tulisi toiminnassaan saavuttaa suojautuakseen kyberuhilta (vs. hallinnalliset toimenpiteet,

jotka edustavat toiminnan vakiintuneisuuteen liittyviä tavoitteita). Jokaisessa osiossa on asetettu omat erilliset kyberturvallistavoitteet.

Yleisten hallintatoimien tavoitteet puolestaan mittaavat sitä kuinka vakiintunutta organisaation toiminta on. Arvioitavat käytännöt ovat samat jokaisen osion kohdalla. Huomionarvoista on, että kypsyystasolla 1 ei ole asetettu hallinnallisia tavoitteita, ts. tason 1 saavuttamiseksi toiminnan ei tarvitse olla vielä vakiintunutta eikä tason saavuttamiseksi tarvitse välttämättä noudattaa muodollisia prosesseja.

Käytännöt Kyberturvallisuuden kypsyystaso määritellään arvioimalla toimintaa kuvaavia käytäntöjä. Jokainen Kybermittarin osio ja tavoite koostuu joukosta käytäntöjä. Käytännöt edustavat tyypillisiä ja hyväksi havaittuja kyberturvallisuuden menettelytapoja, joita eri toimialojen organisaatiot toiminnassaan noudattavat. Käytännöt on järjestetty tavoitteiden mukaisesti siten, että kunkin kypsyystason toimintaa edustaa joukko käytäntöjä.

3.3 Kypsyystason laskentamalli

Kybermittarin kypsyystason laskentamalli määrittää organisaation kypsyystason käyttäen asteikkoa 0-3. Kypsyystaso määräyty toteutettujen käytäntöjen ja niiden edustaman vaativuuden mukaan. Mitä vaativampia käytäntöjä toiminnassa toteutetaan, sitä korkeampi on arvioitavan toiminnan osa-alueen kypsyystaso.

Kypsyystaso lasketaan kolmessa vaiheessa:

1) Jokainen käytäntö arvioidaan joko Toteutuneeksi tai Ei toteutuneeksi:
2) Jokaisen tavoitteen kypsyystaso lasketaan toteutuneiden käytäntöjen (prosenttiosuuden) perusteella; ja
3) Jokaisen osion kypsyystaso määritetään osion heikoimman tavoitteen kypsyystason mukaisesti.

Näin muodostuu kyberturvallisuuden kypsyystaso jokaiselle yhdelletoista osiolle.

Vaihe 1: Käytäntöjen toteutumista arvioidaan neljän vastausvaihtoehdon kautta.

1. **Ei toteutettu** - organisaatio ei toteuta kuvattuja käytäntöjä;
2. **Osittain toteutettu** - organisaatio on vasta alussa kuvattujen käytäntöjen toteuttamisessa tai toiminta on käytännön osalta muuten puutteellista;
3. **Enimmäkseen toteutettu** - organisaatio toteuttaa kuvattuja käytäntöjä ainakin pääosin, vaikka kehitystyö saattaa olla vielä osittain kesken;
4. **Täysin toteutettu** - organisaatio toteuttaa kuvattuja käytäntöjä, eikä merkittäviä kehitystoimenpiteitä tarvita;

Soveltamisohjeita: jos organisaatiolla on puutteita käytännön toteuttamisessa, tulisi valita vastausvaihtoehdoista joko 1 tai 2, vaikka puutteiden korjaamiseksi olisi laadittu kehityssuunnitelmat; kehitystoimenpiteiden edistyessä ja valmistuessa tulisi arviointia päivittää.

Vaihe 2: Tavoitteiden kypsyystaso lasketaan seuraavasti:

- Tasolla 1 tulee toteuttaa kaikki (100%) kyseisen tason käytännöistä;

- Tasolla 2 tulee toteuttaa yli puolet (>50%*) kyseisen tason käytännöistä *ja* kaikki (100%) tason 1 käytännöt; ja
- Tasolla 3 tulee toteuttaa yli puolet (>50%*) kyseisen tason käytännöistä *ja* kaikki (100%) tason 2 ja kaikki (100%) tason 1 käytännöt.

Prosenttiosuuksien laskentaa varten neljä vastausvaihtoa tiivistetään toteutuneeksi tai ei toteutuneeksi siten, että 4. Täysin toteutettu ja 3. Enimmäkseen toteutettu lasketaan toteutuneeksi.

Vaihe 3: Osioiden kypsyystaso määritetään osion heikoimman tavoitteen kypsyystason mukaisesti. Jos osio koostuu esimerkiksi kolmesta tavoitteesta, joiden kypsyystasoiksi on laskettu 1, 2 ja 3, tulee osion kypsyystasoksi näistä heikoin, eli kypsyystaso 1.

Laskentamalli painottaa kokonaisvaltaista riskienhallintaa, jossa toiminnan heikoimman osa-alueen merkitys korostuu. Tietyn kypsyystason saavuttaakseen tulee - tasosta riippuen - toteuttaa joko kaikki tai yli puolet kyseisen kypsyystason käytänteistä. Seuraavalle kypsyystasolle ei voi edetä ennen kuin on toteuttanut *kaikki* alempien kypsyystasojen käytänteet. Organisaatio ei siis voi saavuttaa korkeampia kypsyystasoja ennen kuin sen toiminta täyttää tietyn kypsyystason vaatimukset kaikkien arvioitavien osioiden osalta.

***Huom.!** Tämä poikkeaa C2M2-mallin käyttämästä laskentamallista, jossa jokaisen tason saavuttaminen vaatii kaikkia kyseisen tason ja sitä alempien tasojen käytäntöjen toteuttamista. Kybermittarin laskentamallia on kevennetty, jotta se nostaisi paremmin esiin ylemmillä kypsyystasoilla tehdyn kehitystyön, vaikka jokin yksittäinen kyseisen kypsyystason käytäntö voisikin vielä puuttua.

Lisäksi Kybermittarin arviointimallin kypsyystasoista on hyvä huomata seuraavat:

Kypsyystasot ovat osiokohtaisia. Jokaisen osion kypsyystaso määritetään osiolle asetettujen tavoitteiden ja käytäntöjen perusteella. Koska osiot eivät ole riippuvaisia toisistaan voi yritys saavuttaa hyvin erilaisia kypsyystasoja eri osioissa.

Kypsyystasot ovat kumulatiivisia. Kypsyystason saavuttaminen vaatii sekä kyseisen tason käytänteiden toteuttamista, että kaikkien sitä alempien tasojen käytäntöjen toteuttamista. Kehittyneistä tai kalliista toimista huolimatta ei saavuteta korkeaa kypsyystasoa, mikäli perusasiat eivät ole kunnossa.

Tavoitetasojen asettaminen. Sopiva tavoitetaso riippuu organisaatiosta ja toimialasta. Tavoitteet kannattaa asettaa osiokohtaisesti ja ne kannattaa suhteuttaa organisaation nykytasoon, liiketoiminnallisiin tavoitteisiin, organisaation riskiarvioon sekä mahdollisiin toimialan referenssi- tai suositustasoihin.

4 Yksityiskohtainen ohje arvioinnin vetäjälle

Tämä kappale tarjoaa yksityiskohtaista ohjeistusta Kybermittarin käyttöön. Osio on tarkoitettu erityisesti tukemaan arvioinnin vetäjää ja muita arviointiin osallistuvia tahoja arviointiin valmistautumisessa, arvioinnin toteuttamisessa ja tulosten hyödyntämisessä. Seuraavat alakappaleet kattavat tarkemmin arvioinnin avainhenkilöt, toiminnan osa-alueen määrittämisen, arvioinnin toteutustavat sekä arviointitulosten ja raporttien hyödyntämisen.

4.1 Avainhenkilöistä ja rooleista laajemmin

Arviointia varten on suositeltavaa tunnistaa ja nimetä avainhenkilöt seuraaviin rooleihin: arvioinnin sponsori, arvioinnin vetäjä, arviointiin osallistuvat organisaation asiantuntijat ja mahdollisten kehityssuunnitelmien omistajat.

Arvioinnin sponsori luo edellytykset arvioinnin toteuttamiselle ja vastaa arvioinnin onnistumisesta yhdessä arvioinnin vetäjän kanssa. Hänen tehtävänsä on turvata arvioinnin riittävä resursointi ja organisaatiojohdon tuki. Lisäksi hänellä on tärkeä rooli organisaation johdon sitouttamisessa kyberturvallisuuden pitkäjänteiseen kehittämiseen. Rooli tulee aina nimetä organisaation sisältä.

Arvioinnin vetäjä vastaa arvioinnin toteuttamisesta arvioinnin sponsorin tukemana. Hän vastaa arvioinnin valmisteluista, toteutuksen käytännön järjestelyistä ja tulosten käsittelystä. Lisäksi hän vastaa omasta ja muiden arviointiin osallistuvien perehdyttämisestä Kybermittarin ja sen arviointityökaluun käyttöön. Arvioinnin vetäjän ominaisuuksissa painottuvat kyberturvallisuusosaamisen lisäksi kyky organisoida ja aikatauluttaa arviointi.

Arvioinnin vetäjäksi voidaan nimetä joko organisaation sisäinen vetäjä tai hyödyntää ulkopuolisen palveluntarjoajan osaamista. Rooli voidaan myös jakaa siten, että arvioinnille nimetään organisaation sisältä vastuuhenkilö, mutta arvioinnin käytännön järjestelyt ja läpivienti hankitaan ulkopuolelta.

- **Organisaation sisäinen vetäjä.** Roolin voidaan nimetä esimerkiksi tietoturvapäällikkö tai muu kyberturvallisuuden asiantuntija tai aiheeseen perehtynyt henkilö;
- **Ulkopuolinen arvioinnin vetäjä.** Palveluntarjoajan osaamista voidaan hyödyntää arvioinnissa esimerkiksi arvioinnin vetäjänä, ulkopuolisena asiantuntijana tai kehitystoimenpiteiden suunnittelussa.

Ulkoista palveluntarjoajaa voidaan suositella yhtä lailla pienille kuin suurillekin yrityksille. Ulkopuolisen asiantuntijan hyödyntämistä suositellaan etenkin niille organisaatioille, joille kypsyysmallien käyttäminen ei ole tuttua entuudestaan tai joilla on rajalliset resurssit kyberturvallisuuden kehittämiseen. Pienen ja keskisuuren yrityksen kohdalla hyötyä saadaan erityisesti ulkopuolisen kokemuksen muodossa - suurten yritysten kohdalla hyödyt voivat painottua enemmän arvioinnin organisoinnin ja aikataulutuksen puolelle.

Organisaation asiantuntijat Arviointiin tarvitaan asiantuntemusta mm. organisaation liiketoiminnan, kyberturvallisuuden sekä riskien- ja henkilöstönhallinnan osa-alueilta. Arvioinnin vetäjä määrittää yhdessä sponsorin kanssa arviointiin tarvittavat osallistujat etenkin liiketoiminnan näkökulmasta. Asiantuntijoiden määrä vaihtelee organisaation koosta riippuen. Pienemmissä yrityksissä koko arvioinnin voi hoitaa muutama avainhenkilö; suuremmissa arviointiin voi olla järkevä kutsua asiantuntijoita useilta eri osastoilta.

Taulukossa 1 on listattu keskeisiä asiantuntijoita eri aihealueiden kysymysten vastaamiseen. Luettelossa korostuvat tietoturvajohtajan ja -päällikön roolit, mutta näiden roolien sijasta voidaan käyttää muita henkilöitä, joilla on arvioinnin kohteen kannalta relevantteja kyberturvallisuuteen liittyviä vastuita.

Taulukko 1: Kybermittarin aihealueiden täyttämisen keskeiset roolit.

Kybermittarin osa-alue	*Keskeiset roolit*
CRITICAL *Kriittisten palveluiden suojaaminen*	Riskienhallintapäällikkö, tietoturvajohtaja ja -päällikkö, sekä liiketoiminnan edustajat yhdessä
RISK *Riskienhallinta*	Riskienhallintapäällikkö, tietoturvajohtaja ja -päällikkö
ASSET *Suojattavien kohteiden, muutosten ja konfiguraatioiden hallinta*	Tietoturva- ja tietohallintojohtaja yhdessä (*OT omaisuus: lisäksi asiasta vastaavat liiketoiminnan edustajat)
PROGRAM *Kyberturvallisuuden kehitysohjelman hallinta*	Tietoturvajohtaja/päällikkö tai muu kyberturvallisuudesta organisaatiossa vastaava henkilö
DEPENDENCIES *Toimitusketjun ja ulkoisten riippuvuuksien hallinta*	Hankintapäällikkö, riskienhallintapäällikkö, Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä
ACCESS *Käyttövaltuuksien ja pääsynhallinta*	Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä
RESPONSE *Tapahtumien ja poikkeamien hallinta*	Tietoturvajohtaja/päällikkö, tietohallintojohtaja ja riskienhallintapäällikkö yhteisesti sekä asiaa hoitavat liiketoiminnan edustajat
ARCHITECTURE *Kyberturvallisuus-arkkitehtuuri*	Tietoturvajohtaja/päällikkö yhdessä relevanttien arkkitehtien kanssa
SITUATION *Tilannekuva*	Tietoturvajohtaja/päällikkö ja tietohallintojohtaja yhdessä
THREAT *Uhkien ja haavoittuvuuksien hallinta*	Tietoturvajohtaja ja -päällikkö yhteisesti, sekä asiaa hoitavat liiketoiminnan edustajat
WORKFORCE *Henkilöstöhallinta*	Tietoturvajohtaja yhteistyössä henkilöstöjohtajan kanssa

Kehityssuunnitelmien omistajat vastaavat tulosten pohjalta muodostetuista kehityssuunnitelmista. Heidän tehtävänsä on koordinoida kehityssuunnitelman laadintaa, varmistaa, että toimenpiteille haetaan tarvittavat resurssit ja seurata suunnitelmien toteutumista. Vastuuhenkilö voi olla sama kuin arvioinnin sponsori tai arvioinnin vetäjä. Kyberturvallisuuden kehittämisen kannalta on tärkeää, että rooli on näkyvästi annettu erikseen nimetylle taholle ja että hänellä on velvollisuus raportoida yrityksen johdolle. Rooli on suositeltavaa nimetä organisaation sisältä.

4.2 Arvioitavan toiminnan osa-alueen määrittelystä

Arvioinnin sponsori ja arvioinnin vetäjä määrittävät yksityiskohtaisesti arvioinnin kohteena olevan toiminnan osa-alueen. **Toiminnan osa-alueella tarkoitetaan niitä *toimintoja* ja toimintojen tuottamisen kannalta kriittisiä *järjestelmiä, prosesseja* ja *tieto-omaisuutta,* joita arvioinnissa tarkastellaan**. Toimintojen ja niiden riippuvuuksien määritys on arvioinnin onnistuneen toteuttamisen kannalta kriittinen työvaihe. Tarkka rajaus ja dokumentointi mahdollistavat arvioinnin toteuttamisen tavoiteajassa, arviointitulosten vertailukelpoisuuden ja myöhempien kehitystoimenpiteiden oikean kohdistamisen.

Kriittisten toimintojen tunnistaminen

Arviointi suositellaan kohdistamaan ***toimintoihin*, joita organisaatio tarvitsee tuottaakseen joko yhteiskunnan tai oman (liike)toimintansa kannalta kriittisiä palveluita**. Kybermittarin ensisijainen kohde ovat yhteiskunnan toiminnan kannalta huoltovarmuuskriittiset organisaatiot, mutta malli sopii yhtä hyvin kaikenlaisten organisaatioiden käytötön. Tällöin tarkasteltavaksi valitaan esimerkiksi organisaation oman liiketoiminnan kannalta kriittiset toiminnot ja niiden toimintavarmuuden kannalta tärkeimmät riippuvuudet.

Rajaus voidaan toteuttaa monella tapaa, esimerkiksi:

- Kattamaan **koko organisaatio**, esim. pienissä ja keskisuurissa yrityksissä;
- **Organisaatiorakenteen** mukaisesti, esim. maa- tai liiketoimintayksikköön;
- **Toimintojen** mukaisesti, esim. yli organisaatiorajojen tuotettuun palveluun.

Organisaatio voi valita tarkasteluun esimerkiksi tietyn toiminnon tai palvelun, kuten lämmöntuotannon, vesihuollon tai maksuliikennepalvelun, ja näiden toimintojen tuottamisen kannalta kriittiset järjestelmät, prosessit ja tieto-omaisuudet. Toisaalta arviointi voidaan kohdistaa yhtä lailla tiettyyn organisaation osaan, kuten liiketoiminta-alueeseen, yksikköön tai toimintamaahan kerrallaan. Maantieteellistä jaottelua ei suositella paitsi, jos se täyttää jonkin ylläolevista kuvauksista.

Pienet tai keskisuuret toimijat voivat kohdistaa arvioinnin koko organisaation toiminta-alueeseen. Suuremmat toimijat puolestaan voivat rajata arvioinnin koskemaan esimerkiksi tiettyä palvelukokonaisuutta, liiketoimintayksikköä tai yksittäistä tuotantolaitosta. Vaikka Kybermittari soveltuukin kokonaisen organisaation kyberturvallisuuden arviointiin ja kehittämiseen, on suositeltavaa kohdistaa tarkastelu varsinkin suuremmissa organisaatioissa vain yhteen kriittiseen toimintoon tai organisaation osaan kerrallaan. Yhtenä kokonaisuutena käsittely edellyttää, että noudatettavat prosessit ja käytännöt ovat riittävän yhteneväiset koko arvioitavalla toiminnan osa-alueella.

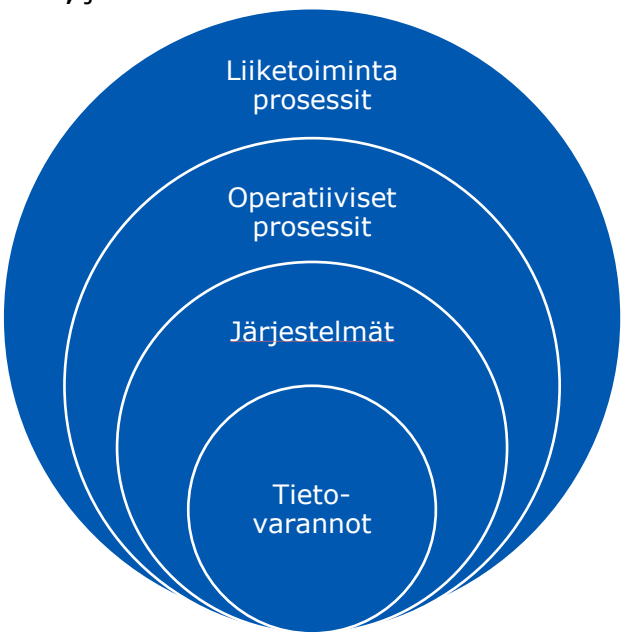
Mikäli halutaan tarkastella kerralla useita toiminnan osa-alueita, on suositeltavaa muodostaa jokaisesta omat arviointinsa. Tällöin yksittäisen arvioinnin tulokset ja kehitystoimenpiteet on helpompi kohdistaa oikein ja arviointiprosessi säilyy maltillisena. Koko organisaation laajuisesti toteutettujen käytäntöjen osalta voidaan hyödyntää samoja vastauksia näissä eri arvioinneissa.

Kriittisten riippuvuuksien tunnistaminen

Kriittisten palveluiden ja toimintojen lisäksi arvioinnin kohteen määrittämiseksi tulee tunnistaa näiden toimintavarmuuden kannalta tärkeimmät riippuvuudet. Tällaisia ovat lähtökohtaisesti kaikki kriittisten palveluiden tuottamiseen liittyvät:

- **Liiketoimintaprosessit ja operatiiviset prosessit**;
- **Järjestelmät ja osajärjestelmät;** ja
- **Tietovarannot**.

Tunnistettavia riippuvuuksia ovat erilaiset järjestelmät, sekä niihin liittyvät osajärjestelmät ja tietovarannot. Riippuvuuksia ovat niin ikään näihin liittyvät ja liiketoimintaprosessit ja operatiiviset prosessit, mukaan lukien sisäiset palvelut ja ulkoisen toimitusketjun tuottamat kriittiset palvelut. Riippuvuuksista kannattaa priorisoida ja valita merkittävimmät sekä dokumentoida nämä valinnat selkeäksi osaksi arviointia.



Kuva 2: Esimerkki lähestymistavasta kriittisten toimintojen ja niiden riippuvuuksien tunnistamiseen.

Riippuvuuksia voidaan tunnistaa lähtemällä liikkeelle prosesseista ja etenemällä niihin liittyviin järjestelmiin ja tietoon. Toisaalta voidaan aloittaa palveluiden ja toimintojen kannalta kriittisestä tiedosta ja edetä sitä kautta kohti järjestelmiä ja prosesseja. Kuva 2 havainnollistaa näitä riippuvuuksia.

Prosessi toiminnan osa-alueen ja riippuvuuksien tunnistamiseen voi olla esimerkiksi:

1. Tunnistetaan organisaation kriittiset toiminnot tai palvelut;
2. Mikäli toimintoja tai palveluita on useita, valitaan näistä ne, joiden osalta arviointi halutaan toteuttaa;
3. Jokaista kriittistä toimintoa tai palvelua kohden tunnistetaan ja listataan näihin liittyvät kriittiset riippuvuudet, mukaan lukien:
    a. Prosessit, jotka ohjaavat kriittisiä toimintoja ja hyödyntävät suojattavia järjestelmiä. Lähde liikkeelle esimerkiksi liiketoimintakriittisten prosessien listauksesta ja kriittisyys-luokittelusta.
    b. Järjestelmät, jotka tuottavat yhteiskunnalle tai organisaatiolle kriittistä toimintoa tai palvelua. Lähde liikkeelle esimerkiksi järjestelmien omaisuusluettelosta ja kriittisyysluokittelusta. Tunnista järjestelmiin liittyvät sisäiset ja ulkoiset riippuvuudet.
    c. Tieto, jota käytetään kriittisten toimintojen tai palveluiden tuottamisessa tai kriittisen järjestelmän toiminnassa. Lähde liikkeelle esimerkiksi suojattavan tiedon omaisuusluettelosta.

Yhteiskunnan kannalta kriittinen palvelu. Palvelu on yhteiskunnalle kriittinen, mikäli sen häiriö vaikuttaa merkittävään asiakasmäärään, laajaan maantieteelliseen alueeseen tai palvelun häiriöllä on vakavia seurannaisvaikutuksia. Kriittisyyden määrittelyssä auttavat esimerkiksi Huoltovarmuuskeskuksen toimialamääritykset.

Organisaation (liike)toiminnan kannalta kriittinen palvelu. Liiketoiminnan kannalta kriittisten palveluiden tunnistaminen kannattaa aloittaa esimerkiksi organisaation tavoitteista tai liiketoimintastrategian painopistealueista.

4.3 Arvioinnin toteutustavasta

Arvioinnin vetäjä auttaa organisaatiota valitsemaan sopivimman toteutustavan. Arviointi voidaan toteuttaa esimerkiksi ohjattuna työpajana tai itsenäisempänä henkilövetoisena arviointina. Arvioitavia osioita voidaan jakaa eri henkilöiden arvioitavaksi. Toteutustavasta riippuen vetäjä huolehtii joko työpajan käytännön järjestelyistä tai koordinoi muutoin arvioinnin toteuttamisen asiantuntijoiden kanssa.

Ohjattu työpajamuotoinen toimintamalli, on malli jossa arvioinnin vetäjä organisoi arvioinnin kutsumalla asiantuntijat koolle yhteen tai useampaan työpajaan.

Vaiheet, joiden koordinoinnista arvioinnin vetäjä vastaa (mahdollisesti yhdessä arvioinnin sponsorin ja organisaation asiantuntijoiden kanssa), ovat:

1. Asiantuntijoiden nimeäminen ja sitouttaminen työpajaan;
2. Aloituskokous (1 h) tai -viesti arviointiin osallistuville henkilöille;
3. Yksi tai useampi työpaja (voidaan toteuttaa myös sarjana työpajoja pienryhmissä, esim. 2-3 h/työpaja)
4. Tulosten kerääminen yhteen ja analysointi viimeistä työpajaa varten;
5. Tulosten läpikäynti, kehityskohteiden tunnistaminen sekä kehitystoimista vastaavien henkilöiden nimeäminen lopputyöpajassa (2 h)

Vetäjä vastaa arvioinnin läpiviennistä, tehtävien koordinoinnista, riittävästä dokumentoinnista ja työpajojen järjestämisestä. Yksi vetäjän keskeisistä tehtävistä on varmistaa, että jokaisessa keskustelussa ja arvioinnin osassa ymmärretään arvioinnin tarkoitus ja laajuus samalla tavalla. Arvioinnin vetäjälle muodostuu prosessin aikana kattava kokonaiskuva organisaation kyberturvallisuuden tilasta.

Ryhmätyömuotoisessa mallissa aloituskokouksen tarkoitus on viestiä osallistujille arvioinnin tarkoituksesta ja toteutusprosessista. Tarkempi perehdytys arvioitaviin aihealueisiin voidaan toteuttaa työpajan tai työpajojen alussa. Aloituskokouksen voi tarvittaessa korvata myös ryhmälle yhteisesti lähetettävällä tiedotteella.

Yhden pidemmän työpajan lisäksi arviointi voidaan toteuttaa sarjana lyhyempiä aihealuekohtaisia työpajoja, jotka toteutetaan pienryhmissä. Näissä voi olla vetäjän lisäksi paikalla esimerkiksi 2-4 henkilöä sisältäen aihealueen asiantuntijat ja arvioinnin sponsori. Työpajoissa käyty keskustelu luo ymmärrystä kyberturvallisuudesta ja ne voivat toimia tiedon jakamiseen suuremmalle joukolle.

Prosessin lopuksi vetäjä kerää tulokset yhteen ja järjestää lopputyöpajan, jossa käydään läpi työkalun tarjoamat raportit. Työpajassa keskustellaan tunnistetuista puutteista sekä sovitaan kehitystoimenpiteiden ja -suunnitelmien vastuista ja aikataulusta. Työpajan agendalle on hyvä nostaa tulosten analysointiin ja raportointiin liittyvät aiheet sekä keskustelu tavoitetasosta.

Työtavan etuna on, että lopputuloksena muodostuu yhteinen tilannekuva ja ymmärrys aihealueen nykytilasta ja mahdollisesta tavoitetasosta. Arvioinnin aikana kaikki Kybermittarin aihealueet keskustellaan läpi ohjatusti ja samalla jaetaan näkemyksiä ja tietoa. Tämä ehkäisee kyberturvallisuusosaamisen henkilöitymistä.

Haasteena on työtavan vaatima aika ja erityisesti kaikille yhteisen toteutusajan löytäminen. Toisaalta sarjamuotoisten työpajojen etuna on, että jokaisessa työpajassa on läsnä pienempi joukko henkilöitä ja vain ne, joilla on aito kytkös käsiteltävään aihealueeseen. Työtapa voi joidenkin roolien osalta tuntua työläältä, mikäli tietyn henkilön odotetaan osallistuvan kaikkiin keskusteluihin.

Henkilövetoinen arviointi on vaihtoehtoinen toteutustapa Kybermittarin arvioinnille. Siinä arvioinnin vetäjä organisoi arvioinnin toteutuksen yksittäisten organisaation asiantuntijoiden kanssa. Laadukkaan itsearvioinnin edellytyksenä on, että arviointia vetämään valitulla henkilöllä on osaamista kyberturvallisuudesta ja mahdollisuus perehtyä Kybermittariin ennen projektin aloittamista.

Vaiheet, joiden koordinoinnista arvioinnin vetäjä vastaa, ovat:

1. Asiantuntijoiden nimeäminen ja sitouttaminen työpajaan;
2. Aloituskokous (1-2 h) arviointiin osallistuville henkilöille
3. Nimetyt asiantuntijat täyttävät itsenäisesti Kybermittarin heille osoitetut aihealueet sovitun aikataulun mukaisesti
4. Tulosten kerääminen yhteen ja analysointi työpajaa varten
5. Tulosten läpikäynti lopputyöpajassa (2-4 h), johon osallistuvat kaikki arvioinnin täyttämiseen osallistuneet henkilöt

Aloituskokouksen tarkoituksena on perehdyttää eri aihealueiden vastuuhenkilöt Kybermittariin, sen käyttämiseen ja aihealueiden tarkoitukseen. Tämän jälkeen henkilöt täyttävät osioita itsenäisesti tai pienissä ryhmissä, riippuen aihealueesta. Arvioinnin vetäjä ohjaa itsenäistä täyttämistä ja tarjoaa tarvittaessa tulkinta-apua. Tulokset palautetaan arvioinnin vetäjälle, joka kokoaa ne yhteen tulosten läpikäynnin lopputyöpajaa varten. Vetäjä pyrkii tunnistamaan merkittävimmät ristiriidat ja puutteet vastauksissa, jotka nostetaan työpajan agendalle.

Lopputyöpajassa vastauksista keskustellaan ja niitä saatetaan hioa vertailukelpoisemmiksi toisiinsa nähden. Työpajassa käydään lopuksi läpi Kybermittarin tuottamat raportit. Raporttien analysoinnin yhteydessä voidaan käydä jo keskustelua tavoitetasosta. Työpajassa tulee sopia, miten tuloksista raportoidaan eteenpäin ja miten edetään kehityssuunnitelman laadintaan.

Työtavan etuina on sen tehokkuus ja keveys, etenkin aikatauluttamisen näkökulmasta, kun ryhmälle tarvitsee sopia vain lyhyehkö aloituskokous ja puolen päivän työpaja tulosten läpikäyntiin. Työtapa toimii etenkin silloin, kun organisaatiossa on selkeästi tunnistettavissa vastuuhenkilöt eri aihealueille tai niiden sisältämille tavoitteille.

Itsenäisen työskentelyn haasteena voi olla, että kyberturvallisuuden vastuut henkilöityvät ja arviointi tuottaa mahdollisesti hajanaisen tilannekuva. Lopun työpajasta tulee työläs, jos eri aihealueet on arvioitu perustuen hyvin erilaisiin olettamuksiin. Edellytyksenä työtavan onnistumiselle on, että arvioinnin kohteena olevan toiminnan osa-alue on selkeästi määritetty ja dokumentoitu ja se viestitään kaikille arviointiin osallistuville.

4.4 Arviointitulokset ja raportit

Kybermittarin automaattiset raportit tukevat arviointitulosten analysointia ja tulosten hyödyntämistä. Raportteja on mahdollista rikastaa erilaisilla referenssi- ja vertailutiedoilla ja hyödyntää niitä sopivien tavoitetasojen asettamisessa. Työkalu muodostaa kolme raporttia, joista jokainen kuvaa organisaation kypsyystasoa hiukan eri näkökulmista tai eri tarkkuustasolla. Nämä raportit ovat:

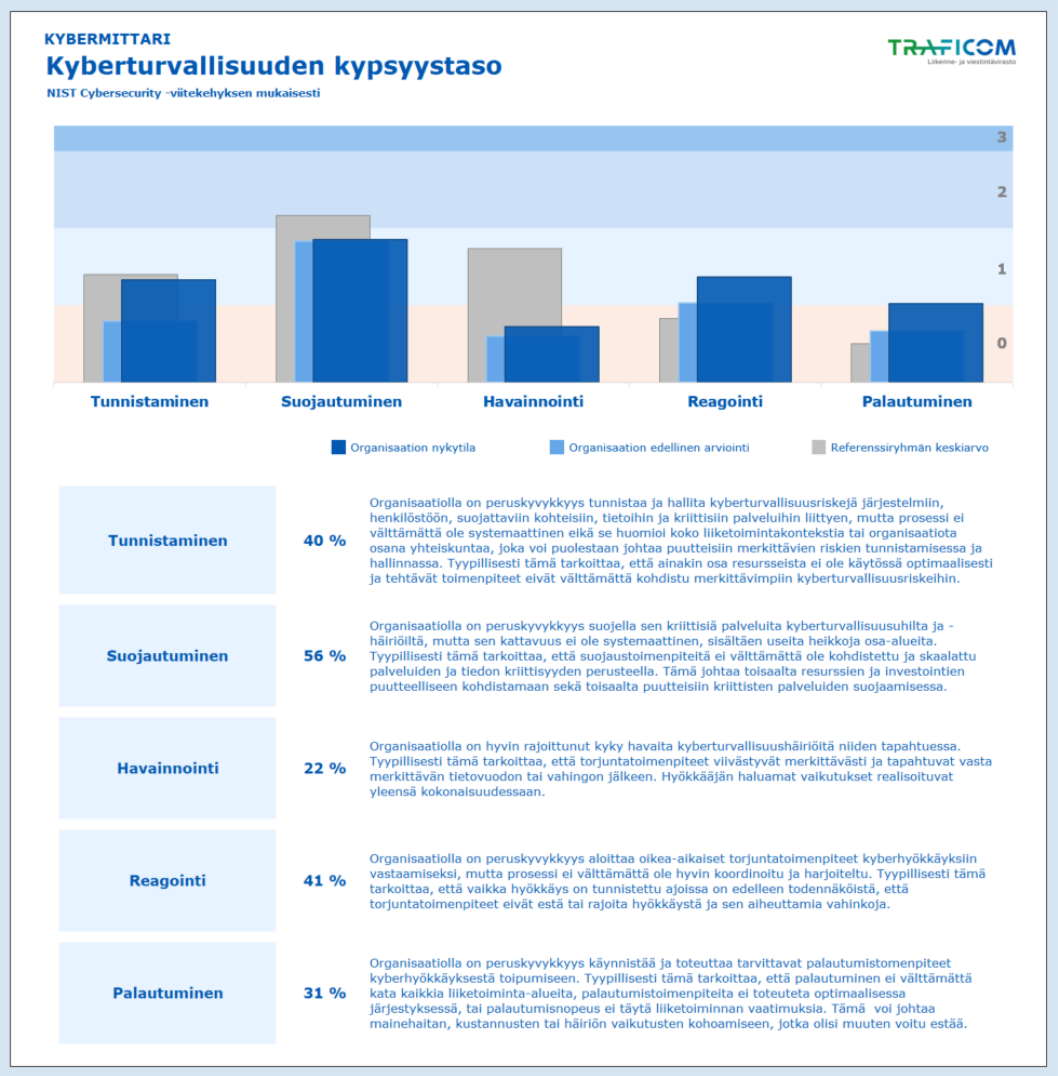
1. **Johdolle suunnattu kypsyysraportti** on yleistason raportti, joka on suunnattu nimensä mukaisesti johdon raportointiin tai käytettäväksi esimerkiksi ulkoisessa viestinnässä; sekä

2. **Kybermittarin kypsyysraportti** on tekninen raportti, joka on suunnattu kyberturvallisuuden ja riskienhallinnan ammattilaisille sekä muille teknisille vastuuhenkilöille käytettäväksi esimerkiksi organisaation nykytilan, tavoitetilan määrittämiseen ja kehitystoimenpiteiden tunnistamiseen;

3. **Yksityiskohtainen NIST Cybersecurity Framework Core -raportti** on toinen tekninen raportti, joka esittää Kybermittarin arviointitulokset NIST-mallin mukaisena lopputuloksena. Raportti on suunnattu esimerkiksi organisaatioille, jotka jo käyttävät jotain toista NIST-pohjaista arviointimallia tai haluavat muutoin analysoida tai viestiä tuloksia tätä mallia käyttäen.

Raportteja voidaan rikastaa referenssi- ja vertailutiedolla esimerkiksi organisaation edellisen arvioinnin tuloksilla tai toimialan keskimääräisillä kypsyystuloksilla. Samaa ominaisuutta voidaan vaihtoehtoisesti hyödyntää esimerkiksi organisaation tavoitetason visualisoimiseksi.

Johdolle suunnattu kypsyysraportti on tarkoitettu erityistesti arviointitulosten raportointiin organisaatiojohdolle sekä tukemaan sisäistä ja ulkoista viestintää.



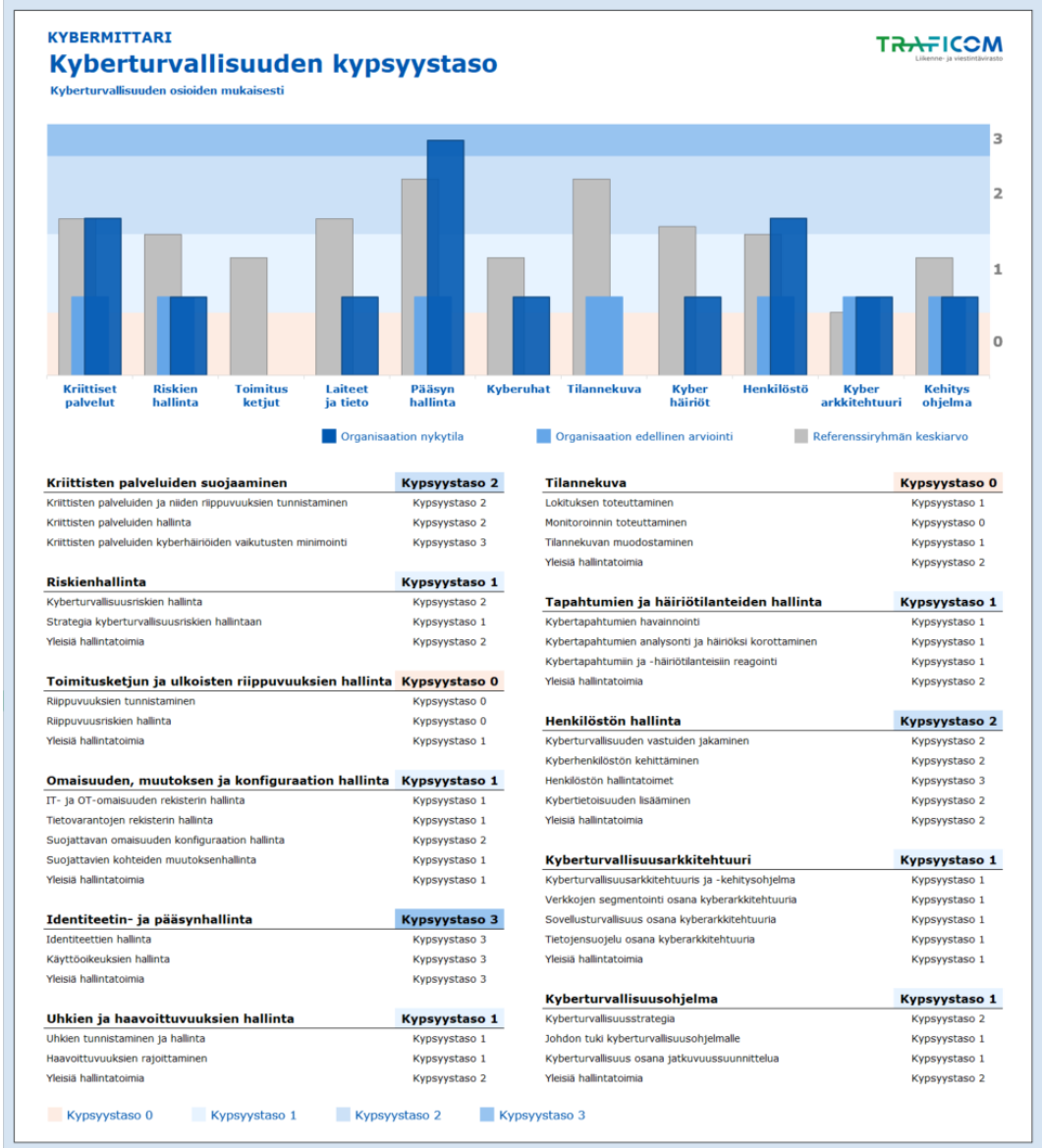
Kuva 3: Kybermittarin johdolle suunnattu kypsyysraportti, joka pohjautuu viiteen kyvykkyyteen: tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen.

Tulokset esitetään viiden NIST Cybersecurity -viitekehyksen mukaisen kyvykkyyden mukaisesti: tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen. Jokaisen kyvykkyyden kypsyystaso esitetään prosenttiosuutena, jotka on vielä jaoteltu erikseen tasoille nollasta kolmeen. Jokaisen kyvykkyyden osalta on kuvattu vielä erikseen sanallisesti, mitä saavutettu tulos voisi käytännössä tarkoittaa.

Kypsyysmalli ja ristiin kytkentä. Kypsyystasot määritetään toteutuneiden Kybermittarin käytäntöjen perusteella. Käytännöt on ensin ristiin kytketty soveltuvin osin NIST-viitekehyksen käytäntöihin. Kunkin viiden kyvykkyyden kypsyystaso lasketaan sitten toteutuneiden käytäntöjen mukaisesti: taso 0 tarkoittaa, että alle 30% kyvykkyyteen viittaavista käytännöistä on toteutettu (vastaavasti taso 1 alle 60%, taso 2 alle 90% ja taso kolme yli 90%).

Huomionarvoista on, että NIST-viitekehys ei ole kypsyysmalli, joten ristiin kytkentä ja kypsyystasot ovat vain suuntaa-antavia. Ristiin kytkentä Kybermittarin ja NIST-viitekehyksen käytäntöjen välillä löytyy Kybermittarin arviointityökalusta.

Kybermittarin kypsyysraportti on yksityiskohtaisempi Kybermittarin raportti, joka on tarkoitettu arviointitulosten analysointiin, raportointiin ja sisäisen kehitystyön ohjaamiseen. Raportti on suunnattu erityisesti kyberturvallisuuden ja riskienhallinnan ammattilaisille sekä muille teknisille vastuuhenkilöille.

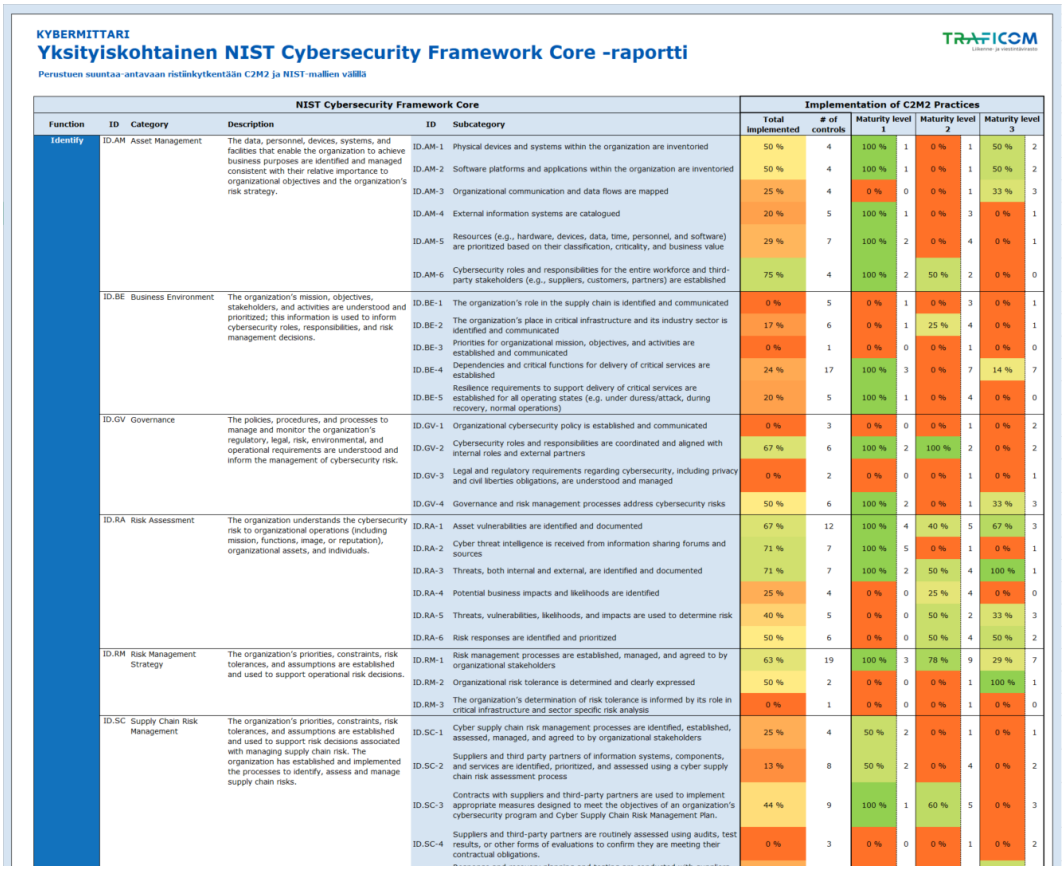


Kuva 4: Kybermittarin kyberturvallisuuden kypsyysraportti, joka pohjautuu yhteentoista kyberturvallisuuden osioon ja esittää konkreettiset kehitysalueet.

Tulokset esitetään yhdentoista Kybermittarin kyberturvallisuuden kyvykkyyden mukaisesti. Jokaisen kyvykkyyden kypsyystaso esitetään tasoille nollasta kolmeen. Osiokohtaisen kuvaajan lisäksi, raportti esittää jokaisen tavoitteen kypsyystason.

Kypsyysmalli. Kypsyystasojen laskentamalli noudattaa kappaleessa 3.3 kuvattua Kybermittarin laskentamallia. Huomionarvoista on, että C2M2-mallin pisteytykseen verrattuna Kybermittari käyttää kevennettyä arviointia kypsyystasoilla 2 ja 3. Tason voi saavuttaa, kun vähintään 50% kyseisen tason käytännöistä on täytetty kunkin tavoitteen osalta. Myös tämä on tarkemmin kuvattu kappaleessa 3.3.

Yksityiskohtainen NIST Cybersecurity Framework Core -raportti on yksityiskohtaisempi raportti, joka on tarkoitettu arviointitulosten analysointiin, raportointiin ja sisäisen kehitystyön ohjaamiseen. Raportti on suunnattu erityisesti kyberturvallisuuden ja riskienhallinnan ammattilaisille sekä muille teknisille vastuuhenkilöille ja niille organisaatioille, joilla on aiempaa kokemusta NIST-viitekehyksen käytöstä.



KYBERMITTARI

Yksityiskohtainen NIST Cybersecurity Framework Core -raportti

Perustuen suuntaa-antavaan ristiinkytkentään C2M2 ja NIST-mallien välillä

NIST Cybersecurity Framework Core						Implementation of C2M2 Practices							
Function	ID	Category	Description	ID	Subcategory	Total implemented	# of controls	Maturity level 1		Maturity level 2		Maturity level 3	
Identify	ID.AM	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1	Physical devices and systems within the organization are inventoried	50 %	4	100 %	1	0 %	1	50 %	2
				ID.AM-2	Software platforms and applications within the organization are inventoried	50 %	4	100 %	1	0 %	1	50 %	2
				ID.AM-3	Organizational communication and data flows are mapped	25 %	4	0 %	0	0 %	1	33 %	3
				ID.AM-4	External information systems are catalogued	20 %	5	100 %	1	0 %	3	0 %	1
				ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	29 %	7	100 %	2	0 %	4	0 %	1
				ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	75 %	4	100 %	2	50 %	2	0 %	0
	ID.BE	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1	The organization's role in the supply chain is identified and communicated	0 %	5	0 %	1	0 %	3	0 %	1
				ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	17 %	6	0 %	1	25 %	4	0 %	1
				ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	0 %	1	0 %	0	0 %	1	0 %	0
				ID.BE-4	Dependencies and critical functions for delivery of critical services are established	24 %	17	100 %	3	0 %	7	14 %	7
				ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	20 %	5	100 %	1	0 %	4	0 %	0
	ID.GV	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1	Organizational cybersecurity policy is established and communicated	0 %	3	0 %	0	0 %	1	0 %	2
				ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	67 %	6	100 %	2	100 %	2	0 %	2
				ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	0 %	2	0 %	0	0 %	1	0 %	1
				ID.GV-4	Governance and risk management processes address cybersecurity risks	50 %	6	100 %	2	0 %	1	33 %	3
	ID.RA	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1	Asset vulnerabilities are identified and documented	67 %	12	100 %	4	40 %	5	67 %	3
				ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	71 %	7	100 %	5	0 %	1	0 %	1
				ID.RA-3	Threats, both internal and external, are identified and documented	71 %	7	100 %	2	50 %	4	100 %	1
				ID.RA-4	Potential business impacts and likelihoods are identified	25 %	4	0 %	0	25 %	4	0 %	0
				ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	40 %	5	0 %	0	50 %	2	33 %	3
				ID.RA-6	Risk responses are identified and prioritized	50 %	6	0 %	0	50 %	4	50 %	2
	ID.RM	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	63 %	19	100 %	3	78 %	9	29 %	7
				ID.RM-2	Organizational risk tolerance is determined and clearly expressed	50 %	2	0 %	0	0 %	1	100 %	1
				ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	0 %	1	0 %	0	0 %	1	0 %	0
	ID.SC	Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	25 %	4	50 %	2	0 %	1	0 %	1
				ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	13 %	8	50 %	2	0 %	4	0 %	2
				ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	44 %	9	100 %	1	60 %	5	0 %	3
				ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	0 %	3	0 %	0	0 %	1	0 %	2

Kuva 5: Kybermittarin yksityiskohtainen raportti, joka esittää tulokset ja kehitysalueet NIST-viitekehyksen mukaisten käytäntöjen perusteella.

Ristiin kytkentä. Raportin esittämät prosentit ja luvut perustuvat toteutettuihin Kybermittarin käytäntöihin. Käytännöt on ensin ristiin kytketty soveltuvin osin NIST-viitekehyksen käytäntöihin. Prosenttiosuudet lasketaan vertaamalla kunkin kohdan osalta toteutuneita käytäntöjä kaikkiin kyseiseen kohtaan soveltuviin käytäntöihin.

Huomionarvoista on, että ristiin kytkentä on vain suuntaa antava, sillä NIST-viitekehys ei pidä sisällään kypsyysmallia eikä se kata kaikkia Kybermittarin osioita. Ristiin kytkentä Kybermittarin ja NIST-viitekehyksen käytäntöjen välillä löytyy Kybermittarin arviointityökalusta.

Ne kohdat, joissa esitetään nolla käytäntöä tai prosenttia tarkoittavat, että vastaavaa kohtaa ei löydy Kybermittarista.

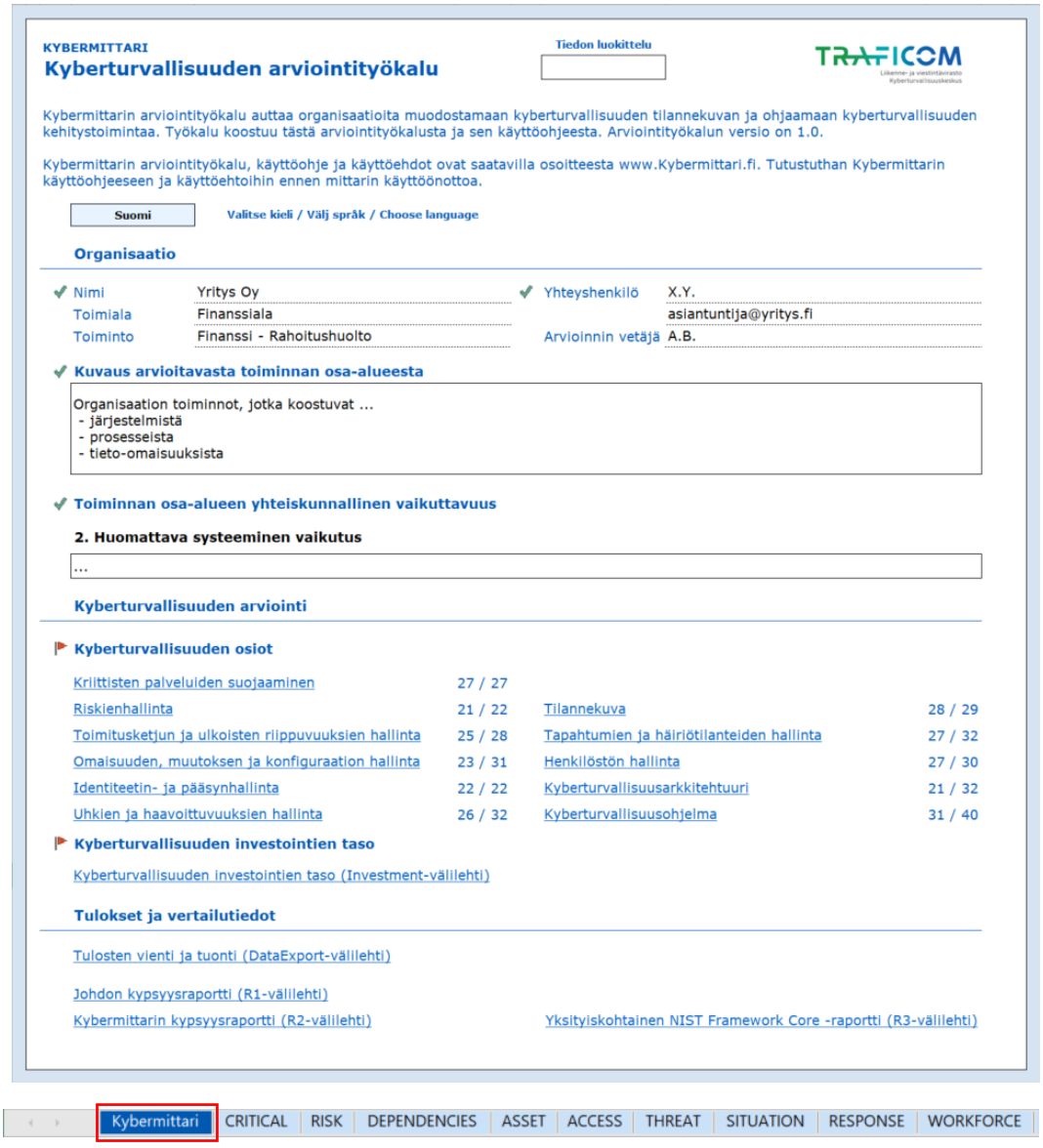
5 Yksityiskohtainen Kybermittarin arviointityökalun täyttöohje

Tämä kappale tarjoaa yksityiskohtaista ohjeistusta Kybermittari-työkalun käyttöön ja tietojen syöttämiseen. Työkalu tukee arvioinnin toteuttamista ja ohjaa arviointiprosessia. Ohjeistus on tarkoitettu erityisesti tukemaan arvioinnin vetäjää ja muita arviointiin osallistuvia tahoja työkalun tehokkaaseen hyödyntämiseen.

5.1 Kybermittari-välilehti

Kybermittari-välilehdeltä löytyvät:

- Työkalun kielivalinta (suomi, ruotsi tai englanti);
- Tiedon luokittelu organisaation määrittelemänä;
- Organisaatio ja toiminnan osa-alue; ja
- Kyberturvallisuuden arviointi, tulokset ja vertailutiedot.



Kuva 6: Kybermittarin arviointityökalun ensimmäinen välilehti, joka esittää yleisnäkymän arvioinnin kohteesta ja tilanteesta.

Työkalun kieleksi voi valita suomen, ruotsin tai englannin. Työkalun tekstit vaihtuvat dynaamisesti vastaamaan valittua kieltä, lukuun ottamatta alasveto-valikoiden vaihtoehtoja (esim. arviointiosioiden vastausvaihtoehtojen käännökset).

Tiedon luokittelu -kohtaan voidaan dokumentoida tiedon luokittelu. Tyypillisesti luokittelun tekee arvioinnin kohteena oleva organisaatio arvioinnin yhteydessä tai sen päätteeksi. Tiedon luokittelu -kohtaa voivat käyttää myös esimerkiksi viranomaiset luokitellessaan heille luovutettuja asiakirjoja.

Organisaatio ja toiminnan osa-alue -kohdassa dokumentoidaan arvioinnin kohteena oleva organisaatio ja arvioitava toiminnan osa-alue. Näiden osalta dokumentoidaan seuraavat tiedot:

- Organisaation nimi, toimiala ja toiminto;
- Yhteyshenkilö ja arvioinnin vetäjä;
- Kuvaus arvioitavasta toiminnan osa-alueesta, johon arviointi kohdistuu; ja
- Toiminnan osa-alueen yhteiskunnallinen vaikuttavuus.

Kyberturvallisuuden arviointi ja **tulokset ja vertailutiedot** -kohdat esittävät näkymän arvioinnin tilanteesta ja tarjoavat suorat linkit sekä arvioinnin osioihin, että loppuraportteihin.

Täyttöohje: täytä välilehdelle organisaation nimi, toimiala (esim. logistiikka) ja toiminto (esim. maakuljetus). Toimialojen ja toimintojen luokittelu noudattelee Huoltovarmuuskeskuksen määrittämiä huoltovarmuuskriittisiä toimialoja ja näiden toimialapooleja. Vaihtoehdot on esitetty taulukossa 2.

Mikäli organisaatio ei tunnista luokitteluaan kyseiseltä listalta, valitaan vaihtoehdoksi molempiin valikoihin "ei-hvk toimiala". Luokittelu tukee myöhempää tilastointia ja vertailutiedon muodostamista, eivätkä ne vaikuta itse arviointiin tai arvioinnin lopputulokseen.

Täytä lisäksi organisaation yhteyshenkilö ja arvioinnin vetäjänä toiminut henkilö ja organisaatio. Näitä tietoja tarvitaan jälkeenpäin mahdollisia tarkentavia kysymyksiä tai selvityksiä varten.

Täytä kuvaus arvioinnin kohteena olevasta toiminnan osa-alueesta, mkl. kriittiset riippuvuudet kuten prosessit, järjestelmät ja tietovarannot. Tarkempia ohjeita toiminnan osa-alueen ja kriittisten riippuvuuksien määrittämiseen löytyy kappaleesta 4.2. Kuvaus toiminnan osa-alueesta dokumentoidaan tulosten analysointia ja vertailua varten. Tämä on erityisen tärkeää, jotta myöhemmin tiedetään mihin toimintoihin, järjestelmiin, prosesseihin ja tieto-omaisuuksiin arviointi kohdistui.

Taulukko 2: Kybermittarin tilastointia varten käyttämät huoltovarmuuskriittisten toimialojen ja toiminnan osa-alueiden määritelmät.

Kriittinen toimiala	Kriittinen toiminnan osa-alue
Elintarvikehuolto	*Alkutuotanto* *Elintarviketeollisuus* *Kauppa ja jakelu*
Finanssiala	*Rahoitushuolto* *Vakuutusala*
Kriittinen teollisuustuotanto	*Kemia* *Metsä* *MIL* *Muovi ja kumi* *Rakennus* *Teknologia*
Logistiikka	*Ilmakuljetus* *Maakuljetus* *Vesikuljetus*
Terveydenhuolto	*Terveydenhuolto* *Vesihuolto*
Tietoyhteiskunta	*Digi* *Media*
Ei huoltovarmuus-kriittinen toimiala	*Toiminta, joka koskee jotain muuta kuin huoltovarmuuskriittistä toimintaa*

Täytä vielä arvio toiminnan osa-alueen yhteiskunnallisesta vaikuttavuudesta tilanteessa, jossa palvelu tai toiminta olisi pois käytöstä. Tämä koskettaa niitä organisaatioita, jotka tuottavat *yhteiskunnan kannalta kriittisiä palveluita*. Vaikutusta kuvataan kolmen valittavan vaihtoehdon kautta sekä vapaamuotoisella tarkentavalla kuvauksella. Valittavat vaihtoehdot ovat:

1. **Vähäinen systeeminen vaikutus:** Vaikutus kohdistuu vain organisaatioon itseensä tai vain vähäiseen määrään kumppaneita ja/tai asiakasorganisaatioita, tai vaikutus rajautuu alle 50 000 kansalaiseen.

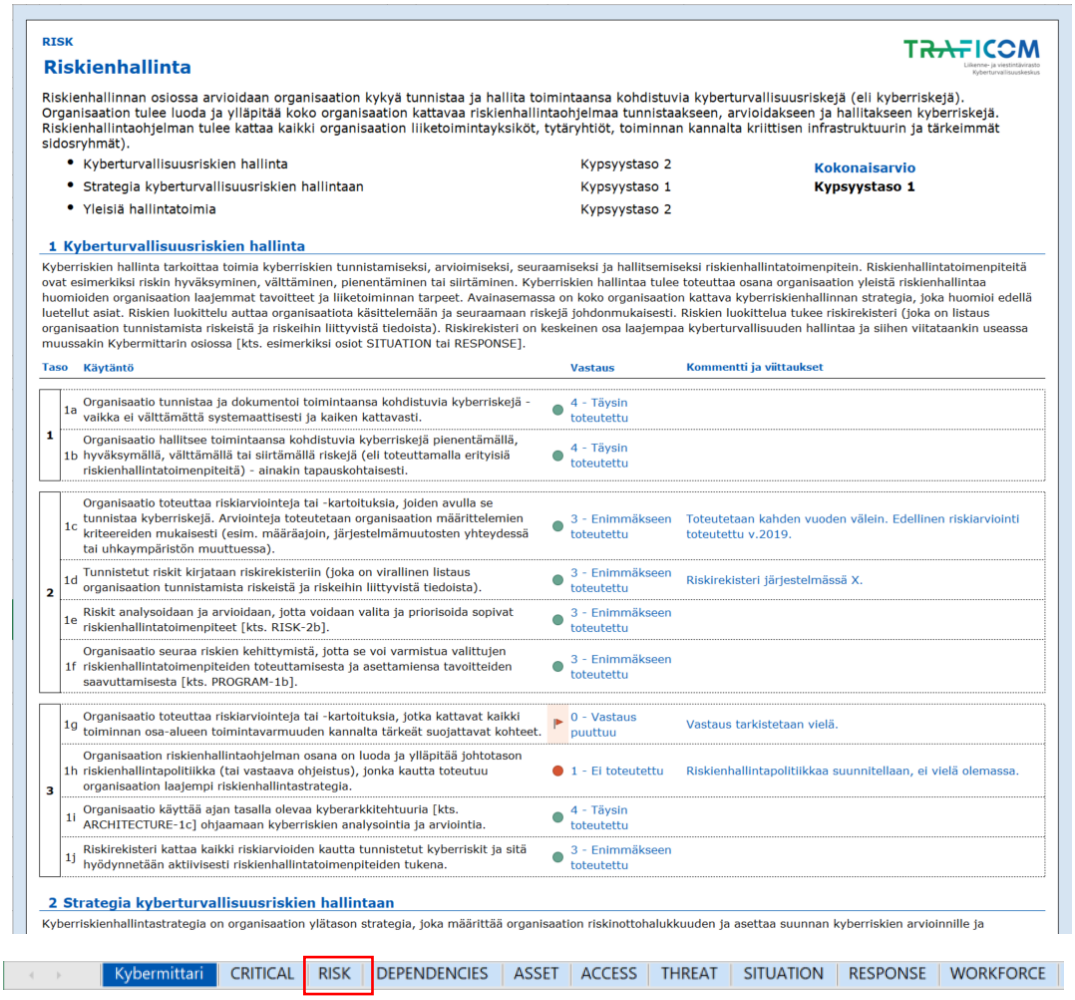
2. **Huomattava systeeminen vaikutus:** Toiminta vaikeutuu huomattavalle määrälle kumppaneita ja/tai asiakasorganisaatioita tai yli 50 000 kansalaisen elämä vaikeutuu tai he kärsivät vahinkoja.

3. **Rampauttava systeeminen vaikutus:** Rampauttaa yhteiskunnan perustoimintoja tai aiheuttaa vahinkoa yli 100 000 kansalaiselle.

Kun organisaatio ja arvioitava toiminnan osa-alue on dokumentoitu, voidaan edetä täydentämään osiokohtaisia välilehtiä.

5.2 Osiokohtaiset välilehdet

Yksitoista kyberturvallisuuden osiota löytyvät kukin omalta välilehdeltään. Kybermittari-välilehti sisältää suorat linkit sekä tilannekuvan kustakin osiosta.



Kuva 7: Esimerkki Kybermittarin arviointityökalun osiokohtaisesta välilehdestä, joita on Kybermittarissa yhteensä yksitoista.

Jokainen välilehti pitää sisällään seuraavat kohdat:

- Osion nimen, esittelyn ja yhteenvedon osiolle asetetuista tavoitteista;
- Jokaista tavoitetta kohden nimi, esittely sekä asetetut käytännöt; ja
- Jokaista käytäntöä kohden (vasemmalta oikealle):
    - Kypsyystaso, käytännön tunniste ja kuvaus;
    - Vastausvaihtoehto 1-4 (monivalinta); ja
    - Tilaa kommenteille ja viittauksille (vapaa tekstikenttä).

Täyttöohje: arviointi tapahtuu vastaamalla esitettyihin käytäntöihin sopivalla vastausvaihtoehdolla. Vastausvaihtoehdoista ja niiden soveltamisesta on kerrottu enemmän kappaleessa 3.3. Kommentit ovat vapaavalintaisia.

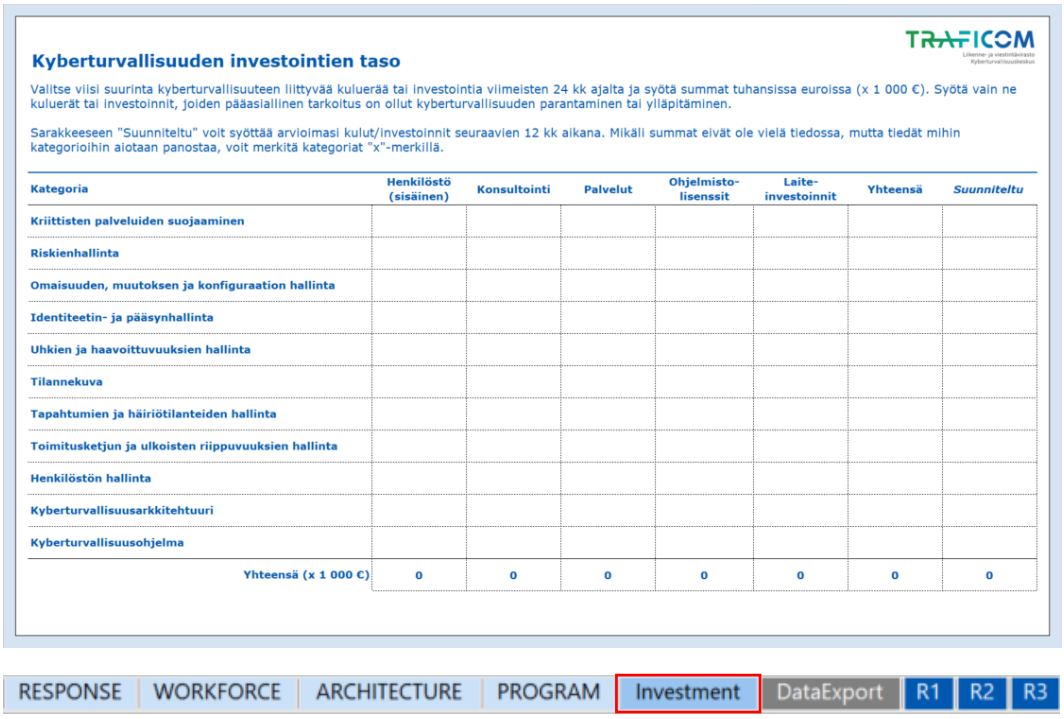
Työkalu laskee annettujen vastausten perusteella automaattisesti kypsyystason kyseisen tavoitteen, osion ja koko organisaation kohdalta sitä mukaa kun työkalua täytetään.

Osiot voidaan arvioida missä tahansa järjestyksessä, mutta on suositeltavaa aloittaa osiosta "Kriittisten palveluiden suojaaminen". Kyseinen osio antaa hyvän pohjan myöhempien osioiden tulkintaan.

Kun arvioinnin kaikki osiot on täydennetty, voidaan edetä arvioimaan investointien taso ja tarkastelemaan mallin tuottamia arviointituloksia.

5.3 Investoinnit-välilehti

Kyberturvallisuuden investointien taso löytyy omalta välilehdeltään. Tämän välilehden tarkoituksena on arvioida kyberturvallisuuteen käytettävien investointien ja kustannusten suuruutta ja kategorisoida ne Kybermittarin avulla arvioitavien osioiden mukaisesti. Tämä mahdollistaa investointien vaikuttavuuden analysoinnin, kun arvioinnin lopuksi verrataan kunkin aihealueen saavutettua kypsyystasoa tehtyihin investointeihin.



Kyberturvallisuuden investointien taso

Valitse viisi suurinta kyberturvallisuuteen liittyvää kuluerää tai investointia viimeisten 24 kk ajalta ja syötä summat tuhansissa euroissa (x 1 000 €). Syötä vain ne kuluerät tai investoinnit, joiden pääasiallinen tarkoitus on ollut kyberturvallisuuden parantaminen tai ylläpitäminen.

Sarakkeeseen "Suunniteltu" voit syöttää arvioimasi kulut/investoinnit seuraavien 12 kk aikana. Mikäli summat eivät ole vielä tiedossa, mutta tiedät mihin kategorioihin aiotaan panostaa, voit merkitä kategoriat "x"-merkillä.

Kategoria	Henkilöstö (sisäinen)	Konsultointi	Palvelut	Ohjelmisto-lisenssit	Laite-investoinnit	Yhteensä	*Suunniteltu*
Kriittisten palveluiden suojaaminen							
Riskienhallinta							
Omaisuuden, muutoksen ja konfiguraation hallinta							
Identiteetin- ja pääsynhallinta							
Uhkien ja haavoittuvuuksien hallinta							
Tilannekuva							
Tapahtumien ja häiriötilanteiden hallinta							
Toimitusketjun ja ulkoisten riippuvuuksien hallinta							
Henkilöstön hallinta							
Kyberturvallisuusarkkitehtuuri							
Kyberturvallisuusohjelma							
Yhteensä (x 1 000 €)	0	0	0	0	0	0	0

Kuva 8: Kybermittarin arviointityökalun kyberturvallisuuden investointien välilehti, jolla kerätään tietoa kunkin osion investoinneista ja niiden laadusta.

Täyttöohje: taulukkoa täytettäessä on huomioitava seuraavat asiat:

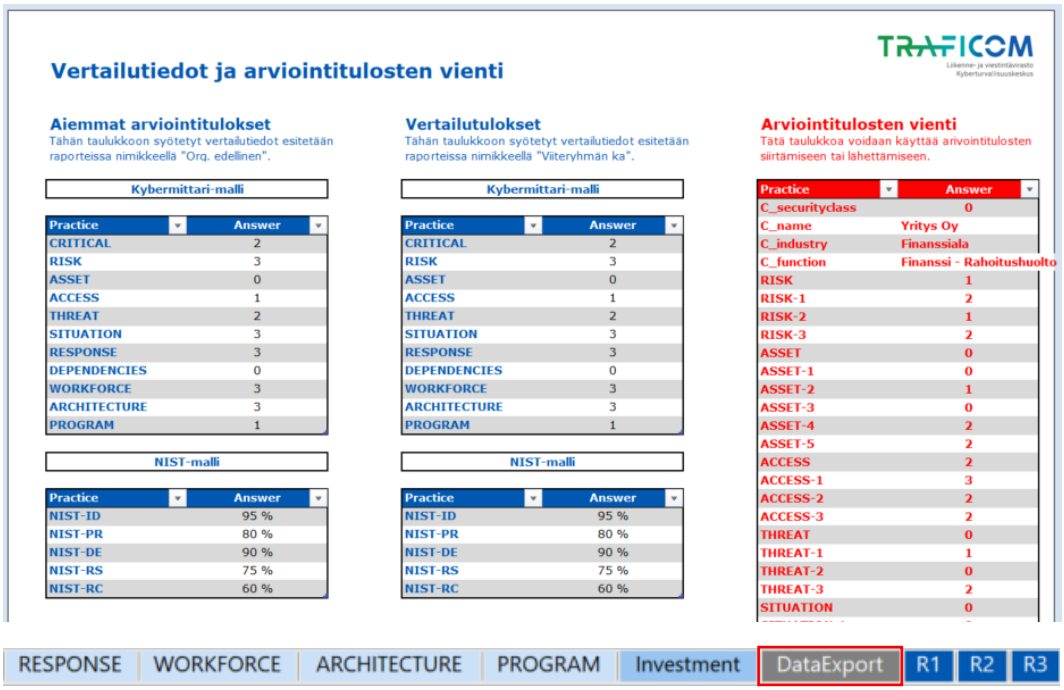
- Investointien tarkastelujakso on viimeiset 24 kuukautta;
- Summat kirjataan tuhansissa euroissa (x 1 000 €);
- Investoinneista ja kustannuksista kirjataan vain ne, joiden pääasiallinen syy on ollut kyberturvallisuuden kehittäminen tai ylläpito. Kyberturvallisuuteen liittyviä kyvykkyyksiä ja toiminnallisuuksia, jotka tulevat muun syyn takia tehdyssä investoinnissa tai kustannuksissa, ei kirjata mukaan; ja
- Tarkastelu suositellaan rajaamaan esimerkiksi 5-10 suurimpaan kuluerään.

Taulukon "Suunniteltu"-sarakkeeseen on puolestaan tarkoitus kerätä tiedot suunnitelluista menoista tulevien 12 kuukauden aikana. Kirjaa ylös vain ne menot, jotka on jo hyväksytty tai jotka ovat niin pitkällä prosessissa, että hyväksyntä vaikuttaa todennäköiseltä. Mikäli summat eivät ole vielä kuitenkaan selvillä, riittää että merkitset rastilla kategorian johon menot kohdistuvat. Täyttämistä helpottaa, mikäli arvioinnissa käydään ensin läpi kypsyysmallin osiot, jotta tiedetään mitä kukin rivi kustannustaulukossa pitää sisällään.

5.4 Raportit ja vertailutiedot

Kybermittarin arviointityökalu tuottaa arvioinnin pohjalta kolme automaattista raporttia. Lisäksi työkalu tukee raporttien rikastamista ulkopuolelta tuodulla vertailutiedolla sekä arviointitulosten vientiä .xml-muodossa.

Vertailutiedot. Arviointityökalun tuottamia raportteja voi rikastaa lisäämällä työkaluun vertailutietoa Tulokset-välilehden kautta. Tiedot luetaan automaattisesti työkalun tuottamiin raportteihin.



Kuva 9: Kybermittarin arviointityökalun tulokset välilehti, jonka valmiiden taulukoiden avulla voidaan joko viedä/tallentaa tuloksia Kybermittarista tai rikastaa automaattisia raportteja.

Täyttöohje: merkittyihin kenttiin voidaan kopioida tai kirjoittaa halutut vertailuarvot. Kenttiin syötetyt arvot näkyvät automaattisesti tuotetuissa raporteissa.

Tulokset-välilehdellä on paikka kaksille vertailutuloksille. Kohdat on nimetty "Aiemmat tulokset" ja "Vertailutulokset", mutta organisaatio voi hyödyntää kohtia haluamallaan tavalla.

Arviointitulosten vienti. Arviointityökalun muodostamat arviointitulokset on mahdollista siirtää työkalusta toiseen muotoon, esimerkiksi säilömistä tai lähettämistä varten. Siirrettäviin arviointituloksiin sisältyy

- Organisaation perustiedot, jotta tulokset osataan kohdistaa ja tulkita myöhemmin oikein;
- Numeeriset tulokset jokaisen kunkin osion, tavoitteen ja käytännön osalta, mutta ei kommentteja tai sisäisiä viittauksia; ja
- Numeeriset arvot kyberturvallisuuden investointien tasoista.

Organisaation täyttämät kommentit, viittaukset tai henkilötiedot, eivät sisälly arviointitulosten siirtoon.

Tulokset-välilehdellä on valmis taulukko arviointituloksista. Taulukko päivittyy automaattisesti arvioinnissa annettujen vastausten perusteella.

Käyttöohje: arviointitulokset voidaan siirtää taulukosta joko viemällä tulokset työkalusta .xml-muodossa - tai kopioimalla tulokset leikepöydän kautta toiseen työkaluun.

Huom.! Mikäli taulukon arvoja muokataan tai niiden päälle kirjoitetaan muita arvoja, eivät arviointitulokset välttämättä päivity enää aiotulla tavalla.

Automaattiset raportit. Arviointityökalu muodostaa täytettyjen vastausten ja mahdollisten vertailutietojen perusteella kolme automaattisesti päivittyvää raporttia:

- Kybermittarin kypsyysraportti (R1-välilehti);
- Johdolle suunnattu kypsyysraportti (R2-välilehti); ja
- Yksityiskohtainen NIST-viitekehyksen kypsyysraportti (R3-välilehti).

Käyttöohje: raporttien tieto luetaan piilotetulta *Data*-välilehdeltä (arviointitulosten osalta) sekä *Tulokset*-välilehdeltä (vertailutietojen osalta), edellä mainituista kohdista. Raportit päivittyvät automaattisesti osiokohtaisille välilehdille annettujen vastausten ja syötetyn vertailutiedon perusteella.

6 Sanasto

Kybermittarin keskeisimmät termit on koottu erilliseksi sanastoksi. Tämän osion tarkoituksena ei ole tarjota kattava kyberturvallisuuden sanasto ja näin ollen sen ulkopuolelle voi jäädä termejä, joiden ymmärtäminen on välttämätöntä Kybermittarin arvioinnin laatimisessa. Tämän vuoksi organisaatioita suositellaan hyödyntävän virallisia Sanastokeskuksen julkaisemia dokumentteja Kyberturvallisuuden sanasto (TSK 52) sekä Kokonaisturvallisuuden sanasto (TSK 50). Sanastot ovat saatavissa suomeksi, ruotsiksi ja englanniksi Sanastokeskuksen internetsivulta osiosta julkaisut.

Termi	***Selite***
C2M2 (Cybersecurity Capability Maturity Model)	Yhdysvaltain energiaviraston ylläpitämä kyberturvallisuuden kyvykkyyden kypsyysmalli. C2M2 tukee organisaatiota havainnoimaan, kohdistamaan, hallinnoimaan ja toteuttamaan kyberturvallisuuden käytäntöihin liittyviä haasteita. C2M2 on yksi Kybermittarin pohjalla käytetyistä viitekehyksistä.
Huoltovarmuuskriittinen organisaatio	Organisaatio, joka on erityisen merkittävä yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta. Huoltovarmuus-kriittinen organisaatio voi olla yritys tai muu organisaatio. Kybermittarin pääasiallinen tavoite on kehittää näiden kriittisten toimijoiden varautumista ja tästä johtuen Kybermittarissa viitataan näihin organisaatioihin ja niiden tuottamiin yhteiskunnallisesti kriittisiin palveluihin ja toimintoihin. On tärkeä huomata, että Kybermittari soveltuu käytettäväksi yhtä lailla ei-huoltovarmuuskriittisten organisaatioiden arviointiin. Tällöin Kybermittarin yhteydessä käytetyt viittaukset kriittisillä palveluilla ja toiminnoilla tulee tulkita tarkoittamaan esimerkiksi organisaation oman liiketoiminnan kannalta kriittistä palvelua tai toimintaa.
IT-järjestelmä	Informaatioteknologian järjestelmä
Kybermittari	Kybermittari on Traficomin Kyberturvallisuuskeskuksen ja Huoltovarmuuskeskuksen tuottama työkalu, jonka avulla organisaation on mahdollista arvioida kyberturvallisuuden kypsyystasoa arviointina.
Kyberriski, Kyberturvallisuusriski, *”Cyber security risk”*	Kokonaisuus, jossa yhdistyy kybertoimintaympäristön, kyberuhan ja kyberturvallisuuden mahdollinen negatiivinen vaikutus organisaation toimintakykyyn. Esimerkkinä kyberriskistä on, tapahtumaketju, jossa motivoitunut uhkatoimija hyödyntää organisaation toiminnan haavoittuvuutta toteuttaakseen haitallisen toimenpiteen, joka aiheuttaa vahingon ja vaarantaa organisaation kriittisen omaisuuden kuten tiedon tai tuotantoprosessin.
Kyberriskienhallinta, Kyberturvallisuus-	Ennakoiva prosessi, jonka avulla varaudutaan organisaation toimintaan kohdistuviin

riskienhallinta, *"Cyber security risk management"*	kyberturvallisuusuhkiin. Kyberturvallisuuden riskienhallinnassa riskit tunnistetaan, arvioidaan ja käsitellään sekä ne raportoidaan ja niitä seurataan säännöllisesti.
Kybertoimintaympäristö, *"Cyber environment"*	Yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva kokonaisuus, jossa organisaation tiedonkäsittely toteutetaan. Organisaation kybertoimintaympäristö muodostuu teknisistä ja teknologisista valinnoista, toimialan erityispiirteistä sekä yhteyksistä organisaation ulkopuolisiin sidosryhmiin kuten viranomaisiin, sopimuskumppaneihin ja asiakkaisiin.
Kyberturvallisuus, *"Cyber security"*	Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus eroaa perinteisestä tietoturvallisuudesta siinä, että se on laajempi kokonaisuus, jossa tavoitteena on hallita myös fyysiseen turvallisuuteen kohdistuvia uhkia.
Kyberturvallisuus-arkkitehtuuristrategia	Kyberturvallisuusarkkitehtuurille asetetut tavoitteet, prioriteetit, vastuut ja seurantaprosessi. Sen pitää olla linjassa yleisen kyberturvallisuusstrategian ja yritysarkkitehtuurin kanssa.
Kyberturvallisuus-strategia	Määrittelee organisaation kyberturvallisuustavoitteet, tavoitteiden prioriteetin, vastuut ja seurannan. Se voi olla dokumentoitu erillisenä dokumenttina, mutta on usein dokumentoitu johdon asettamassa kyberturvallisuuspolitiikassa (tietoturvapolitiikassa).
Kyberuhka, Kyberturvallisuusuhka *"Cyber threat"*	Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon. Kyberuhka voi aiheuttaa organisaatiolle kyberturvallisuusriskin. Esimerkkinä kyberuhkasta etähallintayhteys, jota ulkopuolinen hyökkääjä voi hyödyntää päästäkseen organisaation tietojärjestelmiin. Se muodostaako etähallintayhteys organisaatiolle riskin riippuu käytössä olevista tietoturvakontrolleista ja siitä, voiko yhteyden kautta vaarantaa organisaation liiketoiminnan näkökulmasta kriittisen toiminnan tai tiedon.
Käytäntö (Kybermittarissa)	Kybermittarin kontekstissa käytännöllä viitataan väittämiin, jotka on ryhmitelty Kyberturvallisuuden aihealueiden tavoitteiden alle. Kybermittarissa organisaatio arvioi käytäntöjen toteutumista omassa toiminnassaan neliportaisen asteikon avulla, ja tulosten perusteella määräytyy aihealue ja tavoitekohtainen kypsyys.
NIST (National Institute of Standards and Technology)	NIST on yhdysvaltalainen kauppaministeriön alainen virasto, jonka tehtävänä on kehittää ja edistää mittaustekniikoita, standardeja ja tekniikkaa. NIST tuottaa kyberturvaan ja yksityisyyden suojaan liittyviä standardeja ja parhaita käytäntöjä, joilla tuetaan organisaation kyberturvallisuuden kyvykkyyksiä.

Omaisuusrekisteri, *"Inventory of assets"*	Luettelo yrityksen suojattavista kohteista. Omaisuusluettelo sisältää tiedot esimerkiksi yrityksen suojattavista tieto-omaisuuksista, laitteista ja niiden konfiguraatioista kuten yrityksen työasemista ohjelma- ja datatietoineen, tietoverkoston rakenteen, IPR:stä, lisensseistä, henkilötiedoista, fyysisten tilojen valvontajärjestelmistä ja tilojen pohjapiirroksista
Osio (Kybermittarissa)	Kybermittarin kontekstissa kyberturvallisuuden osiolla tarkoitetaan yhtätoista kokonaisuutta, joiden suhteen kyberturvallisuuden kyvykkyyttä arvioidaan.
OT-Järjestelmä	Operatiivisella teknologialla (OT) tarkoitetaan yleisesti tieto- ja viestintäjärjestelmiä, joilla valvotaan ja hallitaan teollisia tai fyysisiä laitteita, prosesseja tai tapahtumia. Perinteisesti termillä OT on viitattu nimenomaan teollisiin ohjausjärjestelmiin, ja sillä on pyritty erottamaan toisistaan termit OT ja IT (informaatioteknologia), jolla puolestaan viitataan perinteisiin tieto-ja viestintäjärjestelmiin. Kybermittarin yhteydessä määritelmä OT kattaa perinteisten teollisten ohjauslaitteiden lisäksi myös muut näihin rinnastettavissa olevat laitteet, jotka ovat joko kytköksissä fyysiseen maailmaan tai täyttävät muutoin OT-laitteille tyypilliset kyberturvallisuuden haasteet. Näitä laitteita voivat olla esimerkiksi terveydenhuollon hoitolaitteet, finanssialan pääte- tai automaattilaitteet, rakennusteollisuuden tai logistiikan nostin-, kuljetus- ja muut automaatiolaitteet, tai kiinteistöautomaation lämmityksen, ilmastoinnin tai kulunhallinnan ohjauslaitteet. Kyberturvallisuuden kannalta OT-järjestelmiin ja -laitteisiin liittyy usein ominaisia haasteita. OT-järjestelmät ovat enenevässä määrin kytkettyinä verkkoon, mutta jäävät usein IT-kontrollien ulkopuolelle, niitä ei voida päivittää tai ne jäävät kokonaan tunnistamatta.
Resilienssi	Organisaation kriisinkestävyys tai kriisinsietoisuus eli kyky ylläpitää toimintakykyä muuttuvissa olosuhteissa sekä valmius kohdata häiriöitä ja kriisejä ja palautua niistä.
Suojattava kohde, *"Asset"*	Organisaation fyysinen tai tieto-omaisuus, jolla on arvoa liiketoiminnalle. Esimerkiksi asiakastiedot, tuotantojärjestelmien asetusarvot tai tuotantolaite
Tavoite (Kybermittarissa)	Kybermittarin kontekstissa tavoitteella tarkoitetaan aihealueeseen liittyvää kokonaisuutta, joiden suhteen aihealueen kyvykkyyttä arvioidaan.
Tilannekuva, *"Situational awareness"*	Organisaation tieto, siitä missä tilassa organisaation kypsyys kyberturvallisuudesta on. Hyvä tilannekuva koostuu kyvystä kerätä tietoa, ymmärtää ja analysoida sitä sekä reagoida uhkiin reaaliajassa. Osa tilannekuvan muodostamista on organisaation ymmärrys siitä, mitkä kyberturvallisuuden osa-alueet

	ovat hallinnassa ja missä on haasteita ja parannettavaa.
Vakioidut perusasetukset, *”Configuration baseline”*	Vakioidut perusasetukset on asetuksia, jotka on määritelty ja dokumentoitu niin että niihin prosessin voi turvallisesti palauttaa häiriön jälkeen
Yhteiskunnalle kriittinen palvelu	Palvelu on yhteiskunnalle kriittinen, mikäli sen häiriö vaikuttaa merkittävään asiakasmäärään, laajaan maantieteelliseen alueeseen tai sillä on vakavia seurannaisvaikutuksia.

7 Lähdeluettelo

[1] NIST Cybersecurity Framework Version 1.1, NIST, 04 2018 [Saatavilla osoitteesta: https://doi.org/10.6028/NIST.CSWP.04162018]

[2] Cybersecurity Capability Maturity Model (C2M2) version 1.1, U.S. Department of Energy, 02 2014 [Saatavilla osoitteesta: https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf]

[3] Cybersecurity Capability Maturity Model (C2M2) version 2.0 (draft), U.S. Department of Energy, 06 2019 [Saatavilla osoitteesta: https://www.energy.gov/sites/prod/files/2019/08/f65/C2M2 v2.0 06202019 DOE for Comment.pdf]

[4] Kansallinen riskiarvio 2018, Sisäministeriö, 01 2019 [Saatavilla osoitteesta: http://urn.fi/URN:ISBN:978-952-324-245-6]

[5] Yhteiskunnan turvallisuusstrategia 2017, Turvallisuuskomitea, 11 2017 [Saatavilla osoitteesta: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf]