Kansallisessa turvallisuusauditointikriteeristössä esitettyjen vaatimusten mallintaminen ArchiMate -kuvauskielellä

Hannu Tirkkonen

Haaga-Helia ammattikorkeakoulu

Tradenomi, tietojenkäsittely

Opinnäytetyö

2024

Tiivistelmä

Tekijä
Hannu Tirkkonen

Tutkinto
Tradenomi, tietojenkäsittely

Raportin/Opinnäytetyön nimi
Kansallisessa turvallisuusauditointikriteeristössä esitettyjen vaatimusten mallintaminen ArchiMate -kuvauskielellä

Sivu- ja liitesivumäärä
55 + 3

Tämän toiminnallisen opinnäytetyön tarkoituksena oli mallintaa Kansallinen turvallisuusauditointikriteeristö (Katakri) ArchiMate mallinnuskielellä ja tutkia voidaanko luodun mallin avulla arvioida tarkasteltavan kohteen tietoturvallisuuden tilaa esitettyjen turvallisuuskriteerien ja vaatimusten perusteella. Toiminnallisen osuuden tavoitteena oli julkaista Katakrista ensimmäinen, vapaasti saatavilla oleva viranomaisten julkaisemista kriteeristöistä luotu ArchiMate -malli ja vastata siten julkisesti saatavilla olevien turvallisuuskriteeristöjen mallinnusten tarpeeseen.

Opinnäytetyön tietoperustassa pääpaino on rakenteissa, jotka muodostavat toiminnallisen osuuden mallinnuksen rungon. Katakri kuvataan siten, että malli mahdollistaa kriteereissä esitettyjen vaatimusten tarkastelun riskien ja tietoturvallisuuden näkökulmasta. ArchiMate standardin ja sen riskien ja turvallisuuden hallinnan mukauttamismekanismien kuvaaminen muodostavat perusteet opinnäytetyössä syntyvälle varsinaiselle mallinnukselle.

Toiminnallinen osuus sisältää Katakrin mallinnuksen ja soveltamisesimerkkejä, joilla tarkasteltavaan kohteeseen voidaan kohdistaa vaatimuksia ja visuaalisen mallin avulla konkreettisesti pienentää riskejä.

Opinnäytetyön perusteella voidaan todeta, että ArchiMate-standardi tarjoaa mallinnusrakenteet tehokkaaseen riski- ja turvallisuuskäsitteiden kuvaamiseen ja yhdistämiseen. ArchiMate-kieli tarjoaa mallintajille välineet määritellä elementeille myös lisätietoja, joita voidaan käyttää arkkitehtuurien analysointiin ja riskien ja turvallisuusongelmien vaikutuksen määrittämiseen.

Opinnäytetyön keskeinen tulos julkisesti saatavilla olevana mallina tarjoaa runsaasti jatkojalostamismahdollisuuksia, kuten viranomaisten julkaisemien muiden kriteeristöjen mallinnukset. ArchiMate-kieli tarjoaa lisäksi edistyneitä soveltamismahdollisuuksia, kuten tekoälyn ja automaation hyödyntämisen kokonaisarkkitehtuurissa.

Toiminnallisen työn mallinnuksesta muodostui lopulta niin laaja, että se julkaistiin lisäksi kokonaisuudessaan GitHub -verkkopalveluun, josta se on vapaasti ladattavissa. Arkkitehdit ja tietoturva-asiantuntijat voivat mallin avulla suunnitella uusia, kansallista tai kansainvälistä turvaluokiteltua tietoa suojaavia ratkaisuja hyödyntäen olemassa olevaa, uudelleenkäytettävää turvallisuuskriteerin mallinnusta.

Asiasanat
Kansallinen turvallisuusauditointikriteeristö, tietoturva, kokonaisarkkitehtuuri, vaatimustenhallinta, mallintaminen, ArchiMate

Abstract

Author(s)
Hannu Tirkkonen

Degree programme
Bachelor of Business Administration, Business Information Technology

Report/Thesis Title
Modelling the requirements presented in the national security audit criteria by using the ArchiMate modelling language.

Number of pages and appendix pages
55 + 3

The purpose of this product-based thesis was to model the National Security Audit Criteria (Katakri) using the ArchiMate modelling language and to study whether the created model can be used to assess the information security status of the target organisation based on the presented security criteria and requirements. The objective of the actual outcome was to publish the first freely available ArchiMate model based on the national security audit criteria and thus fulfils the need for publicly available security criteria modelling.

The focus of the theoretical framework of the thesis is on the structures that form the model as the actual outcome. Katakri is described in such way that the model enables risk and security assessment based on the requirements presented in the criteria. The description of the ArchiMate standard and its adaptation mechanisms for risk and security management form the basis for the actual modelling created in the thesis.

The empirical part contains Katakri's modelling and application examples, which can be used to apply requirements to the target under inspection and to concretely reduce risks with the help of a visual model.

Based on the thesis, it can be concluded that The ArchiMate standard provides the modelling constructs to efficiently describe and interconnect the risk and security concepts. The ArchiMate language provides modelers with the tools to define additional information for elements, which can be used to further analyse architectures and determine the impact of risks and security issues.

The key outcome of the thesis as a publicly available model offers plenty of further processing possibilities, such as the modelling of other criteria sets published by the authorities. The ArchiMate language also offers advanced application possibilities, such as the utilization of artificial intelligence or automation in the enterprise architecture.

The actual model eventually became so extensive that it was also published in its entirety to GitHub, where it can be freely downloaded. Architects and information security specialists can use the model to design new solutions protecting national or international classified Information, making use of existing, reusable security audit criteria model.

Keywords
National security audit criteria, information security, enterprise architecture, requirements management, modelling, ArchiMate

Sisällys

1 Johdanto

Kansallinen turvallisuusauditointikriteeristö (Katakri) on tietoturvavaatimuksiin perustuva viranomaisten tietoturvallisuuden auditointityökalu, jota voidaan käyttää arvioitaessa organisaatioiden kykyä suojata turvallisuusluokiteltua tietoa. Kriteeristönä Katakriin on koottu voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin perustuvia vaatimuksia. Vaatimusten lisäksi Katakri pitää sisällään myös toteutusesimerkkejä, miten useimmissa ympäristöissä voidaan saavuttaa hyväksyttävä suojausten vähimmäistaso. Yhtenä keskeisenä Kansallisen tietoturvakriteeristön lähteenä on ollut laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906. (Kansallinen turvallisuusviranomainen 2020, 4–5.)

Tiedonhallintalaissa todetaan, että organisaatioiden tiedonhallintayksikössä on ylläpidettävä sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia. Valtiovarainministeriö on julkaissut suosituksen tiedonhallintamallista liitteineen, joissa todetaan tiedonhallintamallin sisältävän kokonaisarkkitehtuurikuvauksiin sisältyviä toiminta-, tieto- ja tietojärjestelmäkuvauksia ja joissa suositellaan kokonaisarkkitehtuurikuvausten hyödyntämistä osana tiedonhallintamallia. (Valtionvarainministeriö 2020, 14)

Digi- ja väestötietovirasto (DVV) vastaa julkisen hallinnon kokonaisarkkitehtuurimenetelmän kehittämisestä. Julkishallinnon organisaatioiden kokonaisarkkitehtuurityön tukemiseksi Digi- ja väestötietovirasto julkaisee muun muassa yhteisiä ohjeita ja menetelmäkuvauksia. DVV ohjeistaa käyttämään kokonaisarkkitehtuurityössä JHS179 -kokonaisarkkitehtuurimenetelmää ja ArchiMate kuvauskieltä. JHS179 perustuu kansainväliseen, avoimeen ja yleisimmin käytössä olevaan kokonaisarkkitehtuurin TOGAF viitekehykseen. (Digi- ja väestötietovirasto s.a.)

Vaatimustenhallinta, ja siten Katakrissa esitettyjen vaatimusten hallinta on olennainen osa turvallisuusluokiteltua tietoa käsittelevien organisaatioiden kokonaisarkkitehtuurityötä. ArchiMate on yksi yleisimmistä kokonaisarkkitehtuurin kuvauskielistä, jota käytetään myös Digi ja väestöviraston kokonaisarkkitehtuurikuvausten esimerkkien mallinnuksissa ja valittu käytettäväksi myös tässä opinnäytetyössä.

1.1 Opinnäytetyön tavoitteet ja rajaukset

Opinnäytetyön tavoitteena on mallintaa Kansallinen turvallisuusauditointikriteeristö (Katakri) käyttämällä Archimate -kuvauskieleltä. Opinnäytetyössä termi malli eroaa tiedonhallintalaissa kuvatusta tiedonhallintamallista, joka on kuvaus organisaation toimintamallista. Tämän opinnäytetyön tuloksena syntyvä malli on Katakrin kriteereistä ja vaatimuksista ArchiMate -kuvauskielellä luotu visuaalinen malli.

Opinnäytetyön mallinnuksen tarkoituksena on tutkia, tarjoaako ArchiMate-standardi menetelmät tehokkaaseen riski- ja turvallisuuskäsitteiden kuvaamiseen ja lisätietojen yhdistämiseen ja soveltuuko Archimate -kuvauskieli siten mallintamaan Katakrissa esitetyt kriteerit ja niihin liitetyt vaatimukset.

Opinnäytetyössä kuvataan ensin Katakri, sen osa-alueet ja rakenne yleisesti. Opinnäytetyössä kuvataan Katakria vain yleisellä tasolla, eikä itse kriteerejä tai niissä esitettyjen vaatimusten taustoja pyritä analysoimaan tai tutkimaan tarkemmalla tasolla. Seuraavaksi kuvataan kokonaisarkkitehtuurin mallinnuskieli ArchiMate ja miten sitä voi hyödyntää mallintamaan organisaatioiden riskien ja turvallisuuden hallintaa ja kriteeristöjä, kuten Katakri.

Opinnäytetyön empiirisessä osuudessa kuvataan, miten ArchiMatella voidaan mallintaa Katakrissa esitetyt kriteerit ja niiden vaatimukset. Toiminnallisessa osuudessa Katakrista luodaan malli, joka pitää sisällään mahdollisimman paljon kriteeristöjen sisällöstä, jotta mallia itsessään voi käyttää tiedon lähteenä mallinnettaessa palveluita, joiden halutaan täyttävän Katakrissa esitetyt kriteerit ja niiden vaatimukset. Syntyvän mallin perusteella pohditaan ArchiMaten mallinnuskielen hyödyllisyyttä ja toimivuutta tarkasteltaessa järjestelmien tietoturvallisuutta kriteeristöissä esitettyjen vaatimusten pohjalta.

1.2 Käytetyt menetelmät

Toiminnallisen opinnäytetyön menetelmiksi muodostui soveltava kirjallisuuskatsaus, kriteeristöjen vertailu ja toiminnallisen osuuden mallintaminen. Kirjallisuuskatsauksessa pyrittiin tutkimaan riskien ja turvallisuudenhallinnan mallinnuksiin liittyviä tieteellisiä artikkeleita, kirjoja ja muita julkaisuja. Toiminnallisen työn mallinnuksen tueksi vertailtiin muita kriteeristöjä ja standardeja, kuten Julkisen hallinnon tietoturvallisuuden arviointikriteeristöä (Julkri), Pilvipalveluiden turvallisuuden arviointikriteeristöä (PiTuKri) ja ISO/IEC standardeja 27001, 27002 ja 42010. Kirjallisuuskatsaus ja vertailu auttoi tunnistamaan mallinnuksiin liittyviä parhaita käytäntöjä, kuten soveltuvat mallinnuselementit ja dokumentoinnin sisällyttämisen osaksi mallinnuksia. Toiminnallisessa osuudessa syntyneen Katakrin mallinnuksen avulla voitiin hahmottaa kriteeristön keskeiset osa-alueet ja niihin liittyvät vaatimukset ja suhteet. Mallinnuksen avulla voidaan kriteeristöjen vaatimukset täyttäviä ratkaisuja kuvata paremmin käytännössä. Näitä erilaisia menetelmiä yhdistämällä saatiin kattava näkemys riskien ja turvallisuudenhallinnan mallintamisesta ja vaatimusten soveltamisesta organisaatioiden näkökulmasta.

1.3 Keskeiset käsitteet

Archi	Avoimen lähdekoodin ArchiMate -mallinnustyökalu (Beauvoir & Sarrodie 2023).
ArchiMate	Kokonaisarkkitehtuurin mallinnuskieli, joka on kehitetty Open Group -organisaation toimesta (Open Group 2023).
Arkkitehtuurivaatimusten julkaisuarkisto	Arkkitehtuurivaatimusten tallentamiseen ja julkaisemiseen soveltuva tekninen järjestelmä ja sen ympärille rakennetut palvelut, esim. kuvauskanta.
Attribuutti	Tietokentässä määritetty ominaisuus, esim. lukuarvo tai teksti.
coArchi	Archi -mallinnustyökalun laajennos, jonka avulla mallinnuksissa voidaan hyödyntää Git versiohallintajärjestelmiin perustuvia kuvauskantoja (repository).
DVV	Digi- ja väestötietovirasto.
Git	Hajautettu versionhallintajärjestelmä.
GitHub	Verkkopalvelu, joka tarjoaa sijoituspaikan Git-versionhallintaa käyttäville projekteille.
Julkri	Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Valtiovarainministeriö 2023).
JHS 179	Julkishallinnon suositus kokonaisarkkitehtuurin kehittämiseksi (Juhta 2017).
JUHTA	Julkisen hallinnon tietohallinnon neuvottelukunta.
Katakri	Kansallinen turvallisuusauditointikriteeristö.
Kokonaisarkkitehtuuri	Toiminnan, prosessien ja palvelujen, tietojen, tietojärjestelmien ja niiden tuottamien palvelujen muodostaman kokonaisuuden rakenteen kuvaus (Juhta 2017).
Kuvauskanta	Tietovaranto (repository), johon luodaan, ylläpidetään ja hallitaan arkkitehtuurimalleja.

NSA	Kansallinen turvallisuusviranomainen.
PiTuKri	Pilvipalveluiden turvallisuuden arviointikriteeristö.
Ratkaisunäkymä	Ratkaisunäkymä sisältää arkkitehtuurinäkymää tukevat ratkaisujen rakennuskomponentit (ratkaisut), jotka yritys on suunnitellut tai ottanut käyttöön.
Repository	Kuvauskanta.
Tiedonhallintalaki	Laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906.
TOGAF	The Open Group Architecture Framework, kokonaisarkkitehtuurin viitekehys (Open Group 2022a).
Validaattori	Toiminto, joka tarkastaa dokumentin oikeellisuuden dokumenttityypin määritysten mukaisesti.
Viitekehys	Malli, jonka mukaan organisaation tai muun kehittämiskohteen rakenteita jäsennetään, hallitaan ja kehitetään (Juhta 2017).

2 Katakri

Kansallinen turvallisuusauditointikriteeristö, eli Katakri on tietoturvallisuuden auditointityökalu, jota voidaan käyttää arvioitaessa tarkasteltavan organisaation kykyä suojata kansallista tai kansainvälistä, kuten EU:n ja soveltuvin osin myös Naton turvallisuusluokiteltua tietoa. Katakriin on koottu turvallisuusluokiteltujen tietojen hallinnan vähimmäisvaatimukset perustuen kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin. Katakriin itseensä ei ole lisätty uusia vaatimuksia, vaan siihen on koottu keskitetysti vaatimukset, jotka perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Katakrin ylläpidosta ja hallinnoinnista on vastannut vuodesta 2014 lähtien ulkoministeriössä toimiva Kansallinen turvallisuusviranomainen (NSA). Ensimmäinen Katakri valmistui vuonna 2009 ja viimeisin, Katakri 2020 vuonna 2020. Katakri 2020:ssa on tarkennettu ja täydennetty kysymyksiä muun muassa tietosuojan, riskienhallinnan, tietoturvaviestinnän ja käyttäjätunnistamisen osalta. Rakenteellisesti Katakri jakautuu kolmeen osa-alueeseen, jotka ovat turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen tietoturvallisuus. Katakri on ladattavissa ulkoministeriön verkkosivuilta. (Kansallinen turvallisuusviranomainen 2020, 5.)

Katakriin on luotu myös erillinen arviointityökalu, johon on koottu Katakrin vaatimukset. Työkalu on tarkoitettu turvallisuusluokitellun tietojen suojausten arviointiin ja suunnattu erityisesti apuvälineeksi, jota voi hyödyntää itsearvioinneissa ja tarkastuksissa. Arviointityökalu on julkaistu Microsoft Excel taulukkolaskentaohjelman tiedostomuodossa ja se on ladattavissa Kyberturvallisuuskeskuksen sivustolta. (Kyberturvallisuuskeskus 2021.)

2.1 Osa-alue T: Turvallisuusjohtaminen

Katakrin turvallisuusjohtaminen keskittyy organisaation johtamiseen ja menetelmiin, joilla turvallisuus ja turvallisuuden hallinta jalkautetaan osaksi organisaation toimintaa. Osa-alueen vaatimusten tavoitteena on varmistaa, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä, riittävät menetelmät ja prosessit turvallisuusluokiteltujen tietojen käsittelemiseksi ja että näitä tietoja käsittelevä henkilöstö toimii vaatimusten mukaisesti. Turvallisuusjohtamisen osa-alue jakaantuu hallinnolliseen tietoturvallisuuteen ja henkilöstöturvallisuuteen. (Kansallinen turvallisuusviranomainen 2020, 8.)

Hallinnollisen tietoturvallisuuden kriteerit käsittävät vaatimukset organisaation johdolle, turvallisuusperiaatteille ja vastuille. Osio kattaa myös ohjeistukset, poikkeustilanteet ja tietojen luokittelun. Henkilöstöturvallisuuden vaatimukset pitää sisällään vaatimuksia mm. henkilöstöön, salassapitoon ja käsittelyoikeuksiin liittyen. (Kansallinen turvallisuusviranomainen 2020, 8.)

2.2 Osa-alue F: Fyysinen turvallisuus

Fyysisen turvallisuuden osa-alueella kuvataan vaatimukset fyysisten ja teknisten turvatoimien toteuttamiseksi siten, että organisaatio kykenee estämään luvattoman pääsyn turvallisuusluokiteltuihin tietoihin. Fyysisen turvallisuuden osa-alue jakaantuu yleisiin, turvallisuusalueiden ja tietoaineistoturvallisuuden vaatimuksiin. Fyysisen turvallisuuden yleisissä vaatimuksissa kuvataan turvatoimien tavoitteet, riskien arviointi, toisiaan täydentävien turvatoimien valinta sekä tiedon käsittelyn ja säilytyksen vaatimukset. Fyysisen turvallisuuden turvallisuusalueet on jaettu Katakrissa kolmeen eri alueeseen, jotka ovat hallinnollinen alue, turva-alue ja teknisesti suojattu turva-alue. Vähimmäisvaatimukset on kuvattu jokaisen turvallisuusalueen alaluvuissa. Turva-alueiden vähimmäisvaatimukset ovat osin päällekkäisiä ja ne on kuvattu jokaisen turvallisuusalueen alaluvuissa. Tietoaineistoturvallisuuden vaatimukset kuvaavat paperimuodossa olevien turvallisuusluokiteltujen tietojen käsittelyn vaatimukset niiden elinkaaren aikana. (Kansallinen turvallisuusviranomainen 2020, 22–23.)

2.3 Osa-alue I: Tekninen tietoturvallisuus

Katakrin teknisen tietoturvallisuuden osa-alueella kuvataan vähimmäisvaatimukset turvallisuusluokitellun tiedon käsittelyyn tietojenkäsittely-ympäristöissä. Osa-alue on jaettu tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden alaosioihin. Osa-alueen nimen mukaisesti Teknisen tietoturvallisuuden kriteerit keskittyvät ns. teknisiin aiheisiin, kuten ohjelmistoihin, laitteistoihin ja niiden välisiin yhteyksiin ja hallintatoimiin. Alue pitää sisällään verkkojen rakenteellisen turvallisuuden ja verkkojen vyöhykkeistämisen ja järjestelmien hallinnoinnin. (Kansallinen turvallisuusviranomainen 2020, 63–64.)

Tietoliikenneturvallisuuden kriteerit käsittävät mm. verkon rakenteellisen turvallisuuden, verkkojen vyöhykkeistämisen, suodatussäännöstöt, hallinnoinnin ja hallintayhteydet (Kansallinen turvallisuusviranomainen 2020, 65–74). Tietojärjestelmäturvallisuuden kriteereihin sisältyy mm. pääsyoikeuksien hallinnointi, toimijoiden tunnistaminen, järjestelmäkovennukset, haittaohjelmasuojaus, tapahtumien jäljitettävyys ja poikkeamista toipuminen (Kansallinen turvallisuusviranomainen 2020, 75–93). Käyttöturvallisuus pitää sisällään vaatimuksia mm. tiedon sähköisen välityksestä, muutoshallintamenettelyistä, tietojen käsittelystä, etähallinnasta ja varmuuskopioinnista (Kansallinen turvallisuusviranomainen 2020, 94–106).

Katakri pitää sisällään vaatimuksista myös toteutusesimerkkejä, miten useimmissa ympäristöissä voidaan saavuttaa hyväksyttävä suojausten vähimmäistaso. Katakrissa esitetyt toteutusesimerkit eivät ole sitovia, eikä niissä kuvata kaikkiin ympäristöihin tai tapauksiin riittäviä suojauksia. (Kansallinen turvallisuusviranomainen 2020, 5.)

2.4 Katakrissa esitettyjen kriteerien rakenne

Katakrissa esitetyt kriteerit noudattavat samaa ylätason rakennetta, joka pitää sisällään kriteerin nimen, lähteet, vaatimukset ja lisätietoja osuuden. Lisätiedoissa kuvataan mahdolliset toteutusesimerkit ja muita huomioitavia seikkoja.

Kriteereissä esitetään ensiksi kriteerin nimi, esimerkiksi ”T-01 – JOHDON TUKI, OHJAUS JA VASTUU – TURVALLISUUSPERIAATTEET”. Nimen edessä on kriteerin lyhenne, kuten T-01, jossa ensimmäinen kirjain esittää Katakrin osa-aluetta ja numerosarja kriteerin järjestysnumeroa (T=Turvallisuusjohtamisen osa-alue, 01=osa-alueen järjestyksessä ensimmäinen kriteeri). Nimen loppuosa on kuvaava nimi kriteerille. Kriteerin vaatimusosuus voi pitää sisällään useamman vaatimuksen, joiden sisältö vaihtelee yhdestä virkkeestä monitasoisiin ja yksityiskohtaisiin kuvauksiin. Lähteissä esitetään kriteeriin perusteena oleva lainsäädäntö, jossa viitataan lakien ja asetusten momentteihin, jotka ovat kriteerin pohjana. Lisätietoja pitää sisällään tarkemman kuvauksen kriteeristä, mahdollisen toteutusesimerkin ja viittauksen muihin tietoturvalähteisiin. Esimerkki kriteerin rakenteesta on esitetty kuvassa 1. (Kansallinen turvallisuusviranomainen 2020, 69.)

T-02 – TURVALLISUUSTYÖN TEHTÄVIEN JA VASTUIDEN MÄÄRITTÄMINEN

Vaatimus	§ Lähde (906/2019 ja/tai 1101/2019)	§ Lähde (2013/488/EU)
Organisaatio on määritellyt tietoturvallisuuden hoitamisen tehtävät ja vastuut.	906/2019 4 § 1 ja 2 mom	7 artiklan 5 kohta

Lisätietoja

Yleistä: Turvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan, että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa. Tietoturvallisuuteen liittyvät tehtävät ja vastuut tulee kirjata organisaation ja työntekijöiden työjärjestyksiin ja tehtävänkuvauksiin sekä toimintaohjeisiin. Organisaationjohdon tehtävänä on määritellä turvallisuusluokitellun tiedon tiedonhallintaan liittyvät vastuut. Kysymys ei ole tiedonhallintavastuiden delegoinnista, vaan niiden määrittelystä. Vastuut tulisi määritellä erityisesti tietoturvallisuusohjeiden ylläpidosta, riskienhallinnasta, varautumisesta sekä tietoturvallisuuden kokonaisvastuussa olevista henkilöistä.

Toteutusesimerkki: Organisaatio on määritellyt turvallisuuden toteuttamisen tehtävät ja vastuut ainakin seuraavilta osin:
a) turvallisuusjohtaminen
b) fyysinen turvallisuus
c) tekninen tietoturvallisuus

Vastuumäärittely sisältää turvallisuusluokitellun tiedon käyttöympäristön omistajan sekä tietoturvallisuuteen liittyvät vastuut. Tietoturvallisuusdokumentaation kattavuuden ja ajantasaisuuden säännöllinen seuranta on vastuutettu. Tietoturvallisuusdokumentaatio kattaa turvallisuusluokiteltuun tietoon liittyvät prosessit ja käsittely-ympäristöt koko tiedon elinkaaren ajalta, ja se on tarvittavien tahojen saatavilla.

Yritysturvallisuusselvityksissä huomioitavaa: Selvityksen kohteella tulee olla turvallisuusvastaava (Facility Security Officer, FSO). Turvallisuusvastaava on henkilö, jolla on riittävä turvallisuusosaaminen ja jonka yrityksen johto on nimittänyt vastaamaan yrityksen turvallisuusasioista turvallisuusluokiteltujen tietojen suojaamiseen liittyvissä kysymyksistä. Turvallisuusvastaava tekee yhteistyötä toimivaltaisten turvallisuusviranomaisten kanssa. Turvallisuusvastaava huolehtii, että selvityksen kohde toteuttaa edellytetyt tietoturvallisuustoimenpiteet.

Muita lisätietoja: SFS-EN ISO/IEC 27002:2017 5.1.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01; Tiedonhallintalautakunnan suositus 2020:18

Kuva 1. Esimerkki Katakrin kriteeristä (Kansallinen turvallisuusviranomainen 2020, 10)

3 ArchiMate

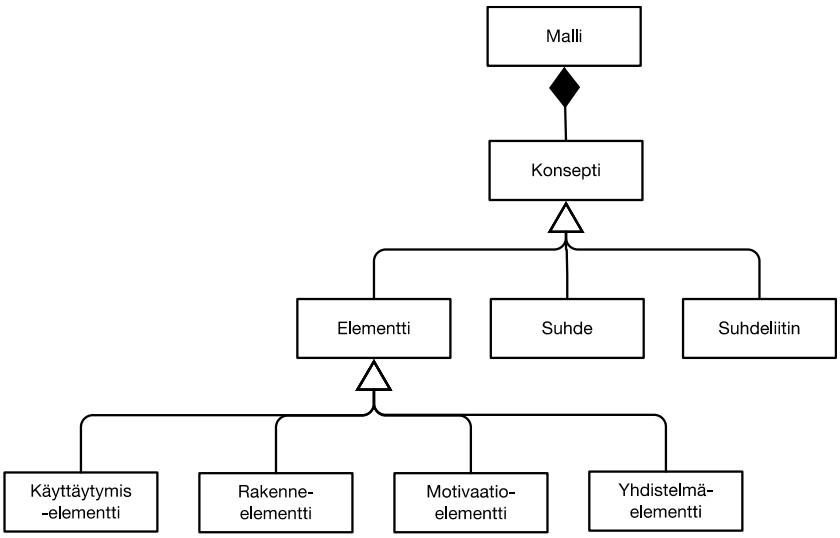
ArchiMate on kokonaisarkkitehtuurin mallinnuskieli, joka on kehitetty Open Group -organisaation toimesta. Kokonaisarkkitehtuurilla tarkoitetaan Open Groupin luomassa ja ylläpitämässä The Open Group Architecture Framework (TOGAF) standardissa esitettyyn viitekehykseen, jossa kuvataan kokonaisarkkitehtuuri oikean tasapainon mahdollistajana liiketoiminnan muutoksen ja jatkuvan toiminnan tehokkuuden välillä. Kokonaisarkkitehtuurilla voidaan kuvata sidosryhmien vaatimusten tunnistamista ja jalostamista, jolloin pystytään osoittamaan, kuinka huolenaiheet ja vaatimukset kyetään käsittelemään. Kokonaisarkkitehtuurin avulla pystytään näyttämään toimenpiteet, joita aiotaan tehdä sovitettaessa yhteen eri sidosryhmien mahdollisesti ristiriitaiset huolenaiheet. (Open Group 2022a, kappale 1.)

ArchiMate -mallinnuskieli on vapaasti saatavilla standardina Open Groupin verkkosivustolla. Mallinnuskielenä ArchiMate on visuaalinen kieli, jossa on graafisia elementtejä, joiden avulla voidaan kuvata, analysoida ja välittää monia kokonaisarkkitehtuuriin liittyviä asioita. ArchiMate -mallinnuskieli tarjoaa standardin tavan kuvata organisaatioiden eri toimintoja, prosesseja, järjestelmiä ja tietovarastoja sekä niiden välisiä riippuvuuksia ja suhteita. Sen avulla voidaan kuvata laajoja ja monimutkaisia järjestelmiä yksinkertaisella ja selkeällä tavalla. (Open Group 2023, kappale 1.)

ArchiMate mallinnuskieltä käytetään sekä yksityisellä, että julkisella sektorilla osana kokonaisarkkitehtuuria. Suomessa Julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA) on suositellut käyttämään ArchiMate-notaatiota Arkkitehtuurinäkökulmien kuvaamisessa suosituksessaan (Juhta 2017).

3.1 Kielirakenne

ArchiMaten kielimalli perustuu hierarkkiseen rakenteeseen. Malli on kokoelma käsitteitä, jotka ovat joko elementtejä tai suhteita. Elementti on joko käyttäytymis-, rakenne-, motivaatio- tai yhdistelmäelementti. Archimaten ylätason puumainen rakenne on esitetty kuvassa 2. (Open Group 2023, kappale 3.)



Kuva 2 ArchiMaten ylätason hierarkia (mukaillen Open Group 2023, kappale 3.2)

3.2 ArchiMate -kielen kerrostaminen

ArchiMaten ydinkieli määrittelee geneeristen elementtien rakenteen ja niiden suhteet, jotka voidaan erikoistaa eri kerroksiin. ArchiMate-ydinkielessä on määritelty kolme kerrosta seuraavasti:

1. Liiketoimintakerros (Business Layer) kuvaa asiakkaille tarjottavia liiketoimintapalveluita, jotka toteutuvat organisaatiossa liiketoiminnan toimijoiden suorittamilla liiketoimintaprosesseilla.
2. Sovelluskerros (Application Layer) kuvaa liiketoimintaa tukevat sovelluspalvelut ja niitä toteuttavat sovellukset.
3. Teknologiakerros (Technology Layer) käsittää sekä informaatio- että operatiivisen teknologian. Teknologiakerroksessa voidaan mallintaa esimerkiksi prosessointi- tallennus- ja tietoliikenneteknologian sovellus- ja liiketoimintakerroksen tueksi. Teknologiakerroksessa voidaan mallintaa lisäksi toiminnallista tai fyysistä teknologiaa, kuten toimitiloja, fyysisiä laitteita, materiaaleja ja jakeluverkkoja.

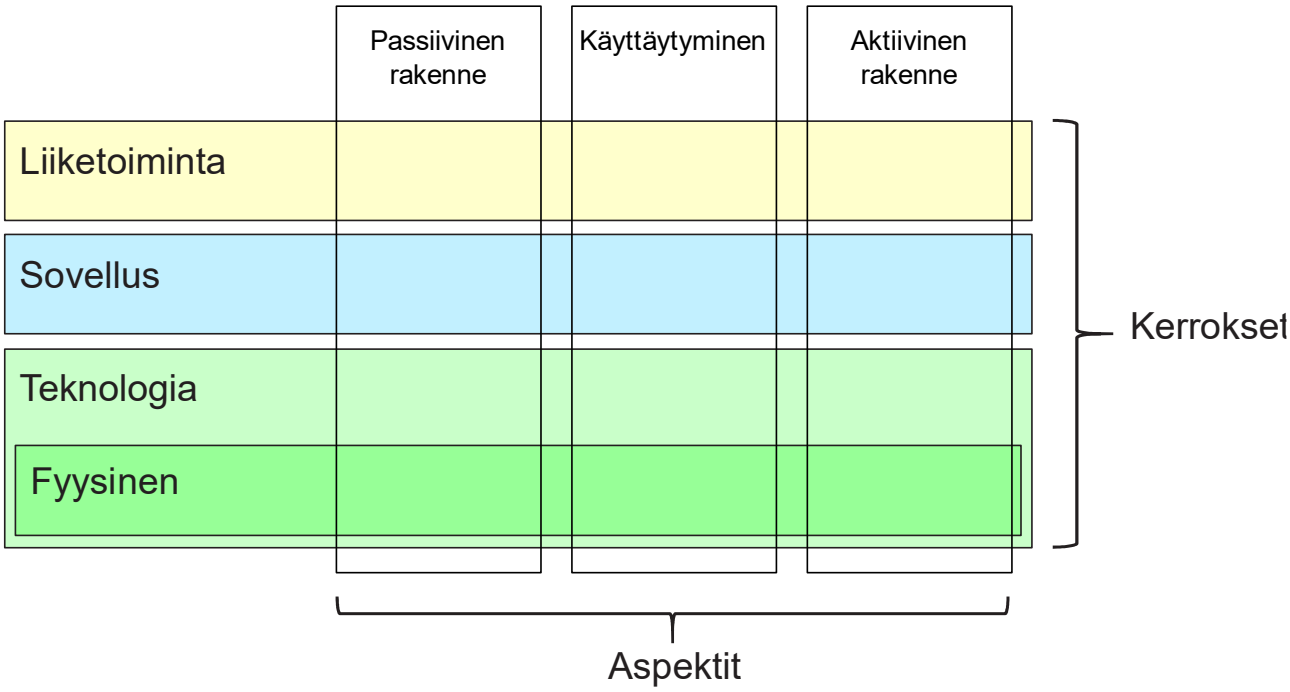
Mallien yleinen rakenne eri kerroksissa on samanlainen ja samantyyppisiä elementtejä ja suhteita käytetään, vaikka niiden luonne ja tarkkuus vaihtelevat. (Open Group 2023, kappale 3.)

3.3 ArchiMaten ydinkehys

ArchiMaten ydinkehys (ArchiMate Core Framework) koostuu yhdeksän solun kehyksestä, jota käytetään ArchiMate ydinkielen elementtien luokittelemiseen. Se koostuu kolmesta kerroksesta (Layers) ja aspektista (Aspects).

Elementtien luokittelussa aspekteihin ja kerroksiin on tärkeää ymmärtää, että elementtejä ei tarvitse tiukasti rajata yhteen aspektiin tai kerrokseen. Eri aspekteja ja kerroksia yhdistävillä elementeillä on keskeinen rooli yhtenäisessä arkkitehtuurikuvauksessa ja asiayhteydestä voi riippua,

katsotaanko tietty tarkastelun kohde, kuten ohjelmisto osaksi sovelluskerrosta (Application) tai teknologiakerrosta (Technology). (Open Group 2023, kappale 3.)



Kuva 3. ArchiMaten ydinkehys (mukaillen Open Group 2023)

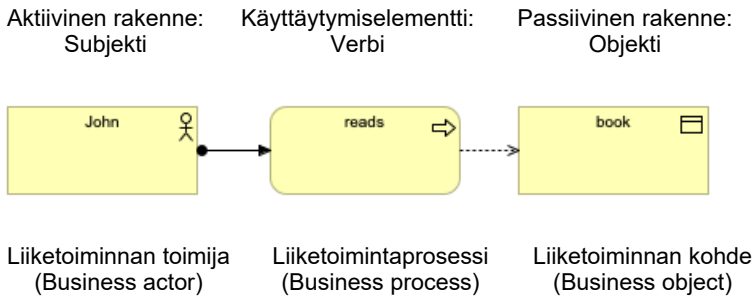
ArchiMate kehyksen rakenne mahdollistaa organisaation mallintamisen eri näkökulmista, jolloin asema soluissa korostaa sidosryhmien huolenaiheita, jotka voivat tyypillisesti kattaa useita soluja. Kehyksen kaksi ulottuvuutta, kerrokset ja aspektit, on esitetty kuvassa 3. (Open Group 2023, kappale 3.4.)

Kehyksellä on kolme kerrosta, joilla kohdetta, kuten organisaatiota voidaan mallintaa. Kerrokset ovat liiketoiminta (Business), sovellus (Application) ja teknologia (Technology)

ArchiMaten aspektit ovat passiivinen rakenne, käyttäytyminen ja aktiivinen rakenne. Passiivinen rakenne edustaa objekteja, joille käyttäytyminen suoritetaan. Nämä ovat yleensä tieto- ja dataobjekteja liiketoiminta ja sovelluskerroksissa, mutta niitä voidaan käyttää myös fyysisten kohteiden esittämiseen. Aktiivinen rakenne edustaa rakenteellisia elementtejä (liiketoiminnan toimijat, sovelluskomponentit ja laitteet, jotka näyttävät todellista käyttäytymistä, eli toiminnan kohteita. Käyttäytyminen edustaa toimijoiden käyttäytymistä tai toimintaa, kuten prosesseja, toimintoja, tapahtumia ja palveluita. Rakenteelliset elementit on liitetty käyttäytymiselementteihin, jotka osoittavat, kuka tai mikä näyttää käyttäytymisen. (Open Group 2023, kappale 3.4.)

ArchiMate kielen aspektit ovat saaneet vaikutteita luonnollisten kielten rakenteesta. Kaikissa kielissä lauseella on subjekti (aktiivinen rakenne) predikaatti (käyttäytyminen tai toiminta) ja objekti

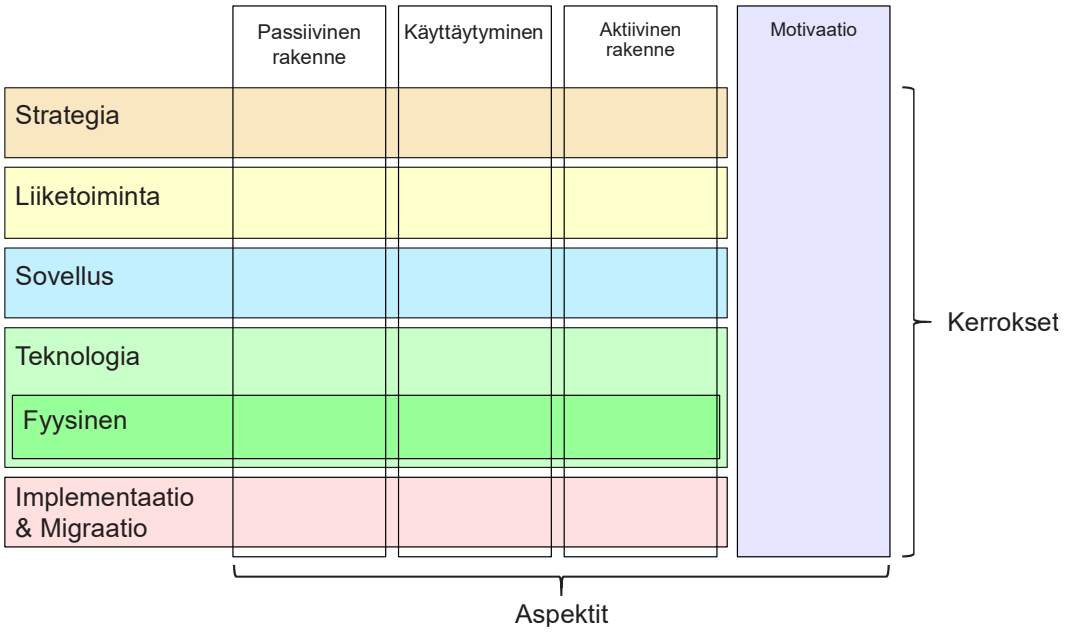
(passiivinen rakenne). ArchiMaten kielen määrityksessä tämä kielirakenne vastaa kuvattua kolmea aspektia, Aktiivinen rakenne(subjekti), Käyttäytyminen (predikaatti) ja Passiivinen rakenne (objekti) jotka on esitetty kuvassa 4. (Open Group 2022b, 13.)



Kuva 4. ArchiMate mallinnuskielen lauserakenne (mukaillen Open Group 2022b, 13)

3.4 ArchiMaten täysi kehys (ArchiMate Full Framework)

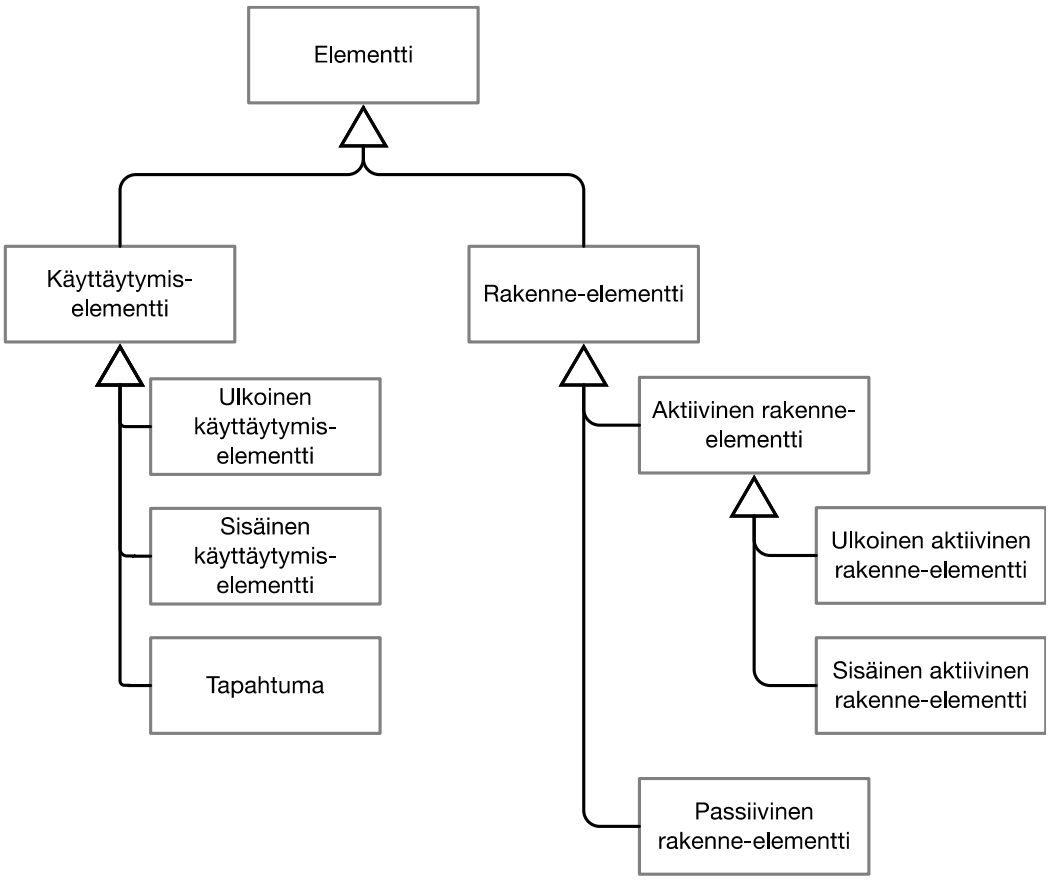
ArchiMaten täysi kehys lisää useita kerroksia ja aspektin (näkökohdan) ydinkehykseen. Kehykseen on lisätty Strategiakerros (Strategy), Implementaatio ja migraatiokerros (Implementation & migration) sekä Motivaatioaspekti. Strategiaelementeillä mallinnetaan strategista suuntaa ja valintoja. Motivaatioelementtejä käytetään mallintamaan motiiveja tai syitä, jotka ohjaavat kokonaisarkkitehtuurin suunnittelua tai muutosta. Implementaatio- ja migraatioelementit tukevat arkkitehtuurien käyttöönottoa ja migraatiota. (Open Group 2023, kappale 3.5.)



Kuva 5. ArchiMaten täysi kehys (mukaillen Open Group 2023, kappale 3.5.)

3.5 Metamalli

ArchiMate-kielen metamalli määrittelee elementit yleisellä, kerroksesta riippumattomalla tavalla. Malli koostuu kahdesta päätyypin elementistä: rakenteesta (structure) ja käyttäytymiselementeistä (behavior). Rakenne-elementit voidaan jakaa aktiivisiin ja passiivisiin elementteihin. Käyttäytymiselementit voidaan jakaa sisäisiin käyttäytymiselementteihin ja ulkoisiin käyttäytymiselementteihin, joita kutsutaan myös palveluiksi sekä tapahtumiin. ArchiMaten käyttäytymis- ja rakenne-elementtien hierarkia esitetään kuvassa 6. (Open Group 2023, kappale 4.)



Kuva 6. ArchiMaten käyttäytymis- ja rakenne-elementtien hierarkia (mukaillen Open Group 2023, kappale 4.1.)

3.6 Aktiiviset rakenne-elementit

Aktiiviset rakenne-elementit ovat kohteita, jotka voivat suorittaa käyttäytymistä. Elementit voidaan jakaa sisäisiin aktiivisiin rakenne-elementteihin ja ulkoisiin aktiivisiin rakenne-elementteihin. Sisäisinä rakenne-elementteinä voi esittää esimerkiksi liiketoiminnan toimijoita, sovelluskomponentteja ja noodeja. Ulkoiset aktiiviset rakenne-elementit esitetään rajapintoina. Aktiiviset rakenne-elementit esitetään suorakulmaisilla laatikoilla tai kuvakkeella yksinään. Aktiivisen rakenne-elementin merkintätapa esitetty taulukossa 1. (Open Group 2023, kappale 4.1.1.)

3.7 Käyttäytymiselementit

Käyttäytymiselementit edustavat organisaation dynaamisia puolia. Käyttäytymiselementit voidaan jakaa sisäisiin ja ulkoisiin käyttäytymiselementteihin. Ulkoiset käyttäytymiselementit esitetään palveluina. Käyttäytymiselementit merkitään pyöreäkulmaisilla laatikoilla tai kuvakkeella yksinään. Käyttäytymiselementin merkintätapa esitetty taulukossa 1. (Open Group 2023, kappale 4.1.2.)

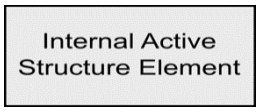
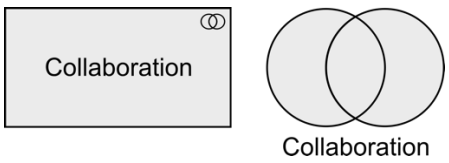
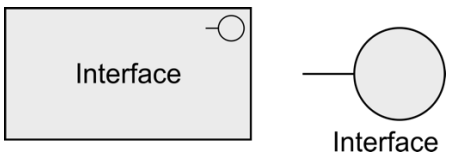
3.8 Passiiviset rakenne-elementit

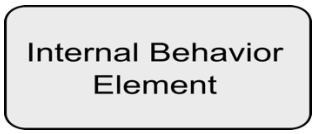
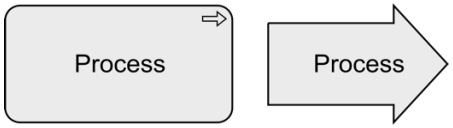
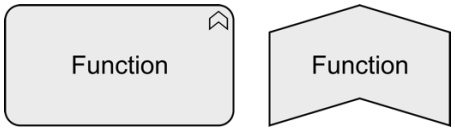
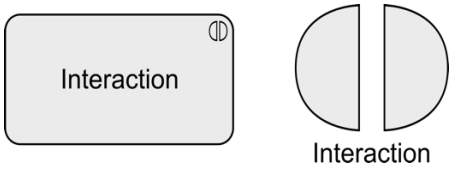
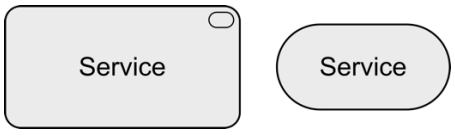
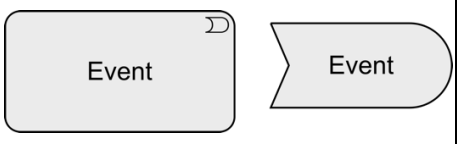
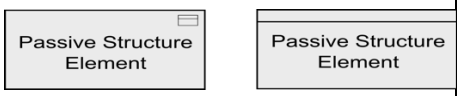
Passiiviset rakenne-elementit ovat rakenteellisia elementtejä, jotka eivät voi suorittaa käyttäytymistä. Passiivinen rakenne-elementti edustaa kohdetta, jolle käyttäytyminen suoritetaan ja ovat usein tieto- tai dataobjekteja, mutta voivat edustaa myös fyysisiä kohteita. Passiivisen rakenne-elementin merkintätapa esitetty taulukossa 1. (Open Group 2023, kappale 4.1.3.)

3.9 Kooste rakenne- ja käyttäytymiselementeistä

Taulukossa 1 esitetään kooste ArchiMaten rakenne- ja käyttäytymiselementeistä.

Taulukko 1. ArchiMaten ydinelementit (mukaillen Open Group 2023, kappale 4.3.)

Elementti	**Erikoistuminen**	**Määritelmä**	**Merkintä**
Aktiivinen Rakenne			
Sisäinen aktiivinen rakenne-elementti		Edustaa kokonaisuutta, joka pystyy käyttäytymään.	
	Yhteistyö	Edustaa sisäisten aktiivisten rakenne-elementtien kokonaisuutta, jotka toimivat yhdessä jonkin kollektiivisen toiminnan suorittamiseksi.	
Rajapinta (ulkoinen aktiivinen rakenne-elementti)		Edustaa yhteyspistettä, jossa yksi tai useampi palvelu esitetään ympäristölle.	

Käyttäytyminen			
Sisäinen käyttäytymiselementti		Edustaa toiminnan yksikköä, jonka yksi tai useampi aktiivinen rakenne-elementti voi suorittaa.	
	Asian käsittely	Edustaa käyttäytymissarjaa, joka saavuttaa tietyn tuloksen.	
	Toiminto	Edustaa tiettyihin kriteereihin perustuvaa käyttäytymismallia, jota hallitaan, suoritetaan tai toteutetaan kokonaisuutena.	
	Vuorovaikutus	Edustaa kollektiivisen käyttäytymisen yksikköä, joka on suoritettava sisäisten aktiivisten rakenne-elementtien toimesta	
Palvelu (ulkoinen käyttäytymiselementti)		Edustaa tarkasti määritettyä käyttäytymistä.	
Tapahtuma		Edustaa tilan muutosta.	
Passiivinen rakenne			
Passiivinen rakenne-elementti		Edustaa elementtiä, jolle käyttäytyminen suoritetaan.	

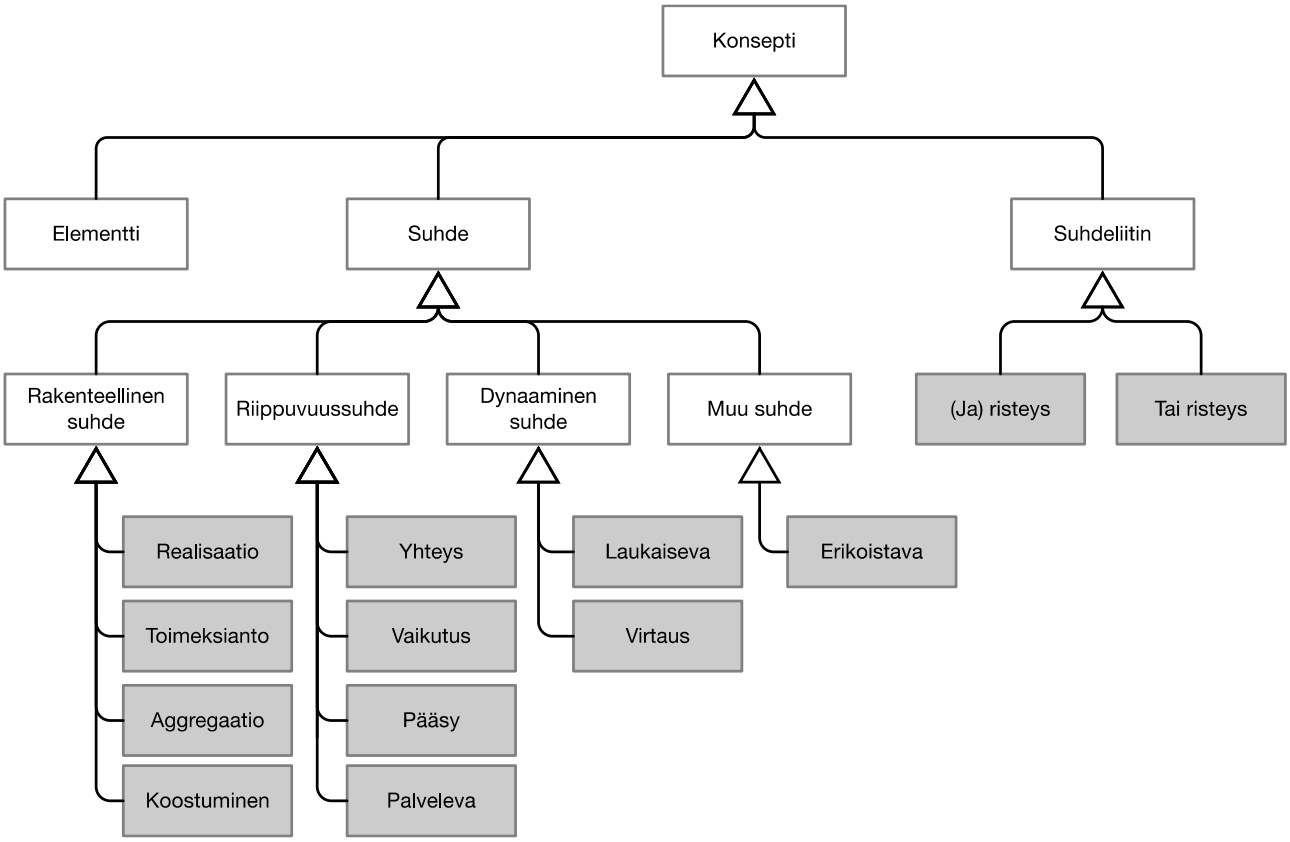
3.10 ArchiMaten suhteet ja suhdeliittimet

ArchiMate kieli määrittelee elementtien lisäksi yleisiä suhteita, joista jokainen voi yhdistää ennalta määritellyn joukon elementtejä.

Suhteet luokitellaan neljään luokkaan:

- Rakenteelliset suhteet, jotka mallintavat saman tai erityyppisten käsitteiden staattista rakennetta tai koostumusta
- Riippuvuussuhteet, jotka mallintavat kuinka elementtejä käytetään tukemaan muita elementtejä
- Dynaamiset suhteet, joita käytetään elementtien välisten käyttäytymisriippuvuuksien mallintamiseen
- Muut suhteet, jotka eivät kuulu mihinkään yllä olevista luokista

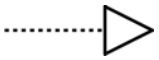
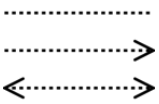
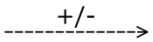
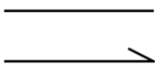
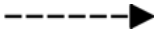
Jokaisella suhteella on päätepisteinä täsmälleen yksi lähtö- ja päätepiste, joka voi olla elementti, suhde tai suhdeliitin. Yhteenveto ArchiMaten suhteista esitetään kuvassa 7. (Open Group 2023, kappale 5.)

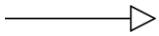
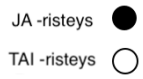


Kuva 7. Yhteenveto ArchiMaten suhteista (mukaillen Open Group 2023, kappale 5.)

Taulukossa 2 esitetään koostetusti ArchiMaten suhteet ja niiden merkintätapa.

Taulukko 2. ArchiMaten suhteet (mukaillen Open Group 2023, kappale 5.6.)

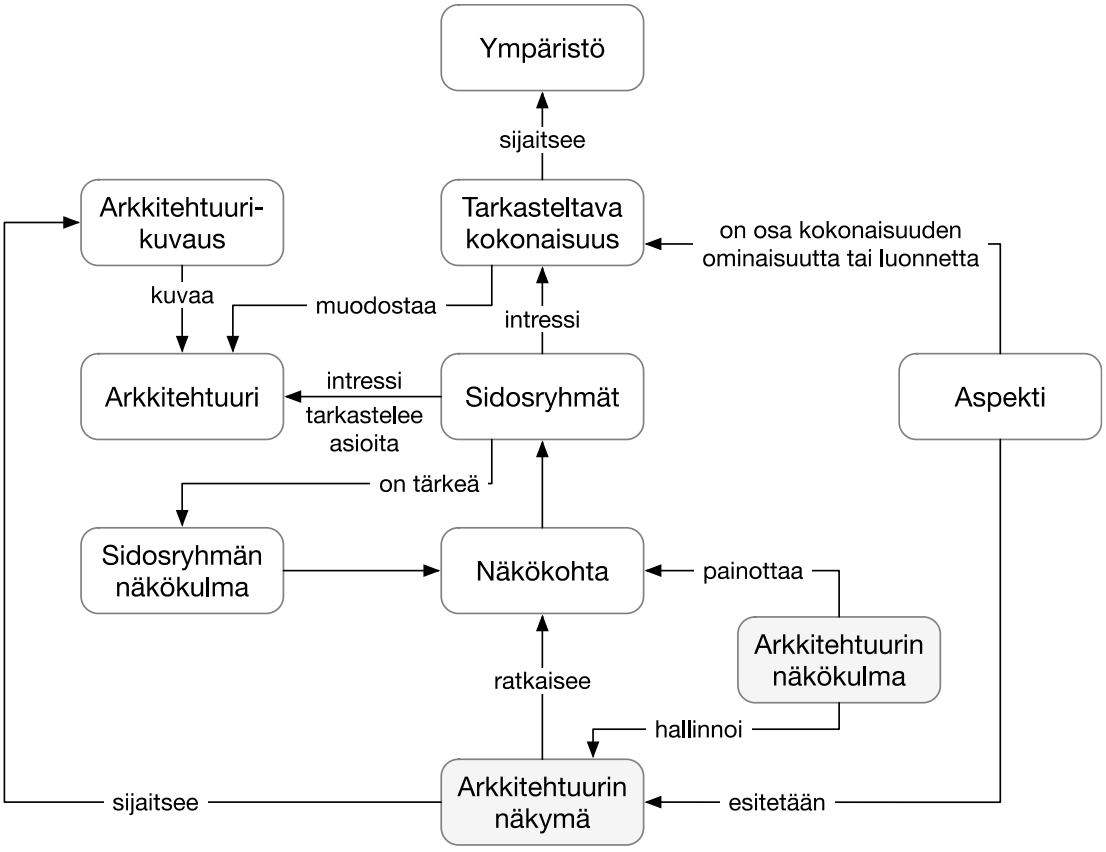
Rakenteelliset suhteet	**Kuvaus**	**Merkintä**
Koostuminen (Composition)	Esittää, että elementti koostuu yhdestä tai useammasta muusta käsitteestä.	
Yhdistäminen (Aggregation)	Esittää, että elementti yhdistää yhden tai useamman muun käsitteen.	
Toimeksianto (Assignment)	Esittää vastuun jakoa, käyttäytymisen suorittamista, tallennusta tai toteutusta.	
Toteutus (Realization)	Esittää, että elementillä on kriittinen rooli abstraktimman elementin luomisessa, saavuttamisessa, ylläpitämisessä tai toiminnassa.	
Riippuvuussuhteet		
Palveleva (Serving)	Esittää, että elementti tarjoaa toiminnallisuutensa toiselle elementille.	
Pääsy (Access)	Edustaa käyttäytymisen ja aktiivisten rakenne-elementtien kykyä tarkkailla tai toimia passiivisten rakenne-elementtien kanssa.	
Vaikutus (Influence)	Esittää, että elementti vaikuttaa jonkin motivaatioelementin toteuttamiseen tai saavuttamiseen.	
Yhteys (Association)	Edustaa määrittelemätöntä suhdetta tai sellaista, jota ei edusta toinen ArchiMate-suhde.	
Dynaamiset suhteet		
Laukaiseva (Triggering)	Edustaa ajallista tai kausaalista suhdetta elementtien välillä.	
Virtaus (Flow)	Edustaa siirtymistä elementistä toiseen.	
Muut suhteet		

Erikoistuminen (Specialization)	Esittää, että elementti on erikoistunut toisesta elementistä.	
Suhdeliittimet		
Risteys (Junction)	Käytetään yhdistämään samantyyppisiä suhteita.	

3.11 ArchiMaten näkymät ja näkökulmat

Katakrin kriteeristö ja sen vaatimukset esitetään opinnäytetyön tuloksena syntyneen mallinnuksen ArchiMaten näkymissä. ArchiMaten käyttämä näkökulmamekanismi noudattaa ISO/IEC 42010 standardia, joka tarjoaa mallin arkkitehtuurien kuvauksille ja on esitetty kuvassa 8. (Open Group 2023, kappale 13.2).

> "Arkkitehtuurin näkökulma tarjoaa tavan tarkastella kokonaisuuden arkkitehtuuria ja antaa arkkitehdeille resurssit kokonaisuuden mallintamiseen suhteessa kyseisen näkökulman painottamiin näkökohtiin. Yhtä näkökulmaa voidaan soveltaa useampiin kokonaisuuksiin. Kukin näkymä on yksi tällainen soveltamiskerta." (ISO 2023, 47)



Kuva 8. Arkkitehtuurin näkymät ja näkökulmat (mukaillen ISO 2023, 18)

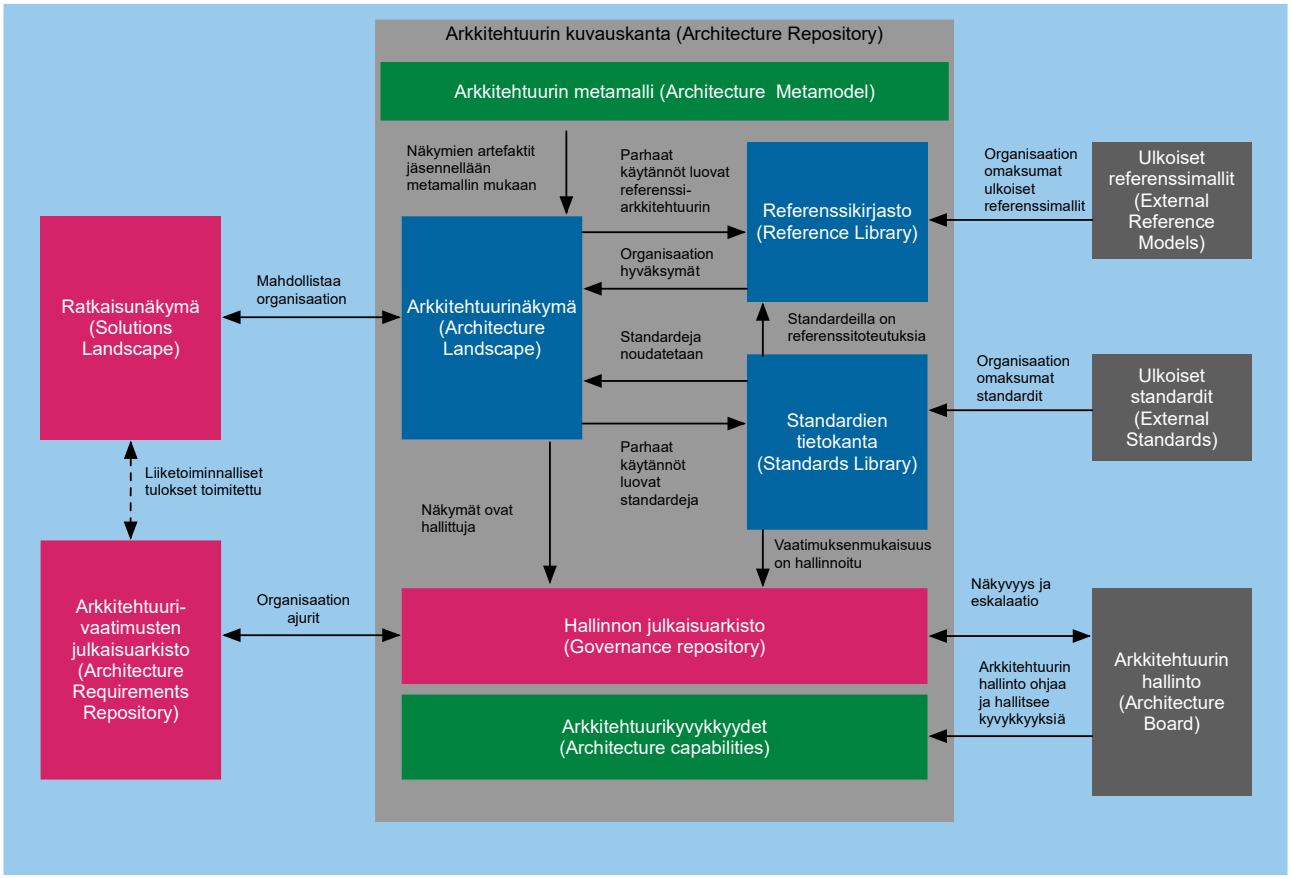
3.12 ArchiMaten tiedostomuoto

ArchiMatella luodut mallit talletetaan XML tiedostomuodossa, joka kuvataan tarkalla tasolla standardin dokumentissa ArchiMate Model Exchange File Format for the ArchiMate Modeling Language. ArchiMaten tukee standardimuotoista XML pohjaista tiedostojen vaihtoa, mikä mahdollistaa mallien käsittelyn eri työkalujen välillä ja siten yhteistyön eri toimijoiden kesken. Tiedostoformaattiin sisältyy pakollisena vaatimuksena elementtien dokumentaatio -ominaisuus, mikä edesauttaa toimijoiden välistä tiedonvälitystä (Open Group 2023, kappale 1.1; Open Group 2019b, kappale 3.1.)

3.13 Mallien ylläpito

Vaikka yksinkertaisimmillaan malleja voidaan käsitellä tiedostotasolla malli kerrallaan, jaettujen julkaisukantojen (repository) hyödyntäminen tehostaa mallien ylläpitoa huomattavasti. Kaupalliset ArchiMate ohjelmistot sisältävät tyypillisesti jaettujen kuvauskantojen ominaisuuden, mutta avoimen lähdekoodin Archi -ohjelmistoon se tulee asentaa coArchi -laajennoksena. Kuvauskantojen avulla malleja ja niiden pääsynhallintaa voidaan hallita keskitetysti ja ne tarjoavat tyypillisesti myös versionhallintaominaisuuksia.

Noudattamalla kokonaisarkkitehtuurimallia, mallinnukset ja niihin liittyvät käytännöt voidaan liittää saumattomasti osaksi organisaation arkkitehtuuritoimintaa, jolloin myös mallinnusprosessit ja -tavat voidaan yhdenmukaistaa. Tallentamalla mallinnukset jaettuihin arkkitehtuurin kuvauskantoihin ja näkymiin, ne ovat hyödynnettävissä palveluiden koko elinkaaren ajan. Kun ratkaisuista luodut mallit tallennetaan ratkaisunäkymiin ja vaatimuksista luodut mallit arkkitehtuurivaatimusten julkaisuarkistoihin, tiedetään organisaatiossa, mistä tietyn alueen mallinnukset löytyvät. Arkkitehtuurin kuvauskannat on esitetty kuvassa 9.



Kuva 9. Arkkitehtuurin kuvauskanta (mukaillen Open Group 2022a, kappale 3.11)

3.14 ArchiMate työkalut

Open Group ylläpitää Open Group Architecture Tool -sertifiointiohjelmaa ArchiMate työkaluille. Sertifiointiohjelma sisältää vaatimuksenmukaisuusvaatimukset, ohjeet ja käytännöt sertifioinnin suorittamiseksi ja sertifioiduista työkaluista pidetään listaa Open Groupin sivustolla. (Open Group s.a.) Tämän opinnäytetyön mallinnuksen kokemuspohja on saatu käyttämällä BizzDesign, Sparx ja Archi -työkaluja, joista sekä BizzDesign ja Sparx on sertifioitu ArchiMate mallinnustyökaluksi. Vaikka Archi -työkalulla ei ole virallista sertifiointia, se valikoitui mm. avoimuuden perusteella opinnäytetyön mallinnuksessa käytetyksi ohjelmaksi.

Bizzdesign Enterprise Studio

Bizzdesign Enterprise Studio on näistä käytetyistä työkaluista laajin ja pitää sisällään kattavat toiminnallisuudet. Työkalun sisäänrakennettuna ominaisuutena on mm. useamman kielen tuki, jolloin esimerkiksi Turvallisuusperiaatteet. -niminen elementti voidaan esittää samassa mallissa myös ruotsiksi nimellä Säkerhetsprinciper ja englanniksi nimellä Security principles, jolloin eri kielille ei tarvitse luoda omia malleja. Bizzdesign sisältää myös useita riskien ja turvallisuudenhallinnan osa-

alueiden laajennoksia ja esimerkkejä, joiden pohjalta se soveltuu hyvin riskien ja turvallisuudenhallinnan osa-alueiden mallintamiseen. (Bizzdesign 2023)

Sparx Enterprise Architect

Sparx Enterprise Architect pitää sisällään myös kattavia ominaisuuksia, kuten velhopohjaisen ArchiMate -näkymien luomisen, mutta jää muissa ominaisuuksissa ja ArchiMate standardin päivitysykleissä jälkeen muista mallinnustyökaluista. Opinnäytetyön mallintamisen aikana Sparx ei vielä tukenut ArchiMaten viimeisintä, 3.2 versiota. Rajoitteista huolimatta Sparx soveltuu myös turvallisuuskriteeristöjen mallintamiseen. (Sparx Systems 2023)

Archi – ohjelmisto

Tämän opinnäytetyön mallinnuksissa käytettiin Archi -ohjelmistoa, joka on puhtaasti ArchiMate mallinnukseen suunniteltu avoimen lähdekoodin mallinnustyökalu. Archi on yksi suosituimmista mallinnustyökaluista ja se on otettu laajasti käyttöön. Muun muassa Euroopan komissio hyödyntää ArchiMate mallinnuskieltä aktiivisesti ja on julkaissut myös oman laajennoksen EIRA viitearkkitehtuurista Archi -ohjelmistolle (Euroopan komissio 2023).

Archi -ohjelmisto oli alun perin osa Ison-Britannian kansallista hanketta, jonka tarkoituksena oli tukea kokonaisarkkitehtuuriohjelmaa korkeakoulusektorilla. Alkuperäistä projektia isännöi Boltonin yliopisto Isossa-Britanniassa. Vuodesta 2013 lähtien Archi -mallinnustyökalua ja siihen liittyviä kehityshankkeita on hallinnoitu archimatetool.com sivustolla, josta ohjelmisto ja sen laajennusosia on myös ladattavissa. (Beauvoir & Sarrodie 2023).

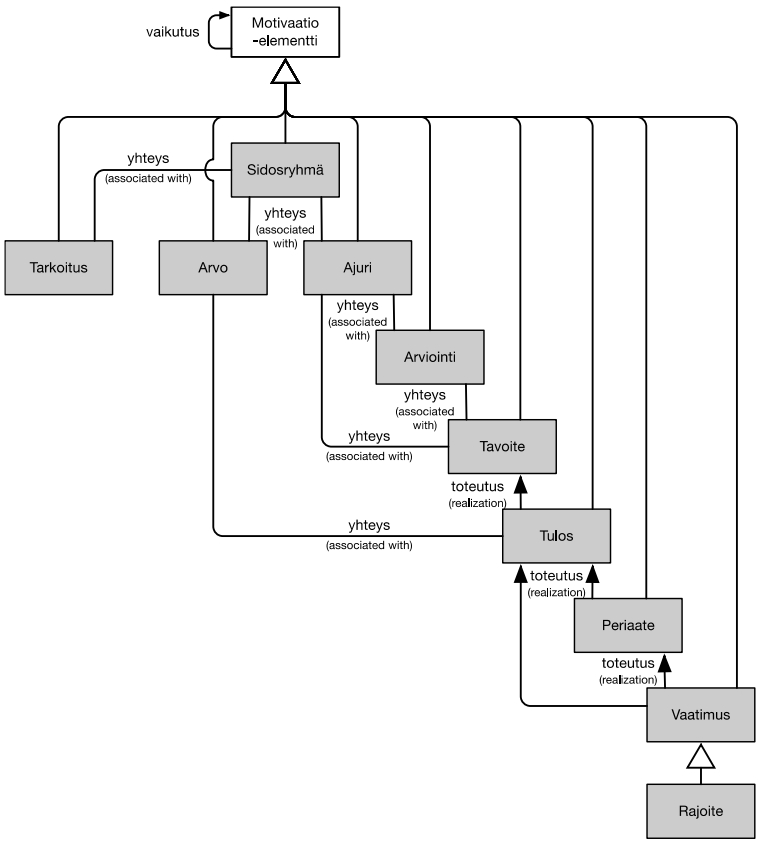
4 Riskien ja turvallisuuden hallinnan mallintaminen ArchiMatella

ArchiMate standardissa itsessään käsitellään riskien ja turvallisuuden hallintaan liittyviä elementtejä vain lyhyesti. ArchiMaten lähtökohtana oli suunnitella mallinnuskieli mahdollisimman pieneksi, mutta silti käyttökelpoiseksi useimpiin kokonaisarkkitehtuurien mallinnustehtäviin. ArchiMate on tarkoituksella rajoitettu käsitteisiin, jotka riittävät mallintamaan yleisimmät käytännön tapaukset (Open Group 2023, kappale 3.1).

Riskien ja turvallisuuden hallinnassa voidaan hyödyntää ArchiMaten motivaatioaspektin sekä strategia- ja liiketoimintakerroksen elementtejä (Open Group 2023, kappale 14.2).

4.1 Motivaatioelementit

Riskien ja turvallisuuden hallinnassa voidaan hyödyntää ArchiMaten motivaatioelementtejä, joita käytetään mallintamaan motiiveja tai syitä, jotka ohjaavat kokonaisarkkitehtuurin suunnittelua ja muutosta. Tietoturvaan liittyvissä mallinnuksissa voidaan käyttää suoraan esimerkiksi motivaatioelementtien arviointien, ajureiden, sidosryhmien, tavoitteiden ja vaatimusten merkintätapoja. Motivaatioelementtien metamalli esitetään kuvassa 9. (Open Group 2023, kappale 6.)



Kuva 10. Motivaatioelementtien metamalli (mukaillen Open Group 2023, kappale 6)

Sidosryhmä (Stakeholder)

Sidosryhmä edustaa yksilön, ryhmän tai organisaation roolia, joka edustaa heidän etujaan. Sidosryhmillä on yksi tai useampi intressi tai huolenaihe organisaatiossa tai sen kokonaisarkkitehtuurissa. Sidosryhmät voivat vaikuttaa toisiinsa. Esimerkkeinä sidosryhmistä ovat yrityksen toimitusjohtaja, hallitus, osakkeenomistajat, asiakkaat ja myös viranomaiset. Sidosryhmien merkintätapa esitetään taulukossa 3. (Open Group 2023, kappale 6.2.1.)

Ajuri (Driver)

Ajuri edustaa sisäistä tai ulkoista tilaa, joka motivoi organisaatiota asettamaan tavoitteensa ja toteuttamaan niiden saavuttamiseksi tarvitut muutokset. Ajureita, jotka liittyvät johonkin sidosryhmään, kutsutaan kyseisen sidosryhmän huolenaiheeksi. Sisäisiä ajureita voivat olla kustannustehokkuus, ja asiakastyytyväisyys. Ajureina voi toimia myös organisaation ulkoiset tekijät, kuten toimintaympäristön taloudelliset muutokset tai muutokset lainsäädännössä. Ajureiden merkintätapa esitetään taulukossa 3. (Open Group 2023, kappale 6.2.2.)

Arviointi (Assessment)

Arviointi esittää organisaation tilanteen analyysin tulosta jonkin ajurin suhteen. Arviointi -merkintää voidaan käyttää mallintamaan vahvuuksia, heikkouksia, mahdollisuuksia tai uhkia mallinnuksen kohteena olevalla alueella. Arvioinneista vahvuudet ja heikkoudet ovat organisaation sisäisiä ja mahdollisuudet ja uhat organisaation ulkoisia. Vahvuudet ja mahdollisuudet voidaan muuttaa suoraan tavoitteiksi. Arviointien merkintätapa esitetään taulukossa 3. (Open Group 2023, kappale 6.2.3.)

Tavoitteet (Goal)

Tavoite edustaa organisaation asettamaa tavoitetta, aikomusta tai haluttua lopputulosta itselleen tai sidosryhmilleen. Tavoite voi edustaa mitä tahansa sidosryhmän haluamaa päämäärää, kuten saavutettua kyvykkyyttä tai tulosta. Tavoitteita voidaan jakaa useampaan alitavoitteisiin. Tavoitteiden merkintätapa esitetään taulukossa 3. (Open Group 2023, kappale 6.3.1.)

Tulokset (Outcome)

Tulokset edustavat tietyn asiantilan seurausta, vaikutusta tai lopputulosta. Tulokset tuotetaan organisaation kyvyillä ja sen arkkitehtuurin ydinelementeillä, joilla saavutetaan halutut ominaisuudet. Tulokset ovat konkreettisia ja ne voidaan yhdistää arviointeihin. Tuloksia voidaan käyttää mallintamaan myös ei-toivottujen vaikutusten mallintamiseen, kuten suunniteltaessa riskien lieventäviä toimenpiteitä. Tulosten merkintätapa esitetään taulukossa 3. (Open Group 2023, kappale 6.3.2.)

Periaate (Principle)

Periaate määrittelee menetelmän, tavan tai linjauksen, millä jokin aikomus on tarkoitus suorittaa tietyssä arkkitehtuurin kontekstissa. Periaatteilla voidaan määritellä yleinen ominaisuus laadullisesti. Periaatteilla voidaan esimerkiksi kuvata organisaation toiminta- ja menettelytavat tai miten kehitystyötä organisaatiossa suoritetaan. Periaatteiden merkintätapa esitetään taulukossa 3. (Open Group 2023, kappale 6.3.3.)

Vaatimus (Requirement)

Vaatimukset määrittävät tietyn arkkitehtuurin osan ominaisuuden, joilla tavoitteilla mallinnetut päämäärät saavutetaan. Vaatimuksilla voidaan kuvata ominaisuuksia, joita järjestelmiltä vaaditaan tavoitteiden toteuttamiseksi. Liiketoiminnan tavoitteet tulee toteuttaa suunnitelmilla tai konkreettisilla muutostavoitteilla, mikä voi asettaa vaatimuksia, ja siten muutoksia olemassa olevaan liiketoiminta-arkkitehtuuriin. Vaatimusten merkintätapa esitetään taulukossa 3. (Open Group 2023, kappale 6.3.4.)

Rajoite (Constraint)

Rajoite edustaa arkkitehtuuriin näkökohtiin, toteutusprosessiin tai toteutukseen liittyvää rajoitusta. Rajoite ei edellytä suunniteltua toiminnallisuutta, vaan asettaa rajoituksen tavalle tai toiminnalle, jolla jokin aikomus on tarkoitus suorittaa tietyssä arkkitehtuurin kontekstissa. Rajoitus voi liittyä esimerkiksi toteutukseen, toiminnallisuuteen tai käyttöönottoon. Rajoitteiden merkintätapa esitetään taulukossa 3. (Open Group 2023, kappale 6.3.5.)

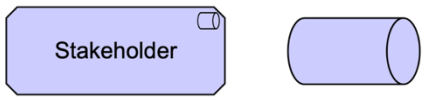
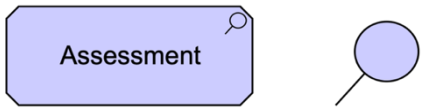
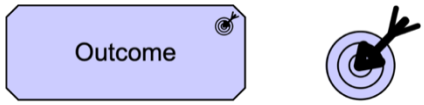
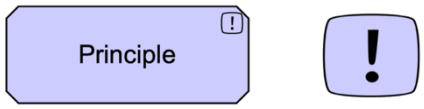
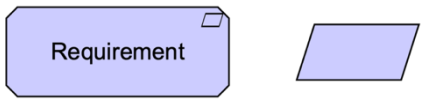
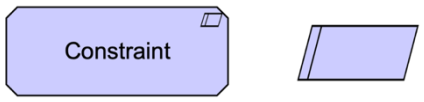
Merkitys (Meaning)

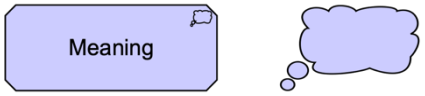
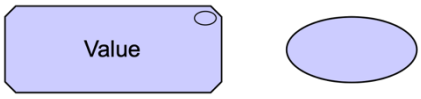
Merkitys esittää kohteen merkitystä tarkasteltavasta näkökulmasta. Se voi edustaa tietoa, asiantuntimusta tai sille annettua tulkintaa tietyssä kontekstissa. Merkitys voidaan liittää mihin tahansa käsitteeseen. (Open Group 2023, kappale 6.4.1.)

Arvo (Value)

Arvo edustaa tarkasteltavan kohteen suhteellista arvoa, hyödyllisyyttä tai tärkeyttä. Arvo voi esittää toiminnan tai palvelun hyödyllisyyttä tai etua sidosryhmälle ja se esitetään usein taloudellisena arvona. (Open Group 2023, kappale 6.4.2.)

Taulukko 3. Motivaatioelementtien merkintätavat (mukaillen Open Group 2023, kappale 6.5.)

Elementti	Määritys	Merkintätapa
Sidosryhmä (Stakeholder)	Sidosryhmä edustaa yksilöä, ryhmää tai organisaatiota.	
Ajuri (Driver)	Ajuri esittää tekijää, mikä motivoi organisaatiota määrittelemään tavoitteensa ja toteuttamaan tarvittavat muutokset niiden saavuttamiseksi.	
Arviointi (Assessment)	Arviointi esittää analyysin tulosta suhteessa johonkin ajuriin.	
Tavoite (Goal)	Tavoite esittää aikomusta, suuntaa tai organisaation ja sen sidosryhmien haluamaa lopputilaa.	
Tulos (Outcome)	Tulos esittää tietyn tilanteen lopputulosta, vaikutusta tai seurausta.	
Periaate (Principle)	Periaate esittää menetelmää, tapaa tai linjausta, millä jokin aikomus on tarkoitus suorittaa tietyssä arkkitehtuurin kontekstissa.	
Vaatimus (Requirement)	Vaatimus edustaa tiettyyn arkkitehtuurin kuvaamaan järjestelmään tai osa-alueeseen kohdistuvaa täsmällistä tarvemääritystä.	
Rajoite (Constraint)	Rajoite esittää arkkitehtuurin näkökohtiin, toteutusprosessiin tai toteutukseen kohdistuvaa rajoitusta.	

Merkitys (Meaning)	Merkitys edustaa arkkitehtuurin käsitteen tulkintaa, esimerkiksi konseptissa olevaa tietoa tai asiantuntemusta ja ilmaisee kyseisen elementin tarkoituksen	
Arvo (Value)	Arvo edustaa konseptin suhteellista arvoa, hyödyllisyyttä tai tärkeyttä.	

4.2 Strategiakerros

Strategiakerroksen elementeillä mallinnetaan tyypillisesti organisaatioiden strategioihin liittyviä tekijöitä ja valintoja.

Resurssi (Resource)

Organisaatioiden tai yksilöiden omistamaa tai hallitsemaa omaisuutta mallinnetaan resurssielementillä, joka sisältyy Archimaten strategiakerrokseen. (Open Group 2023, kappale 7.2.1.)

Kuva 11. ArchiMaten resurssi -elementin merkintätapa (mukaillen Open Group 2023, kappale 7.2.1)

Riskien ja turvallisuuden hallinnan näkökulmasta strategiakerroksen resurssi -elementeillä mallinnetaan usein riskin kohteena olevia resursseja, kuten omaisuutta.

4.3 Liiketoimintakerros

Riskien ja turvallisuuden hallinnassa voidaan hyödyntää ArchiMaten liiketoimintakerroksen elementtejä, joilla mallinnetaan yrityksen toiminnallista organisaatiota teknologiariippumattomalla tavalla. Liiketoimintakerroksen elementeistä voidaan tietoturvaan liittyvissä mallinnuksissa hyödyntää mm. Liiketoiminnan toimijaa (Business Actor) ja tapahtumaa (Business Event). (Open Group 2023, kappale 8.)

Liiketoiminnan toimija (Business Actor)

Toimija edustaa organisaation sisäistä tai ulkoista toimijaa, kuten työntekijää, asiakasta tai yhteistyökumppania. Toimija voidaan liittää yhteen tai useampaan rooliin ja siten suorittaa käyttäytymistä, johon nämä roolit on määritetty. Toimija edustaa aktiivista rakenne-elementtiä ja voivat olla henkilöitä tai organisaatioita (Open Group 2023, kappale 8.2.2.). Toimijoiden merkintätapa esitetään taulukossa 4.

Liiketoimintatapahtuma (Business Event)

Tapahtumat edustavat liiketoiminnassa tapahtuvia tilamuutoksia, jotka voivat laukaista tai keskeyttää liiketoimintaprosesseja ja muita liiketoimintakäyttäytymisiä. Tapahtumat ovat välittömiä, eikä niillä ole kestoa ja ne voivat olla sisäisiä tai ulkoisista ympäristöstä johtuvia. Tapahtumalla voi olla aika-attribuutti, joka ilmaisee ajan tai hetken, jolloin se on tapahtunut (Open Group 2023, kappale 8.3.4.). Tapahtumien merkintätapa esitetään taulukossa 4.

4.4 Archimate kielen mukautusmekanismit

Riskien ja turvallisuuden hallinnan tietoturvaan suoraan liittyviä merkintätapoja käsitellään ArchiMaten standardissa lyhyesti kielen mukautusmekanismit kappaleessa. Mukautusmekanismissä kuvataan, miten kieltä voidaan mukauttaa lisäkäsitteillä ilman, että kieltä kuormitetaan monilla lisäkäsitteillä ja merkinnöillä. Jokaiseen ArchiMate -mallin konseptiin voidaan liittää attribuutteja ja näin rikastaa konsepteja lisätiedoilla. (Specialization of Concepts) avulla (Open Group 2023, kappale 14).

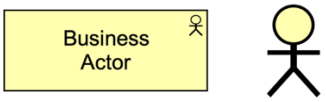
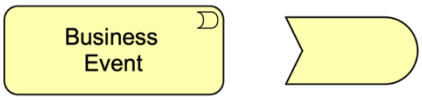
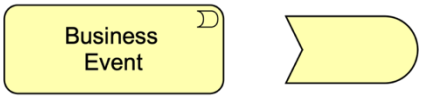
4.5 Attribuuttien lisääminen ArchiMaten konsepteihin

ArchiMate kieli mahdollistaa attribuuttien liittämisen jokaiseen konseptiin, joka voi olla elementti, suhde tai suhdeliitin. Attribuutit tarjoavat mahdollisuuden määrittää konsepteille, tai suhdeliittimille lisäominaisuuksia, kuten lukuarvoja, joiden avulla voidaan suorittaa mallipohjaisia kustannus- tai suorituskykylaskelmia. ArchiMate kieli tarjoaa konsepteille rikastumismahdollisuuden myös profilointi -erikoistumismenetelmällä, jossa tietorakenne voidaan määritellä ja liittää dynaamisesti käsitteisiin erillään ArchiMate -kielestä. Profiilit määritetään attribuuttien ryhminä, joissa jokaisella määritteellä on käyttäjän muutettavissa oleva oletusarvo. Profiilit voivat olla ennalta määritettyjä tai käyttäjän määrittämiä profiileja, joille sallitaan erilaisia attribuutteja, kuten merkkijonoja, kokonaislukuja, reaalilukuja, valuutta-arvoja, päivämääriä tai totuusarvoja. Lisäksi tuetaan monimutkaisia tyyppejä, joiden rakenne koostuu yhdestä tai useammasta perustyypin kentistä tai listoista. (Open Group 2023, kappale 14.1.)

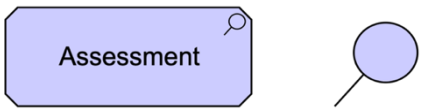
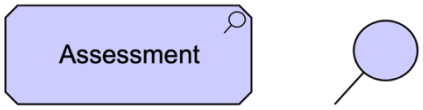
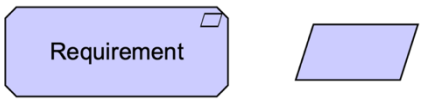
4.6 Käsitteiden erikoistaminen (Specialization of Concepts)

Tietoturvaan liittyviä elementtejä voidaan määritellä käsitteiden erikoistamisominaisuudella (Specialization of Concepts), joka on yksinkertainen tapa määritellä uusia elementtejä ja suhteita olemassa olevien pohjalta. Erikoistamisessa elementit määritellään olemassa olevien isäntäelementtien (parent) pohjalta ja ne perivät näiltä samat ominaisuudet. Elementtien lisäksi myös suhteiden erikoistaminen on sallittua, jolloin suhteet perivät kaikki sen ”emosuhteen” (parent) ominaisuudet. ArchiMate standardissa on kuvattu esimerkkeinä liiketoimintakerroksen ja motivaatioelementtien erikoistaminen tietoturvallisuuden mallintamiseksi taulukoissa 3 ja 4. (Open Group 2023, kappale 14.2.)

Taulukko 4. Esimerkki ArchiMaten liiketoimintakerroksen erikoistumisista (mukaillen Open Group 2023, kappale 14)

Käsite	Erikoistunut konsepti	Kuvaus	Merkintätapa
Toimija (Business Actor)	Uhka-agentti (Threat Agent)	Mikä tahansa vahinkoa aiheuttamaan kykenevä asia, joka voi kohdistua organisaation kokonaisarkkitehtuuriin	
Tapahtuma (Business Event)	Uhkatapahtuma (Threat Event)	Tapahtuma, joka voi vaikuttaa omaisuuteen haitallisesti. Esimerkiksi hyökkäys, joka on seurausta hyökkääjän (uhka-agentin) tahallisesta haitallisesta toiminnasta.	
Tapahtuma (Business Event)	Menetystapahtuma (Loss Event)	Mikä tahansa omaisuuden menetyksen tai vahingoittumisen seuraus.	

Taulukko 5. Esimerkki Archimaten motivaatiokerroksen erikoistumisista (mukaillen Open Group 2023, kappale 14)

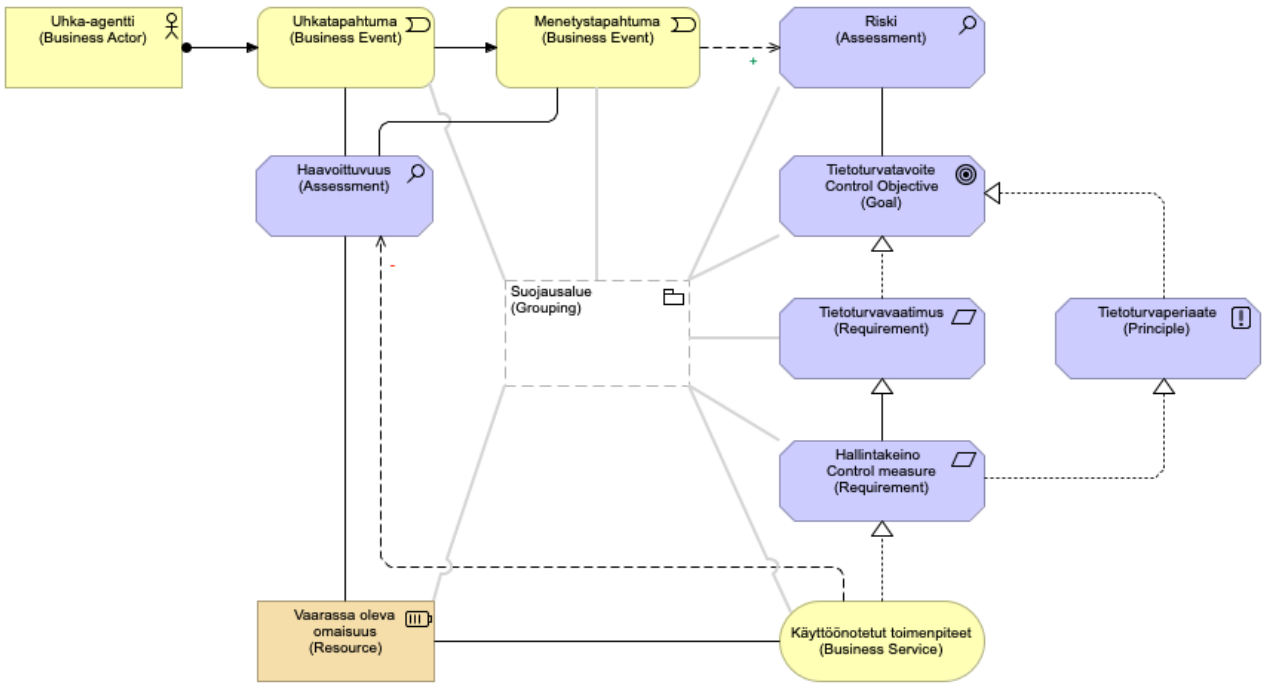
Käsite	Erikoistunut konsepti	Kuvaus	
Arviointi (Assesment)	Haavoittuvuus (Vulnerability)	Todennäköisyys siihen, ettei omaisuus pysty vastustamaan uhka-agentin toimia.	
Arviointi (Assesment)	Riski (Risk)	Tulevien menetyksien todennäköinen laajuus ja toistuvuus.	
Tavoite (Goal)	Ohjaustavoite (Control Objective)	Määrättyjen valvontatoimenpiteiden tavoite, joilla on tarkoitus lieventää organisaatioon kohdistuvia riskejä.	
Vaatimus (Requirement)	Valvontatoimenpide (Control Measure)	Toiminta, jolla vähennetään uhkaa, haavoittuvuutta tai hyökkäystä poistamalla, estämällä tai minimoimalla sen aiheuttama haitta. Valvontatoimenpiteisiin sisältyy myös uhkahavainnot ja ilmoittamiset, jotta voidaan ryhtyä korjaaviin toimenpiteisiin.	

Riskien hallinnan ja tietoturvan mallinnusta ArchiMatella on kuvattu tarkemmin Open Groupin julkaisussa ”How to Model Enterprise Risk Management and Security with the ArchiMate® Language”. Julkaisussa kuvataan tarkemmalla tasolla, miten riskienhallintaa ja turvallisuutta voidaan mallintaa ArchiMate -kielellä. Julkaisussa käsitellään yhteiset riskienhallinnan ja turvallisuuden käsitteet, jotka on sisällytetty ArchiMate standardiin ja kehykseen, ja jotka ovat merkityksellisiä kokonaisarkkitehtuurimallien yhteydessä (Open Group 2019a).

Julkaisu tarjoaa mallinnukseen kolme vaihtoehtoa:

1. ArchiMate elementtien standardin mukainen muokkaamaton käyttö
2. Hyödyntämällä ArchiMate -kielen mukautumismekanismeja määrittelemällä lisäattribuutteja ja erikoistamiselementtejä.
3. Hyödyntämällä lisäelementtejä, jotka eivät vielä ole ArchiMate määrityksessä ja jotka voidaan liittää suoraan olemassa oleviin elementteihin. (Open Group 2019a, 34.)

Julkaisussa turvallisuuskriteerin ja turvallisuustavoitteen käsitteet yhdistetään turvallisuustavoitteen (Control objective) käsitteeseen, jonka mallinnuksessa käytetään tavoite (Goal) -elementtiä. (Open Group 2019a, 34.)



Kuva 12. Riski- ja turvallisuuselementtien vastaavuus ArchiMate kielellä (mukaillen Open Group 2019a, 26)

Riskien hallinnan näkökulmasta Katakrin turvallisuusmalli on yhdistelmämalli, joka koostuu vähimmäissuojauksista, joiden tavoitteena on pienentää tarkasteltavan käyttöympäristön yleisiä turvallisuusluokiteltuun tietoon kohdistuvia riskejä hyväksyttävälle tasolle (Katakri 2020, 114). Nämä vähimmäisuojaukset on kuvattu Katakrin kriteereissä vaatimuksina, jotka mahdollistavat erilaisia toteutustapoja, joilla voidaan useimmissa ympäristöissä saavuttaa hyväksyttävä suojausten vähimmäistaso (Katakri 2020, 5).

Koska opinnäytetyö keskittyy Katakrissa esitettyjen vaatimusten mallinnukseen, voidaan käytettyjen konseptien määrä rajoittaa kriteeristön osalta muutamaan elementtiin. Katakrissa esitetyt

kriteeri käsitellään tavoitteina ja mallinnetaan käyttäen tavoite -elementtiä ja kriteereissä esitetyt vaatimukset mallinnetaan käyttäen vaatimus -elementtiä.

Tavoite- ja vaatimuselementtien lisäksi Katakrin toteutusesimerkkien mallinnuksissa kuvataan myös muita elementtejä, kuten sovellus- ja teknologiaelementtejä. Sovellus- ja teknologiaelementtejä pidetään kokonaisarkkitehtuurin hallinnassa useimmiten liiketoimintaan liittyvinä elementteinä, mutta tietojärjestelmien turvallisuusriskien hallinnan näkökulmasta niitä pidetään kuitenkin tietojärjestelmän omaisuuksina, koska ne ovat osa tietojärjestelmää käsittelevää tietoa ja voivat siten olla tietoturvauhkien tai haavoittuvuuksien lähteen kohteena. (Mayer & Feltus 2017, 108)

5 Kansallisen turvallisuusauditointikriteeristön mallintaminen

Lähtötilanteessa pyrittiin kirjallisuuskatsauksen avulla tutkimaan riskien ja turvallisuudenhallinnan mallinnuksiin liittyviä tieteellisiä artikkeleita, kirjoja ja muita julkaisuja saatavilla olevan tiedon ja käytännön sovellutusten hahmottamiseksi. Viranomaisten kriteeristöt olivat saatavilla Kyberturvallisuuskeskuksen, ulkoministeriön ja valtioneuvoston verkkosivustoilta ja ArchiMate standardi Open Groupin verkkosivustolta. Riskien ja turvallisuudenhallinnan näkökulman tukemiseksi opinnäytetyössä hyödynnettiin ”How to Model Enterprise Risk Management and Security with the ArchiMate® Language” julkaisua ja ArchiMate standardin tukemiseksi useita muita lähteitä, kuten Hosiaisluoman, Lankhorstin ja Wierdan julkaisuja (Open Group 2019a; Hosiaisluoma 2022a; Hosiaisluoma 2022b; Lankhorst et al 2013; Wierda 2021). Kriteeristöjen vertailujen yhteydessä huomattiin, että Katakrin ja Julkrin kriteeristössä viitataan ISO 27001 (Katakri 5 viittausta, Julkri 8 viittausta) ja 27002 (Katakri 29 viittausta, Julkri 82 viittausta) -standardeihin useita kertoja, joten niissä esitettyjen tietoturvatavoitteiden hallintakeinot sisällytettiin mukaan kirjallisuuskatsaukseen ja vertailuun (ISO 2022a, 16; ISO 2022B 19).

Mallinnustyökaluksi valikoitui avoimeen lähdekoodiin perustuva Archi -työkalua, koska se on vapaasti saatavilla archimatetool.com verkkosivustolta. Lisäksi päätettiin hyödyntää Archin coArchi -laajennosta, jonka avulla mallinnuksessa voitiin hyödyntää versionhallintaa. coArchi -laajennos on myös ladattavissa archimatetool.com sivustolta.

Mallinnus aloitettiin luomalla luotiin tyhjä kuvauskanta (repositorio) GitHub verkkopalveluun ja uusi malli Archi -työkaluun. Varsin pian mallinnuksessa kävi ilmi, että elementtien tietojen siirtäminen Katakrista suoraan malliin oli lähdemateriaalin rakenteen vuoksi haastavaa ja aikaa vievää. Koska lähdemateriaalissa kriteerien tiedot oli jaettu vähintään kymmeneen eri kenttään, tietojen sijoittaminen ArchiMate -työkalussa oikeisiin kohtiin oli hidasta. Toiminnallisen osuuden nopeuttamiseksi koko kriteeristö päätettiin muuntaa ensin muotoiluvapaaseen muotoon, jotta itse mallinnus sujuisi mahdollisimman tehokkaasti. Muotoiluvapaasta tekstitiedostosta kriteerien ja vaatimusten elementtien luominen nopeutui huomattavasti.

Yhtenä vaihtoehtona alkuvaiheessa oli julkaista valmis mallinnus GitHub -verkkopalvelussa kuvauskantamuodossa (repositorio), mutta tällöin mallin hyödyntäminen olisi vaatinut Archi ohjelmiston ja sen coArchi -laajennoksen asentamisen. Jotta valmista mallia voi hyödyntää mahdollisimman helposti, se päätettiin julkaista ArchiMate standardin tiedostomuodoissa, joita voi käyttää suoraan ArchiMate -työkaluissa ilman lisäosien asentamista.

Tavoitteena oli julkaista Katakrista malli, jota riskien ja turvallisuuden hallintaan osallistuvat voisivat hyödyntää mallintaessaan suojauksia ympäristöihin, joiden tavoitellaan saavuttavan Katakrissa

esitetyt suojaukset ja siten käyttää mallia osana tietojärjestelmien turvallisuuden arviointiprosessia. Tavoitteena oli lisäksi tarkastella ArchiMaten soveltuvuutta yleisesti riskien ja turvallisuudenhallinnan mallinnuksiin. Laadullisina kriteereinä opinnäytetyössä oli luoda malli, joka pitää sisällään kaikki Katakrin elementit ja vaatimukset, sekä läpäisee muodollisen ArchiMate määrityksen mukaisuuden tarkastuksen.

Katakrista ei ollut opinnäytetyön valmistumiseen mennessä saatavilla mallinnuksia, jolloin jokainen organisaatio joutuu ensin luomaan Katakrin kriteereistä ja vaatimuksista mallin halutessaan mallintaa kriteeristössä esitetyt vähimmäisvaatimukset. Vähimmäisvaatimusten mallinnus aiheuttaa turhaa päällekkäistä työtä, johon tämä opinnäytetyö pyrkii osaltaan vastaamaan. Opinnäytetyön perusteella syntyvä toiminnallinen tuotos talletetaan julkisesti saataville, jolloin se on vapaasti hyödynnettävissä turvallisuusluokiteltujen tietojen suojaamiseksi suunniteltavien menetelmien mallintamiseksi. Koska viranomaisten julkaisemia turvallisuuskriteeristöjä ei ollut mallinnuksen valmistumiseen mennessä vapaasti saatavilla, toiminnallisen osuuden pyrkimyksenä oli myös edistää mallinnusten julkaisuja olemalla ensimmäinen vapaasti saatavilla oleva ArchiMate mallinnus aiheesta.

Yksinkertaisimmillaan Katakrin mallinnukseen olisi riittänyt kriteerien ja vaatimusten elementtien luominen ja liittäminen valituilla suhdeliittimillä, mutta tässä opinnäytetyössä päätettiin sisällyttää jokaiseen kriteerin elementtiin Katakrin sisältö mahdollisimman täydellisenä, jolloin itse mallia voidaan hyödyntää informaation lähteenä.

Vaikka ArchiMate standardissa on rajallinen määrä käytettäviä elementtejä, voi mallintaminen olla aloittelijalle ja joskus myös pidemmän aikaa mallintaneelle välillä haastavaa. ArchiMate standardista, mallinnuksesta ja työkalujen käytöstä on julkaistu useita julkaisuja, joita voidaan hyödyntää mallinnusten aikana.

Opinnäytetyön tuotoksena syntyneestä mallinnuksesta muodostui lopulta hyvin laaja ja sen numeeriset tiedot esitetään taulukossa 6. Mallinnuksen 276 elementistä valtaosa muodostui kriteereistä vaatimuksineen ja 332 suhdeliittimistä valtaosa muodostui kriteerien ja vaatimusten välisistä suhteista. Mallinnukseen muodostui yhteensä 109 näkymää, jotka jaoteltiin osa-alueiden mukaisiin kansioihin, joita muodostui 29. Näkymien määrää kasvatti mallinnustapa, jossa jokaiselle kriteerille luotiin oma näkymä, jotta kriteereitä voidaan käsitellä yksi kerrallaan ja samalla rajata näkymissä olevien visuaalisten elementtien määrää. Taulukon objektit ja yhteydet ovat mallinnuksen näkymissä esiintyviä elementtejä ja suhdeliittimiä, joita käytetään näkökulman mukaan tarvittaessa useampaan kertaan.

Taulukko 6. Opinnäytetyön mallinnuksen numeeriset tiedot

Elementit	276
Suhdeliittimet	332
Kansiot	29
Näkymät	109
Objektit	1420
Yhteydet	1324

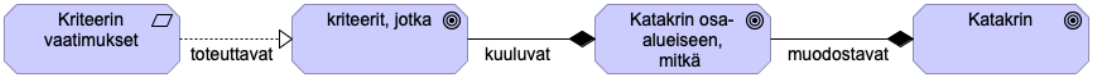
Mallinnuksen laajuuden takia sen sisältöä ei voitu täydellisesti liittää tähän dokumenttiin, eli opinnäytetyön raporttiin.

Katakrin kriteerit esitetään opinnäytetyön raportissa osa-alueittain taulukkomuodossa ja jokaisesta osa-alueesta esitetään mallinnuksen tiivistetty näkymä. Katakrin kriteerien vaatimukset on sisällytetty liitteenä oleviin Katakrin osa-alueiden mallinnusnäkymiin. Normaalitilanteissa mallinnuksissa ei suositella käytettävän liitteen kaltaisia laajoja näkymiä, vaan pyrkimys on luettavuuden ja käytettävyyden kannalta vähentää elementtien, elementtityyppien ja suhteiden määrää, mikä tukee näkymien taloudellisuuden ja mallien visuaalisen kompleksisuuden rajoittamisen ohjeistuksia (Lankhorst et al 2013, 121). Koska näkymiä muodostui mallinnuksessa kokonaisuudessaan yli 100 kappaletta, niitä kaikkia ei liitetty itse raporttiin, vaan lopullinen työ julkaistiin ArchiMate -mallinnusformaateissa GitHub -verkkopalvelussa, josta se on vapaasti saatavilla.

5.1 Katakrin mallinnustapa

Katakrissa esitetyt kriteerit on tässä opinnäytetyössä mallinnettu käyttäen ArchiMaten tavoite (Goal) -elementtiä ja motivaatio (Motivation) näkökulmaa. Myös itse Katakri ja sen osa-alueet on mallinnettu käyttäen samaa tavoite -elementtiä. Kriteereissä esitetyt vaatimukset on mallinnettu käyttämällä vaatimus (Requirement) -elementtiä. Katakrin kriteereissä esitetyt vaatimukset on liitetty toteutus (Realization) suhteella kriteeriin, jotka on liitetty osa-alueeseen koostumus -suhteella ja osa-alue liitetty koostumus -suhteella Katakriin. Kokonaisuudesta on muodostunut ketju, jonka avulla jokainen yksittäinen vaatimus voidaan linkittää Katakriin itseensä.

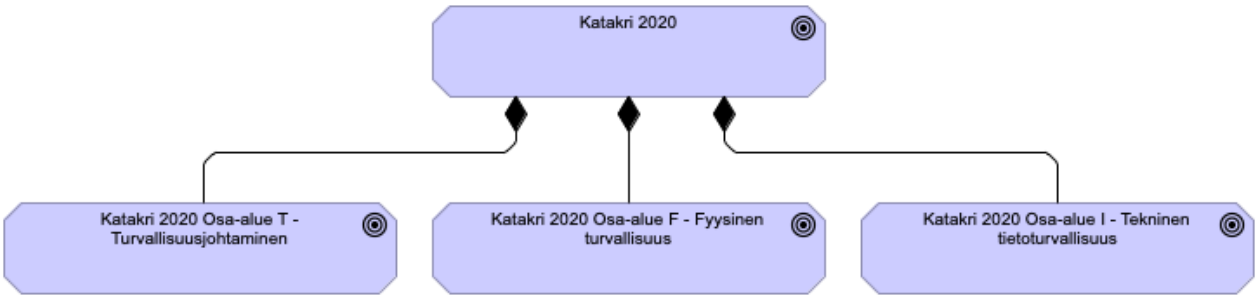
Koska ArchiMaten elementeillä on merkitys, käytetty mallinnustapa on esitettävissä yksinkertaisemmin kielimallia mukailevalla lauseella; Katakrin vaatimukset toteuttavat kriteerit, jotka kuuluvat Katakrin osa-alueisiin, mitkä muodostavat Katakrin. Lause on esitetty kuvassa 13.



Kuva 13. Katakrin mallinnustapa ArchiMate -kielen mukaisesti.

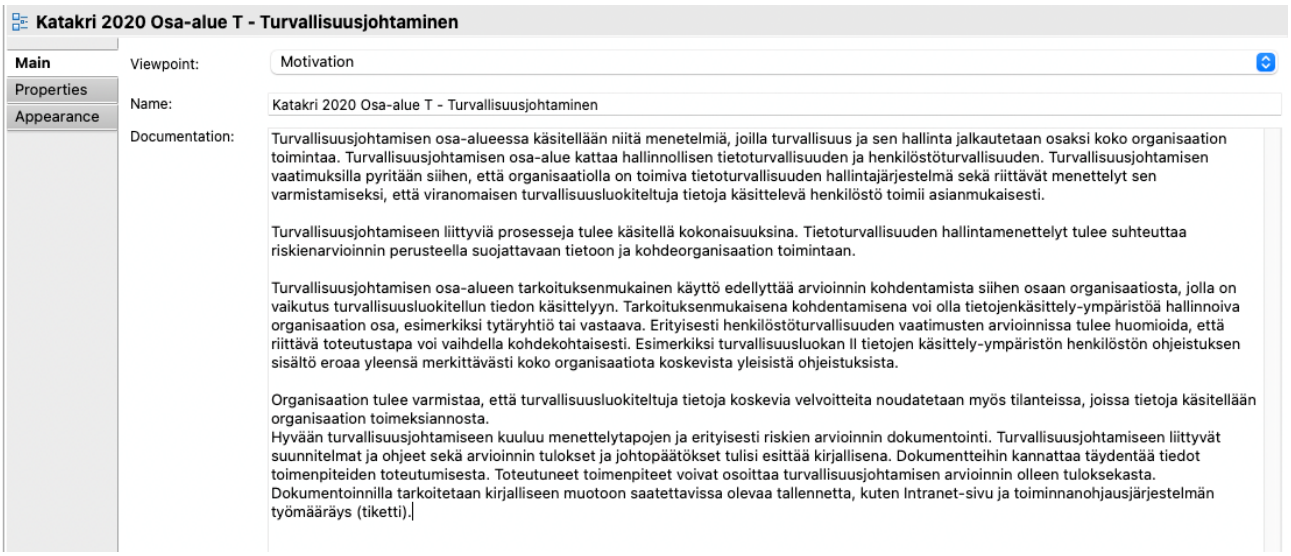
5.2 Osa-alueiden mallintaminen

Katakrin rakenne muodosti mallille rungon, mikä jakaantui osa-alueiden mukaan kolmeen eri alueeseen. Aloitin mallinnuksen luomalla ensin Katakri 2020 tavoitteen, jonka jälkeen loin turvallisuusjohtamisen, fyysisen turvallisuuden ja teknisen tietoturvallisuuden osa-alueet myös tavoite -elementeillä. Yhdistin osa-alueiden tavoite -elementit ArchiMaten rakenteellisella koostumus -suhteen yhteystyypillä. Koostumussuhde edustaa sitä, että elementti koostuu yhdestä tai useammasta muusta käsitteestä ja tässä yhteydessä osa-alue koostuu aina sen alla olevista kriteereistä. Osa-alueiden mallinnus suhteessa Katakriin on esitetty kuvassa 14.



Kuva 14 Katakri osa-alueet mallinnettuna ArchiMate Tavoite -elementeillä

Osa-alueen tavoite -elementtiin sisällytettiin kunkin osa-alueen Katakrissa esitetty tekstisisältö, jolloin elementti toimii samalla tiedon lähteenä.



Kuva 15. Turvallisuusjohtaminen osa-alueen tavoite -elementin sisältö

5.3 Kriteerin mallintaminen

Jokaisesta Katakrin kriteeristä luotiin oma näkymä, joka sisälsi itse kriteerin mallinnettuna tavoite -elementillä ja kriteeriin liitetyt vaatimukset käyttäen vaatimus -elementtejä. Oma näkymä jokaiselle kriteerille yksinkertaisti kriteerien käsittelyä. Käytäntö tavoite -elementin käyttämisestä kriteerin mallintamiseen muodostui kirjallisuuskatsauksen havaintojen perusteella. Katakrin sisällön liittämistä osaksi mallia jatkettiin sisällyttämällä Katakrin kriteereissä kuvattu tekstisisältö kriteerien tavoite -elementtiin. Kuvassa 16 esitetään Katakrissa esitetty tekstisisältö T-01 vaatimukselle ja kuvassa 17 esitetään, miten sama sisältö voidaan esittää hyödyntäen ArchiMaten dokumentaatio -ominaisuutta.

T-01 – JOHDON TUKI, OHJAUS JA VASTUU – TURVALLISUUSPERIAATTEET

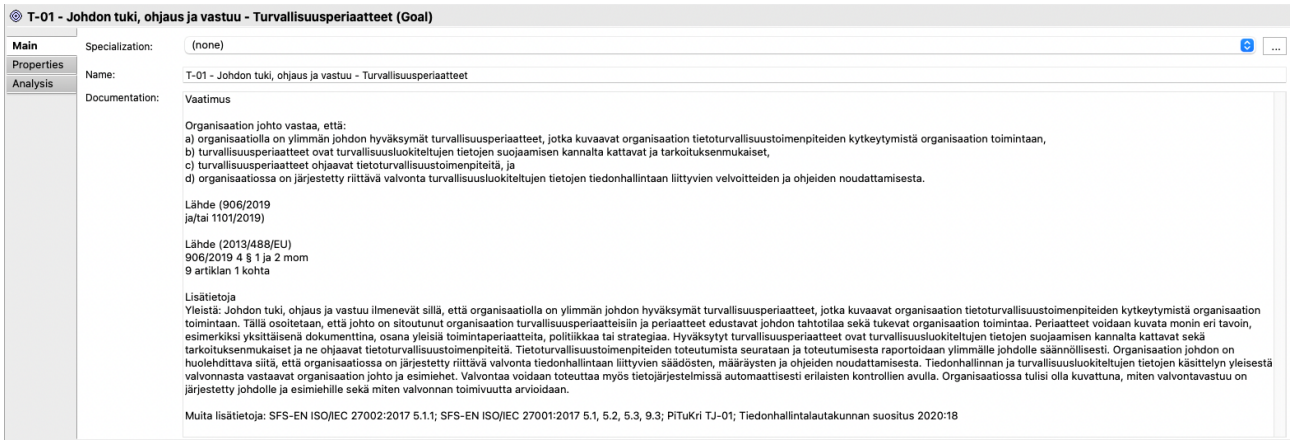
Vaatimus	§ Lähde (906/2019 ja/tai 1101/2019)	§ Lähde (2013/488/EU)
Organisaation johto vastaa, että: a) organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan, b) turvallisuusperiaatteet ovat turvallisuusluokiteltujen tietojen suojaamisen kannalta kattavat ja tarkoituksenmukaiset, c) turvallisuusperiaatteet ohjaavat tietoturvallisuustoimenpiteitä, ja d) organisaatiossa on järjestetty riittävä valvonta turvallisuusluokiteltujen tietojen tiedonhallintaan liittyvien velvoitteiden ja ohjeiden noudattamisesta.	906/2019 4 § 1 ja 2 mom	9 artiklan 1 kohta

Lisätietoja

Yleistä: Johdon tuki, ohjaus ja vastuu ilmenevät sillä, että organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan. Tällä osoitetaan, että johto on sitoutunut organisaation turvallisuusperiaatteisiin ja periaatteet edustavat johdon tahtotilaa sekä tukevat organisaation toimintaa. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina, osana yleisiä toimintaperiaatteita, politiikkaa tai strategiaa. Hyväksytyt turvallisuusperiaatteet ovat turvallisuusluokiteltujen tietojen suojaamisen kannalta kattavat sekä tarkoituksenmukaiset ja ne ohjaavat tietoturvallisuustoimenpiteitä. Tietoturvallisuustoimenpiteiden toteutumista seurataan ja toteutumisesta raportoidaan ylimmälle johdolle säännöllisesti. Organisaation johdon on huolehdittava siitä, että organisaatiossa on järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta. Tiedonhallinnan ja turvallisuusluokiteltujen tietojen käsittelyn yleisestä valvonnasta vastaavat organisaation johto ja esimiehet. Valvontaa voidaan toteuttaa myös tietojärjestelmissä automaattisesti erilaisten kontrollien avulla. Organisaatiossa tulisi olla kuvattuna, miten valvontavastuu on järjestetty johdolle ja esimiehille sekä miten valvonnan toimivuutta arvioidaan.

Muita lisätietoja: SFS-EN ISO/IEC 27002:2017 5.1.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01; Tiedonhallintalautakunnan suositus 2020:18

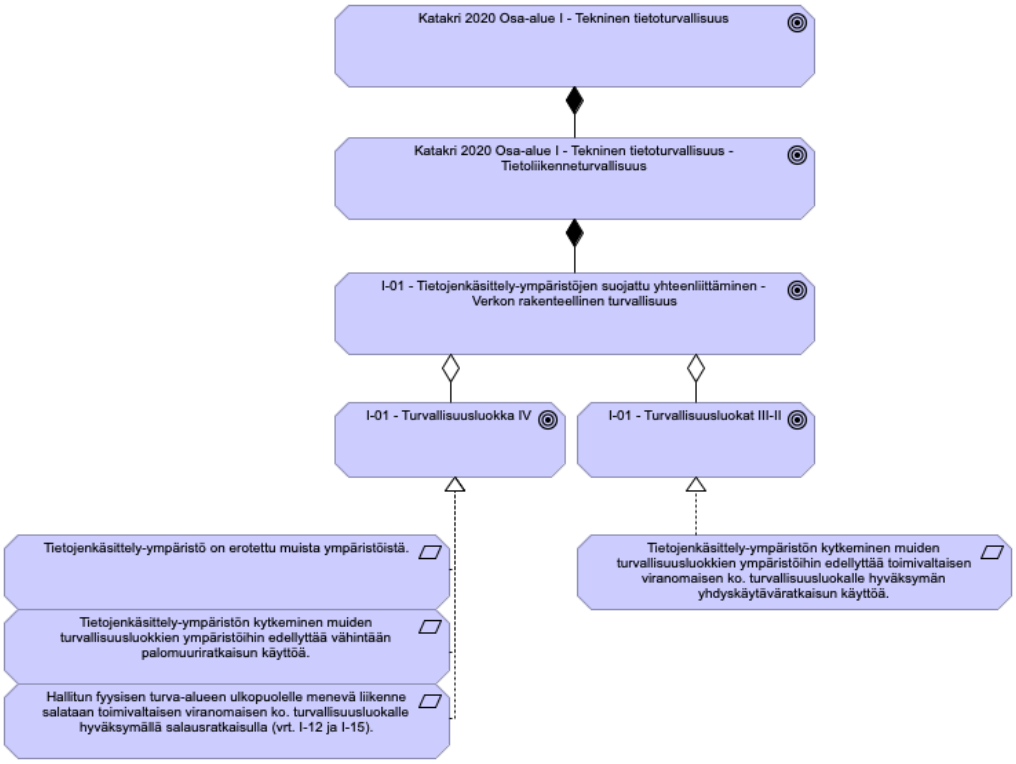
Kuva 16. Katakrin kriteeri T-01 (Kansallinen turvallisuusviranomainen 2020, 9)



Kuva 17. Katakrin tekstisisältö T-01 kriteerille

Sisällyttämällä kriteeristön dokumentaatio mukaan jokaiseen käytettyyn elementtiin, voidaan jatkomallinnuksissa hyödyntää elementtien tietosisältöä ilman, että mallintajan täytyy erikseen tutkia Katakrin dokumentaatiota.

Yksittäisen kriteerin mallinnus vaatimuksineen esitetään kuvassa 18. I-01 kriteerissä erilaisia vaatimuksia kohdistuu eri turvallisuusluokkiin, jolloin esimerkkimallinnukseen on lisätty tavoite -elementti kriteerin ja vaatimusten väliin kuvaamaan erot turvallisuusluokkien välillä. Vaihtoehtoisesti vaatimukset voidaan liittää toteutus -suhteella suoraan itse kriteeriin.



Kuva 18. Verkon rakenteellisen turvallisuuden kriteerin (I-01) mallinnusesimerkki

5.4 Katakri 2020 Osa-alue T – Turvallisuusjohtamisen mallintaminen ArchiMatella

Turvallisuusjohtamisen osa-alue jakaantuu hallinnolliseen tietoturvallisuuteen ja henkilöstöturvallisuuteen.

Hallinnollinen tietoturvallisuus sisältää kahdeksan kriteeriä, jotka on listattu taulukossa 7 ja esitetty mallina kuvassa 19.

Taulukko 7. Hallinnollisen tietoturvallisuuden kriteerit (mukaillen Kansallinen turvallisuusviranomainen 2020, 9–16)

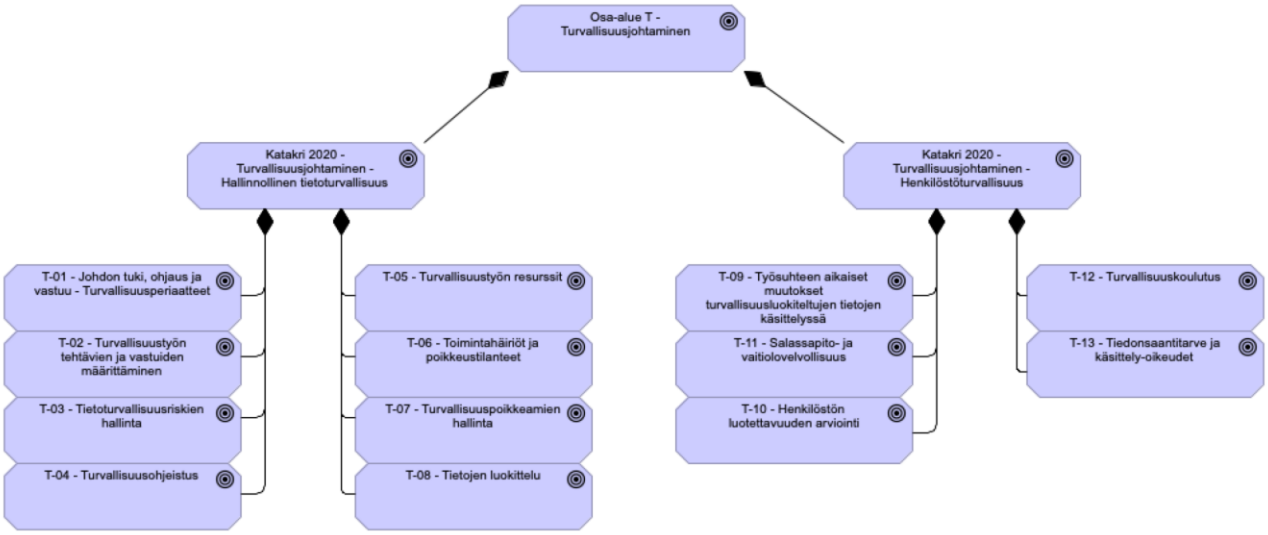
Tunniste	Nimi
T-01	Johdon tuki, ohjaus ja vastuu – turvallisuusperiaatteet
T-02	Turvallisuustyön tehtävien ja vastuiden määrittäminen
T-03	Tietoturvallisuusriskien hallinta
T-04	Turvallisuusohjeistus
T-05	Turvallisuustyön resurssit
T-06	Toimintahäiriöt ja poikkeustilanteet
T-07	Turvallisuuspoikkeamien hallinta
T-08	Tietojen luokittelu

Henkilöstöturvallisuus sisältää viisi kriteeriä, jotka on listattu taulukossa 8 ja esitetty mallina kuvassa 19.

Taulukko 8. Henkilöstöturvallisuuden kriteerit (mukaillen Kansallinen turvallisuusviranomainen 2020, 17–21)

Tunniste	Nimi
T-09	Työsuhteen aikaiset muutokset turvallisuusluokiteltujen tietojen käsittelyssä
T-10	Henkilöstön luotettavuuden arviointi
T-11	Salassapito- ja vaitiolovelvollisuus
T-12	Turvallisuuskoulutus
T-13	Tiedonsaantitarve ja käsittelyoikeudet

Turvallisuusjohtamisen osa-alueen mallintaminen ArchiMatella on esitetty kuvassa 19.



Kuva 19. Katakri 2020 Osa-alue T - Turvallisuusjohtaminen kriteerit mallinnettuna

5.5 Katakri 2020 Osa-alue F - Fyysisen turvallisuuden mallintaminen ArchiMatella

Fyysisen turvallisuuden osa-alue jakaantuu yleisiin, turvallisuusalueiden ja tietoaineistoturvallisuuden vaatimuksiin.

Fyysisen turvallisuuden yleiset vaatimukset sisältää neljä kriteeriä, jotka on listattu taulukossa 9 ja esitetty mallina kuvassa 20.

Taulukko 9. Fyysisen turvallisuuden kriteerit (mukaillen Kansallinen turvallisuusviranomainen 2020, 24–29)

Tunniste	Nimi
F-01	Fyysisten turvatoimien tavoite
F-02	Fyysisten turvatoimien riskien arviointi
F-03	Fyysisten turvatoimien valinta (monitasoinen suojaus)
F-04	Tiedon käsittely ja säilytys

Turvallisuusalueiden kriteerit kattavat kolme aluetta, jotka ovat Hallinnollinen alue (F-05), Turva-alue (F-06) ja Teknisesti suojattu turva-alue (F-07).

Hallinnollinen alue sisältää Hallinnollinen alue -pääkriteerin lisäksi kahdeksan alikriteeriä, jotka on listattu taulukossa 10 ja esitetty mallina kuvassa 20.

Taulukko 10. Hallinnollisen alueen alikriteerit (mukaillen Kansallinen turvallisuusviranomainen 2020, 33–40)

Tunniste	Nimi
F-05.1	Alueen raja ja rakenteet (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet)
F-05.2	Pääsyoikeuksien myöntäminen
F-05.3	Vierailijat
F-05.4	Äänieristys
F-05.5	Tunkeutumisen ilmaisujärjestelmät
F-05.6	Salaa katselun estäminen
F-05.7	Tila- ja laitetarkastukset (ainoastaan tl ii / eu-s)
F-05.8	Tiedon käsittely ja säilyttäminen

Turva-alue sisältää Turva-alue-pääkriteerin lisäksi kymmenen alikriteeriä, jotka on listattu taulukossa 11 ja esitetty mallina kuvassa 20.

Taulukko 11. Turva-alueen alikriteerit (mukaillen Kansallinen turvallisuusviranomainen 2020, 42–55)

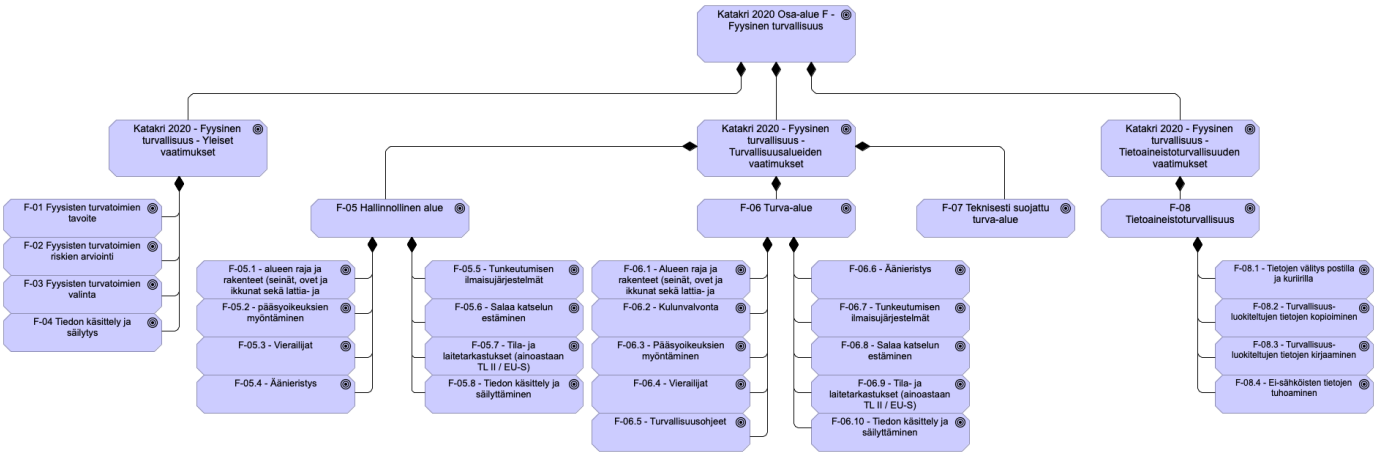
Tunniste	Nimi
F-06.1	Alueen raja ja rakenteet (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet)
F-06.2	Kulunvalvonta
F-06.3	Pääsyoikeuksien myöntäminen
F-06.4	Vierailijat
F-06.5	Turvallisuusohjeet
F-06.6	Äänieristys
F-06.7	Tunkeutumisen ilmaisujärjestelmät
F-06.8	Salaa katselun estäminen
F-06.9	Tila- ja laitetarkastukset (ainoastaan tl ii / eu-s)
F-06.10	Tiedon käsittely ja säilyttäminen

Tietoaineistoturvallisuus sisältää Tietoaineistoturvallisuus -pääkriteerin lisäksi neljä alikriteeriä, jotka on listattu taulukossa 12 ja esitetty mallina kuvassa 20.

Taulukko 12. Tietoaineistoturvallisuuden alikriteerit (mukaillen Kansallinen turvallisuusviranomainen 2020, 58–62)

Tunniste	Nimi
F-08.1	Tietojen välitys postilla ja kuriirilla
F-08.2	Turvallisuusluokiteltujen tietojen kopioiminen
F-08.3	Turvallisuusluokiteltujen tietojen kirjaaminen
F-08.4	Ei-sähköisten tietojen tuhoaminen

Fyysisen turvallisuuden mallintaminen ArchiMatella on esitetty kuvassa 20.



Kuva 20. Katakri 2020 Osa-alue F - Fyysinen turvallisuus mallinnettuna

5.6 Katakri 2020 Osa-alue I - Teknisen tietoturvallisuuden mallintaminen ArchiMatella

Teknisen tietoturvallisuuden osa-alue jakaantuu tietoliikenneturvallisuuden, tietojärjestelmäturvallisuuden ja käyttöturvallisuuden vaatimuksiin.

Tietoliikenneturvallisuus sisältää viisi kriteeriä, jotka on listattu taulukossa 13 ja esitetty mallina kuvassa 21.

Taulukko 13. Tietoliikenneturvallisuuden kriteerit (mukaillen Kansallinen turvallisuusviranomainen 2020, 67–74)

Tunniste	Nimi
I-01	Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen - verkon rakenteellinen turvallisuus
I-02	Vähimpien oikeuksien periaate - tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt ko. turvallisuusluokan sisällä
I-03	Tietojenkäsittely-ympäristön turvallisuus koko elinkaaren ajan - suodatus- ja valvontajärjestelmien hallinnointi
I-04	Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen - hallintayhteydet
I-05	Suojattavien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella - langaton tiedonsiirto

Tietojärjestelmäturvallisuus sisältää yhdeksän kriteeriä, jotka on listattu taulukossa 14 ja esitetty mallina kuvassa 21.

Taulukko 14. Tietojärjestelmäturvallisuuden kriteerit (mukaillen Kansallinen turvallisuusviranomainen 2020, 75–93)

Tunniste	Nimi
I-06	Vähimpien oikeuksien periaate – pääsyoikeuksien hallinnointi
I-07	Monitasoinen suojaaminen - tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuusalueen sisällä
I-08	Vähimmäistoimintojen ja vähimpien oikeuksien periaate - järjestelmäkovennus
I-09	Monitasoinen suojaaminen - haittaohjelmasuojaus
I-10	Monitasoinen suojaaminen - turvallisuuteen liittyvien tapahtumien jäljitettävyys
I-11	Monitasoinen suojaaminen - poikkeamien havainnointikyky ja toipuminen
I-12	Tietoturvallisuustuotteiden arviointi ja hyväksyntä - salausratkaisut
I-13	Monitasoinen suojaaminen koko elinkaaren ajan - ohjelmistojen suojaaminen verkkohyökkäyksiltä
I-14	Monitasoinen suojaaminen - hajasäteily (tempest) ja elektroninen tiedustelu

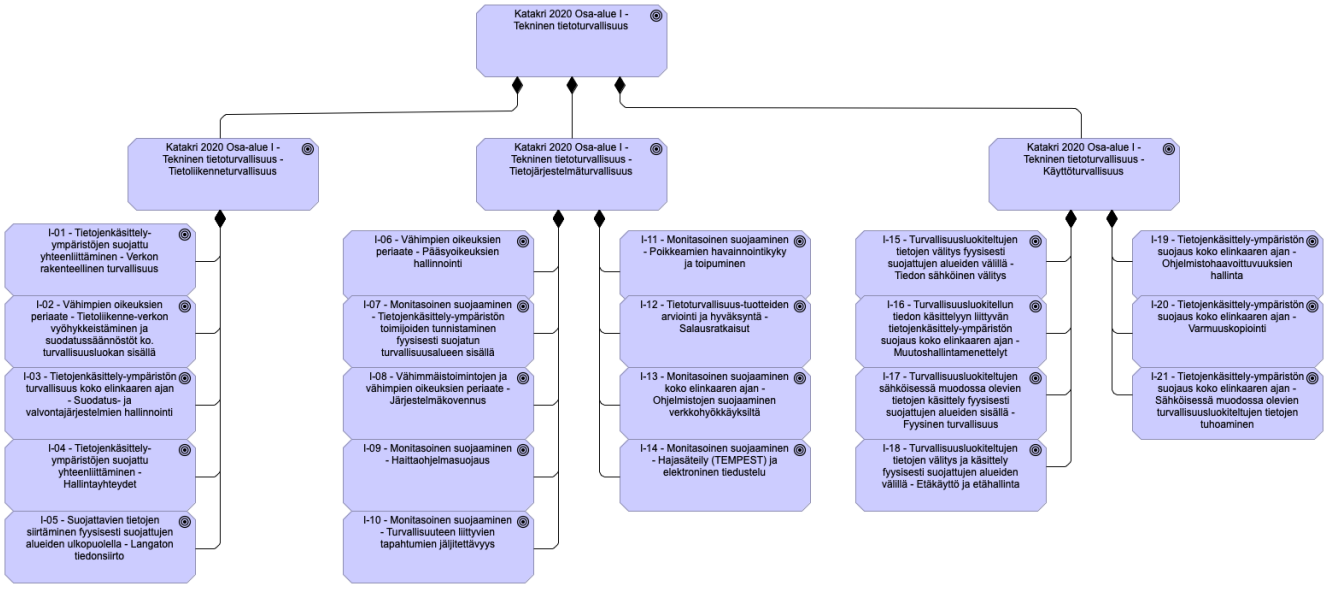
Käyttöturvallisuus sisältää seitsemän kriteeriä, jotka on listattu taulukossa 15 ja esitetty mallina kuvassa 21.

Taulukko 15. Käyttöturvallisuuden kriteerit (mukaillen Kansallinen turvallisuusviranomainen 2020, 94–106)

Tunniste	Nimi
I-15	Turvallisuusluokiteltujen tietojen välitys fyysisesti suojattujen alueiden välillä - tiedon sähköinen välitys
I-16	Turvallisuusluokitellun tiedon käsittelyyn liittyvän tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - muutoshallintamenettelyt
I-17	Turvallisuusluokiteltujen sähköisessä muodossa olevien tietojen käsittely fyysisesti suojattujen alueiden sisällä - fyysinen turvallisuus
I-18	Turvallisuusluokiteltujen tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä - etäkäyttö ja etähallinta
I-19	Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - ohjelmistohaavoittuvuuksien hallinta

I-20	Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - varmuuskopiointi
I-21	Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - sähköisessä muodossa olevien turvallisuus-luokiteltujen tietojen tuhoaminen

Teknisen tietoturvallisuuden mallintaminen ArchiMatella on esitetty kuvassa 21.



Kuva 21. Katakri 2020 Osa-alue I - Tekninen tietoturvallisuus mallinnettuna

5.7 Katakrin toteutusesimerkkien mallintaminen

Organisaatiot voivat hyödyntää ArchiMatella luotua Katakrin mallinnusta itsearvioinnissa omasta turvallisuudestaan osana yritysturvallisuusselvitystä.

Mallin avulla yritys voi arvioida järjestelmiin kohdistettavia suojauksia, joilla voidaan saavuttaa Katakrissa esitetyt hyväksyttävät suojaustasot ja siten hyödyntää mallinnusta osana tietojärjestelmien turvallisuuden arviointiprosessia.

Varsinaisen Katakrin kriteeristöjen ja vaatimusten mallinnuksen lisäksi malliin liitettiin mukaan toteutusesimerkkien mallinnuksia Katakrissa esitettyjen vähimmäisvaatimusten toteuttamiseksi.

Toteutusesimerkit eivät ole täydellisiä, vaan toteutusesimerkeissä esitettyjen menetelmien Archimate -mallinnushahmotelmia, eikä niitä tule siten hyödyntää suoraan osana varsinaisia Katakrin vaatimusten realisointimallinnuksia. Kahteen ensimmäiseen mallinnusesimerkkiin on liitetty lisäksi lyhyt kuvaus mallinnuksen sisällöstä.

Mallinnusesimerkki kriteerille I-01

Verkon rakenteellisen turvallisuuden (I-01 Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen – verkon rakenteellinen turvallisuus) kriteerin vaatimusten realisoinnit voi mallintaa ArchiMatella seuraavalla tavalla.

Esimerkin kriteerissä on eri turvallisuusluokille kohdistuvia vaatimuksia, joista kolme ensimmäistä kohdistuu kaikkiin esimerkin turvallisuusluokkiin.

Kaikkiin esimerkin turvallisuusluokkiin kohdistuvat vaatimukset:

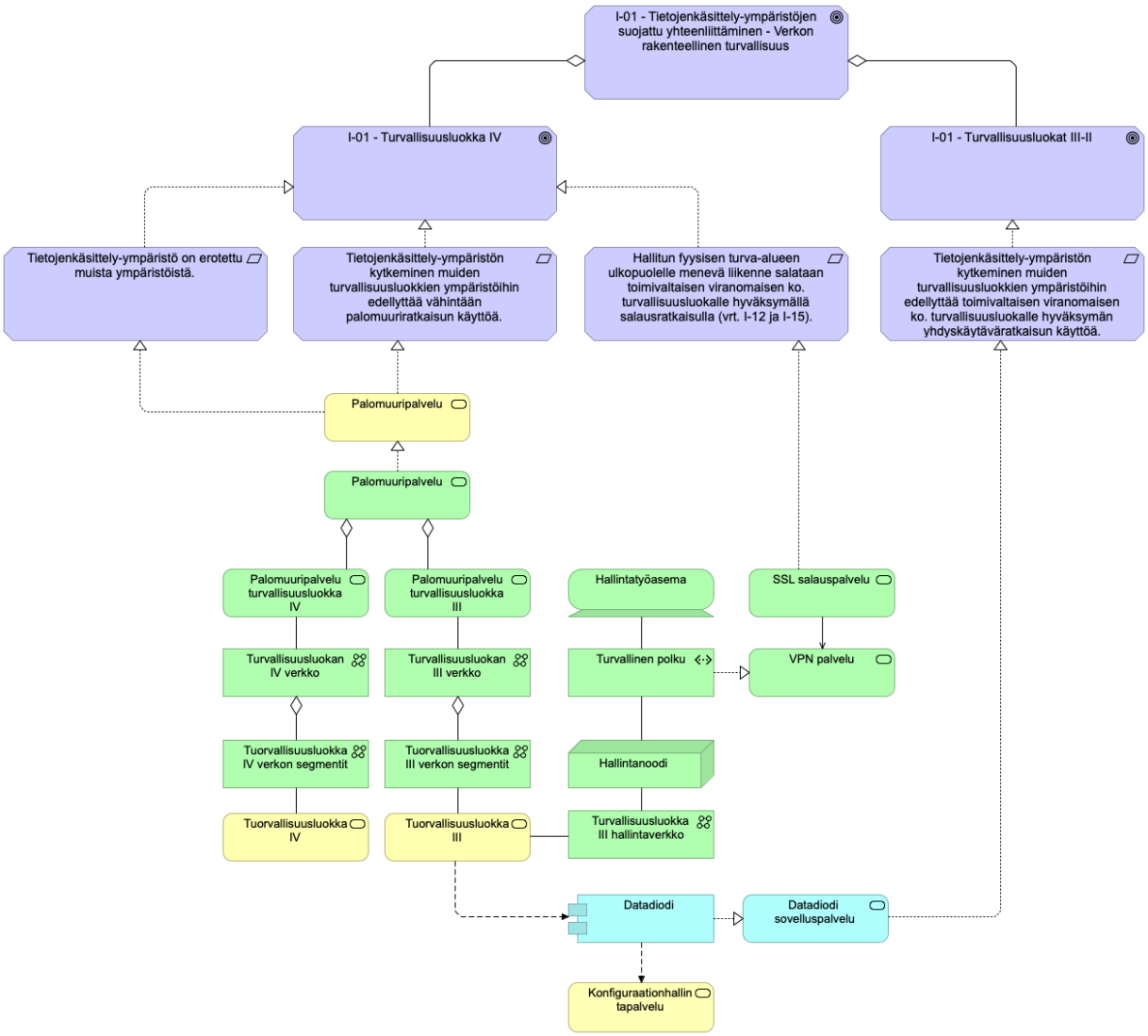
Ensimmäinen, tietojenkäsittely-ympäristön erottaminen muista ympäristöistä -vaatimus realisoidaan tässä esimerkissä palomuuripalvelulla, joka erottaa turvallisuusluokan tietojenkäsittely-ympäristön muista ympäristöistä.

Toisessa vaatimuksessa edellytetään vähintään palomuuriratkaisun käyttöä tietojenkäsittely-ympäristön kytkemiseksi muiden turvallisuusluokkien ympäristöihin, jolloin ensimmäisen vaatimuksen palomuuripalvelulla realisoidaan tässä esimerkissä myös toinen vaatimus.

Kolmas vaatimus edellyttää hallitun fyysisen turva-alueen ulkopuolelle menevän liikenteen salaamista toimivaltaisen viranomaisen hyväksymällä salausratkaisulla. Vaatimus toteutetaan tässä esimerkissä SSL-salauspalvelulla.

Turvallisuusluokkiin III-II kohdistuva vaatimus:

Neljäs vaatimus kohdistuu turvallisuusluokkiin III-II ja edellyttää tietojenkäsittely-ympäristön kytkemistä muiden turvallisuusluokkien ympäristöihin toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä yhdyskäytäväratkaisulla. Vaatimus realisoidaan tässä esimerkissä käyttämällä yksisuuntaisen liikenteen sallivaa datadiodia. Verkon rakenteellisen turvallisuuden kriteerin (I-01) mallinnusesimerkki esitetään kuvassa 22.

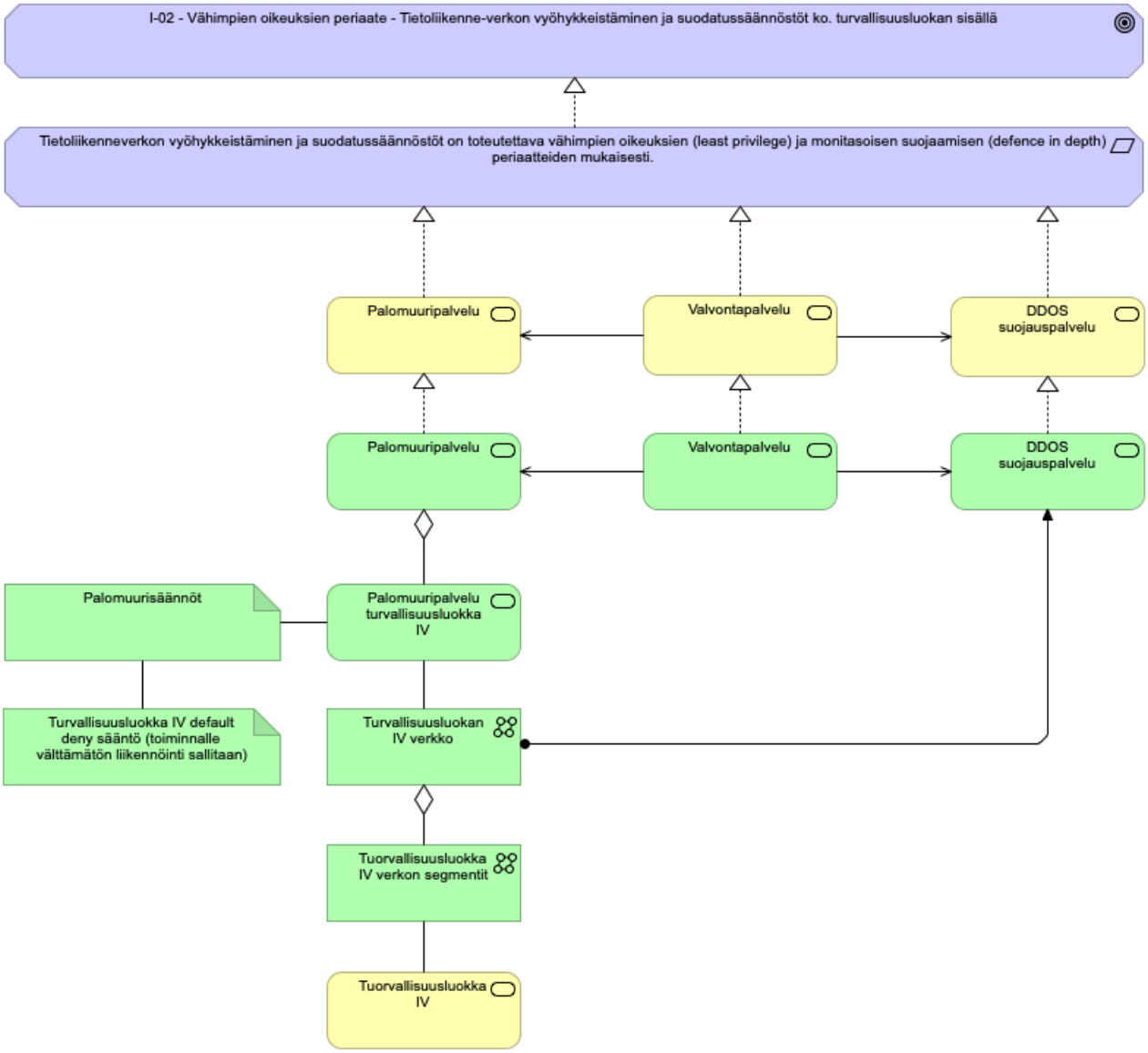


Kuva 22. Verkon rakenteellisen turvallisuuden kriteerin (I-01) vaatimusten realisoinnin mallinnusesimerkki

Mallinnusesimerkki kriteerille I-02

Vähimpien oikeuksien periaate kriteerissä (I-02) esitettyjen vaatimusten realisoinnin voi mallintaa ArchiMatella oheisella tavalla.

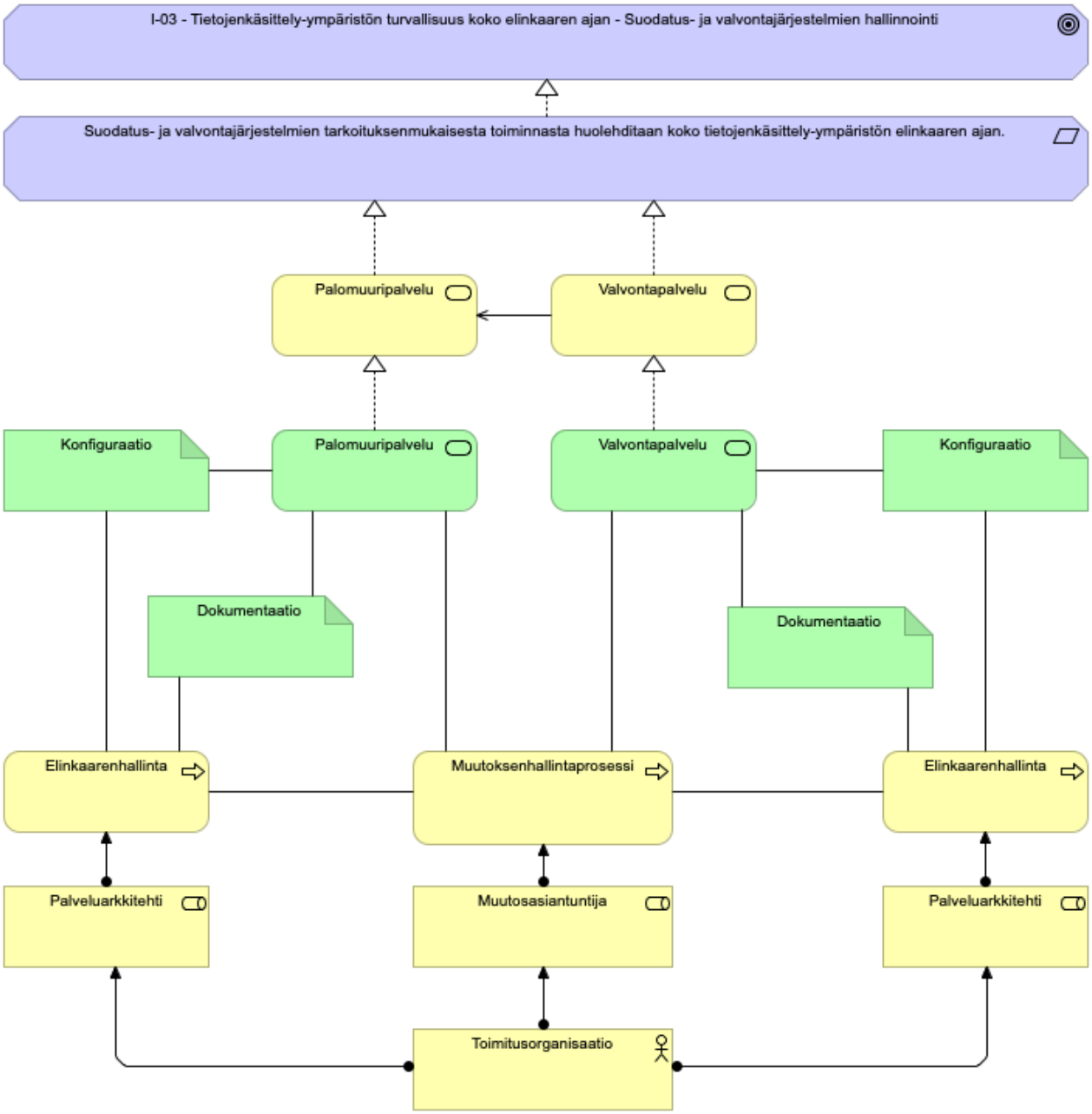
Tässä realisointihahmotelmassa tietoliikenneverkko jaetaan turvallisuusluokan sisällä erillisiin vyöhykkeisiin ja segmentteihin hyödyntämällä palomuuripalvelua. Palomuuripalvelun avulla turvallisuusluokan verkko jaetaan vyöhykkeisiin ja segmentteihin. Verkko-alueiden välistä liikennettä valvotaan ja rajoitetaan default-deny-palomuurisäännöillä, jolloin vain erikseen hyväksytty, toiminnalle välttämätön liikennöinti sallitaan. Tietojenkäsittely-ympäristössä varaudutaan verkkohyökkäyksiin DDOS suojauspalvelulla. Vähimpien oikeuksien kriteerin (I-02) mallinnusesimerkki esitetään kuvassa 23.



Kuva 23. Vähimpien oikeuksien kriteerin (I-02) vaatimuksen realisoinnin mallinnusesimerkki

Mallinnusesimerkki kriteerille I-03

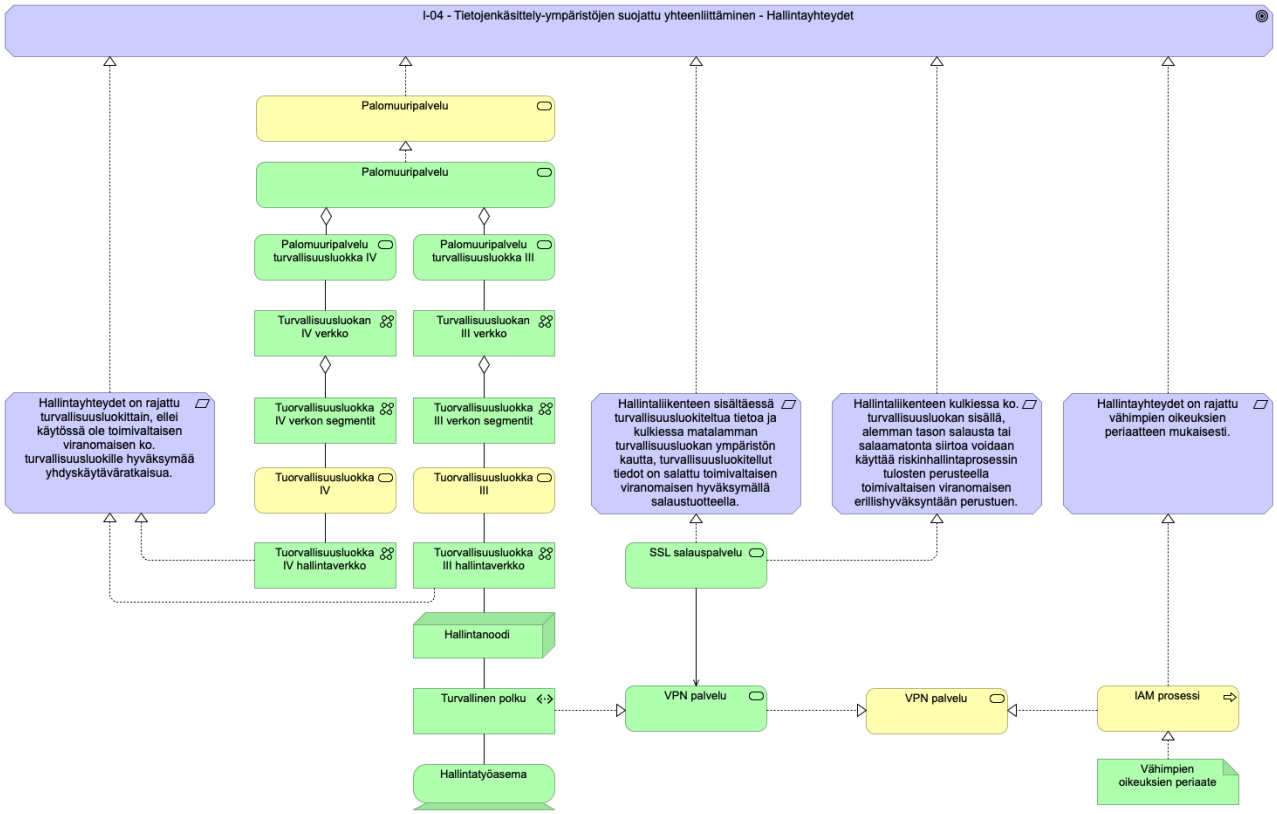
Tietojenkäsittely-ympäristön turvallisuus koko elinkaaren ajan -kriteerin (I-03) vaatimusten realisoinnin voi mallintaa ArchiMatella kuvan 24 mukaisella tavalla.



Kuva 24. Tietojenkäsittely-ympäristön turvallisuus koko elinkaaren ajan -kriteerin (I-03) vaatimuksen realisoinnin mallinnusesimerkki ArchiMatella

Mallinnusesimerkki kriteerille I-04

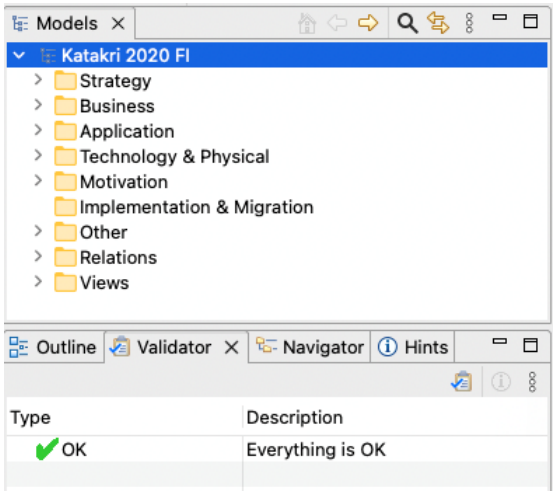
Tietojenkäsittely-ympäristöjen suojatun yhteenliittämisen kriteerin (I-04) vaatimusten realisoinnit voidaan mallintaa ArchiMatella kuvan 25 mukaisella tavalla.



Kuva 25. Tietojenkäsittely-ympäristöjen suojatun yhteenliittämisen kriteerin (I-04) vaatimusten realisointien mallintaminen ArchiMatella.

5.8 Mallin tarkastaminen

Toiminnallisen työn edetessä mallille tehtiin säännöllisesti tarkastuksia Archi -työkalun validaattori toiminnallisuudella, joka tarkasti mallin ArchiMate määritysten perusteella. Validaattori voi neuvoa ja varoittaa mallin eheydestä, kuten käyttämättömistä tai päällekkäisistä elementeistä, virheellisistä suhteista tai tyhjistä näkymistä. Mallinnuksen lopuksi myös valmiille mallille suoritettiin validointi, jonka tulos esitetään kuvassa 26.



Kuva 26. Toiminnallinen työ validoitu ArchiMate määrityksen mukaiseksi

5.9 Toiminnallisen työn julkaisu ja hyödyntäminen

Opinnäytetyön pohjalta syntynyt malli muodostui lopulta niin laajaksi, ettei sitä voitu liittää kokonaisuudessaan suoraan raporttiin. Mallinnuksen yhteensä 109 näkymää voi verrata sivuihin, jolloin näkymien liittäminen raportin liitteeksi olisi kasvattanut raportin kokoa yli sadalla sivulla.

Opinnäytetyön toiminnallisen osuuden valmistuttua mallinnus talletettiin kuvauskannasta Archi -työkalun ja ArchiMate Open Exchange File tiedostomuotoihin ja julkaistiin GitHub -verkkopalvelussa osoitteessa https://github.com/h4nu/Katakri-2020-ArchiMate.

Julkaistu malli voidaan avata suoraan ArchiMate standardia tukevilla ohjelmilla, jolloin sitä voidaan hyödyntää konkreettisesti osana riskien ja turvallisuudenhallinnan mallinnuksia. Julkaistuista malleista katakri-2020-fi.archimate -tiedoston voidaan avata Archi -työkalulla, joka on vapaasti ladattavissa ja asennettavissa archimatetool.com sivustolta. Open Exchange File muodossa oleva malli (Katakri 2020 FI.xml) voidaan tuoda (import) toiminnallisuudella mihin tahansa muuhun ArchiMate standardia tukevaan työkaluun.

6 Pohdinta

Opinnäytetyön perusteella voidaan todeta, että ArchiMate-standardi tarjoaa mallinnusrakenteet tehokkaaseen riski- ja turvallisuuskäsitteiden kuvaamiseen ja yhdistämiseen ja siten soveltuu mallintamaan Katakrissa esitetyt turvallisuuskriteerit ja vaatimukset tarkasteltavan kohteen tietoturvallisuuden tilan arvioimiseksi. Katakrin toteutusesimerkkien mallinnuksien perusteella ArchiMate soveltuu mallintamaan menetelmiä, joilla on mahdollista pienentää tarkasteltavan ympäristön turvallisuusluokiteltuun tietoon kohdistuvia riskejä hyväksyttävälle tasolle. ArchiMate-kielen attribuuttimekanismi tarjoaa mallintajille lisäksi välineet määritellä elementeille lisätietoja, joita voidaan käyttää arkkitehtuurien analysointiin ja riskien ja turvallisuusongelmien vaikutuksen määrittämiseen.

Organisaatiot voivat hyödyntää ArchiMatella luotua mallinnusta itsearvioinnissa omasta turvallisuustasostaan. Valmiin mallin kriteerit ja niissä esitetyt vaatimukset voidaan kohdistaa turvallisuusluokiteltuja tietoja sisältäviin järjestelmiin ja analysoida, miten organisaation hallintakeinot täyttävät kriteereissä esitetyt vähimmäisvaatimukset.

Verrattuna Katakrista Microsoft Excel taulukkolaskentaohjelman tiedostomuodossa julkaistuun arviointityökaluun, visuaalisen ArchiMate -mallin avulla vaatimuksia voidaan kohdistaa tarkasteltavaan kohteeseen ja analysoida konkreettisesti, miten riskejä voidaan pienentää. Mallinnuksen elementeillä ja suhdeliittimillä on määritetty merkitys, jolloin mallinnusten avulla pystytään konkreettisemmin arvioimaan suojausten toteutus verrattuna sanallisiin selitekenttiin taulukkolaskentatiedostossa tai jossain muussa, tekstipohjaisessa arviointilomakkeessa. Mallinnuksen etuna on myös kertaalleen mallinnettujen kriteerien elementtien liitettävyys useampaan tutkittavaan kohteeseen, toisin kuin erillisiin dokumentteihin perustuvassa arvioinneissa, joissa jokaiseen arviointiin tai arviointikohteeseen tulee usein luoda uusi dokumentti.

Katakrin mallinnus osoitti, että laajojen kriteeristöjen mallintaminen voi olla hyvin työlästä, vaikka itse kriteerien mallintaminen on kohtalaisen suoraviivainen toimenpide. Kriteerien alkuperäisen sisällön siirtäminen elementtien dokumentaatioon kasvatti mallinnukseen kulunutta aikaa. Aluksi mallinnusta tehtiin suoraan lähdemateriaalista, mikä osoittautui virheeksi, koska tietojen siirtäminen Katakrista suoraan malliin oli lähderakenteen vuoksi hidasta. Lähdemateriaalissa kriteerien tiedot oli jaettu vähintään kymmeneen eri kenttään, joissa oli hyvin erilaisia muotoiluja. Tiedot jouduttiin lopulta siirtämään yksi kenttä kerrallaan tekstinkäsittelyohjelmaan, josta ne siirrettiin yhteen ArchiMaten dokumentaatio -kenttään. Ylimääräinen työvaihe tuntui aluksi turhauttavalta, mutta osoittautui lopulta oikeaksi valinnaksi ja muodostui jatkossa normaaliksi kriteerien mallinnusten työmenetelmäksi. Kriteerien ja standardien vertailu paljasti erilaisia lähestymistapoja vaatimuksissa esitettyjen toteutusesimerkkien dokumentoinnin suhteen. Katakrissa ja Julkrissa toteutusesimerkit oli kuvattu kriteerien yhteyteen, kun taas ISO/IEC 27001:ssä esitettyjen vaatimusten hallintakeinojen

toteutustapojen tarkempi kuvaus on sisällytetty erilliseen ISO/IEC standardiin 27002 (ISO 2022a, 16; ISO 2022B 19). Mahdollisimman täydellisen dokumentaation sisällyttäminen osaksi mallia vähentää mallinnusten aikaista tarvetta tutkia erillisiä dokumentteja, koska informaatio on saatavilla suoraan mallista itsestään. Lisäksi malliin liitetyn dokumentaation sisältö auttaa lukijaa paremmin ymmärtämään mallinnuksen näkymiä, kuten vaatimuselementtien suhteita.

Valmis malli nopeutti huomattavasti kriteerin ja vaatimusten analysointia ja paljasti toteutusesimerkkien mallinnuksen aikana valmiiden mallien hyödyt ja tarpeellisuuden. Sen sijaan, että vaatimuksia arvioitaisiin erikseen ulkoisista vaatimuslähteistä, esim. Katakrista ja luotaisiin malliin niitä vastaavat elementit, voidaan valmiin mallin kriteerit ja vaatimukset liittää välittömästi osaksi käsiteltävää kokonaisuutta. Kertaalleen mallinnettuja yhteiskäyttöisiä vaatimuksia ja palvelukokonaisuuksia voidaan uusiokäyttää ja liittää tarkastelun kohteisiin, kuten kehitettäviin palveluihin tai niiden osa-alueisiin. Samoin kuin uudelleen käytettävät arkkitehtuuri- ja rakennuskomponentit, standardoidut vaatimusmallit nopeuttavat ja tehostavat organisaation prosesseja.

Tässä opinnäytetyössä mallinnettiin kansallinen turvallisuusauditointikriteeristö Katakri. Samalla periaatteella voi mallintaa myös muita viranomaisten julkaisemia kriteeristöjä, kuten Julkisen hallinnon tietoturvallisuuden arviointikriteeristön (Julkri) ja Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri). Suomalaisten viranomaisten julkaisemissa tietoturvaan liittyvissä Kriteeristöissä on pääosin samankaltainen esitystapa, jossa ensin kuvataan itse kriteeri ja sen jälkeen kriteereihin liittyvät vaatimukset ja lisätiedot. Viranomaisten kriteeristöjen vertailujen yhteydessä tuli ilmi, että niissä viitataan usein eroavilla kriteereillä toisiinsa ristiin, jolloin kriteerien erot saattavat muodostaa haasteita yhtenäiseen ja siten tehokkaaseen riskien ja tietoturvallisuuden hallintaan. Eroavaisuuksien pohjalta on suositeltavaa, että viranomaiset yhtenäistävät kriteeristöjään ja tiettyyn kriteeriin ja siinä esitettyihin vaatimuksiin viitataan mahdollisimman samankaltaisesti.

Koska Katakrista ei ole saatavilla valmista mallinnusta, joutuu jokainen organisaatio luomaan itse mallinsa, mikä aiheuttaa huomattavasti päällekkäistä työtä. Päällekkäisen työn kertaantuu myös muiden viranomaisten julkaisemien kriteeristöjen kohdalla, koska niistäkään ei ole julkaistu valmiita mallinnuksia (Valtiovarainministeriö 2023; Kyberturvallisuuskeskus 2020).

Valmiiden mallien julkaisemisella olisi huomattava yhteiskunnallinen merkitys. Valmiiden mallien julkaiseminen viranomaisten toimesta vähentäisi huomattavasti organisaatioiden riskien ja tietoturvan hallinnan päällekkäistä työtä. Kriteereissä esitettyjen toteutusesimerkkien sisällyttäminen malleihin tehostaisi myös määräysten ja suositusten käyttöönottoa ja parantaisi riskien ja turvallisuuden hallinnan tasoa myös pienemmissä organisaatioissa.

Valmiit, viranomaisten julkaisemat mallit vähentävät myös virhetulkintojen mahdollisuutta ja yhtenäinen malli parantaa laatua organisaatioiden välillä. Valmiita malleja voidaan lisäksi jakaa eri toimijoiden kesken, mikä osaltaan edesauttaa digitalisaatioon liittyviä hankkeita.

Suomalaisten viranomaisten tulisi ottaa mallia Euroopan komissiosta (Euroopan komissio 2023) ja julkaista kriteeristöjään, kuten Katakri myös ArchiMate formaatissa. Valmiiden ArchiMate -mallien avulla organisaatiot voisivat hyödyntää viranomaisten julkaisemia kriteeristöjä tehokkaammin osana kokonaisarkkitehtuurityötä.

Katakrin mallinnuksen yhteydessä huomattiin, että vaikka ArchiMate soveltuu hyvin mallintamaan erilaisia riskien ja turvallisuudenhallinnan kokonaisuuksia, julkisesti saatavilla olevia malleja ei juurikaan löydy. Saatavilla olevien mallien puute selittynee osaltaan riskien ja turvallisuudenhallinnan vaativuuteen ja taloudellisiin intresseihin, joita halutaan suojella pidättäytymällä julkaisemasta taloudellisesti arvokkaita malleja

Opinnäytetyön mallinnus keskittyi Katakrissa esitettyjen kriteerien ja niiden vaatimusten mallintamiseen ja toteutusesimerkeistä sisällytettiin mallinnukseen vain muutama. Katakrissa esitetyt toteutusesimerkit tarjoavat jatkojalostamismahdollisuuksia esimerkiksi niistä luotavan kattavan esimerkkimallinnuksen muodossa, jonka avulla voidaan konkreettisesti näyttää menettelyt hyväksyttävän suojausten vähimmäistason saavuttamiseksi.

Viranomaisvaatimusten lisäksi ArchiMate soveltuu mallintamaan muita riskien ja turvallisuudenhallinnan julkaisuja, kuten ISO standardeja, mikä konkretisoitui samanaikaisesti opinnäytetyön viimeistelyn aikana, jolloin mallinsin myös ISO 27001 standardin. ISO 27001 standardissa määritellään tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitämiseen ja jatkuvaan parantamiseen koskevat vaatimukset.

Normaalien mallinnusmenetelmien, kuten mallinnustyökaluilla tapahtuvien mallien käsittelyn lisäksi ArchiMate tarjoaa mallinnuskielenä mahdollisuuden käsitellä malleja edistyneemmillä menetelmillä, joissa voidaan hyödyntää automaatiota, koneoppimista ja tekoälyä. Näiden edistyneempien menetelmien mahdollisuudet ovat lähes rajattomat, koska ArchiMaten elementeille, suhteille ja suhdeliittimille on määritetty merkitys ja mallinnuskieli tarjoaa mukauttamismenetelmät konseptien rikastamiseksi joko suoraan tai ulkoisten tietorakenteiden avulla. Edistyneiden menetelmien avulla voidaan mm. kehittää sovelluksia, jotka luovat malleja syötteiden, herätteiden tai ympäristön havaintojen perusteella.

Tekoäly tarjoaa mahdollisuuksia myös mallien parantamiseen ja analysoimiseen. Laajojen mallien läpikäyminen manuaalisesti ihmistyönä on hidasta, mutta suuriakin massoja kyetään nopeasti

analysoimaan koneellisesti. Tekoälyn avulla voidaan laajoistakin kuvauskannoista tunnistaa liiketoiminnan kannalta oleellisia kehityskohteita ja tuoda siten lisäarvoa toiminnalle.

Tekoälyn tuomien jalostetumpien sovelluskohteiden rinnalle ArchiMate tarjoaa myös nopeammin hyödynnettäviä tehostamismenetelmiä, kuten kokonaisarkkitehtuurin tehtävien automatisointia hyödyntämällä työkalujen nykyisiä rajapintoja. Liiketoiminnan näkökulmasta voidaan koneellisesti tarkastaa, onko malleissa toteutettu tietyt vaatimukset tai miten kattavasti jotkin muut elementtien tai ryhmien suhteet on katettu. Älykkäiden mallinnusten hyödyntäminen tehostaa kokonaisarkkitehtuurityötä ja tuo siten lisäarvoa liiketoiminnalle.

Laajaan opinnäytetyöprojektiin ryhtyminen palkitsi lopulta monilla hyödyillä oppimisen ja ammatillisen kehittymisen näkökulmista. Suuren vaatimuskokoelman mallintaminen tehosti mallinnuksiin liittyviä rutiineja ja prosesseja kasvattaen samalla mallinnuskyvykkyyksiä. Vaikka opinnäytetyön sisältö pyrittiin pitämään lähtökohtaisesti tarkasti rajattuna, mallinnuskielen tarkastelun välttämätön laajentaminen riskien ja tietoturvallisuuden osa-alueille edesauttoi osaltaan kokonaisarkkitehtuurikyvykkyyksien kehittämistä.

Lähteet

Beauvoir, P., Sarrodie J-B., 2023. Avoimen lähdekoodin ArchiMate -mallinnustyökalu Archi. Luettavissa: https://www.archimatetool.com/. Luettu: 20.4.2023

Bizzdesign 2023. Enterprise Studio ArchiMate -mallinnustyökalu. Luettavissa: https://bizzdesign.com/. Luettu 18.9.2022

Digi- ja väestötietovirasto s.a. Kokonaisarkkitehtuurityön tuki. Luettavissa: https://dvv.fi/arkkitehtuuri Luettu 30.10.2023

Euroopan komissio 2023. European Interoperability Reference Architecture (EIRA). Luettavissa: https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira Luettu 11.12.2023

ISO 2022a. ISO/IEC 27001:2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. SFS Suomen Standardit ry. Helsinki. Luettu 18.12.2023

ISO 2022b. SFS-EN ISO/IEC 27002:2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. SFS Suomen Standardit ry. Helsinki. Luettu 18.12.2023

ISO 2023. SFS-ISO/IEC/IEEE 42010:2023 Ohjelmistot, järjestelmät ja organisaatio. Arkkitehtuurin kuvaaminen. SFS Suomen Standardit ry. Helsinki. Luettu 15.12.2023

Juhta 2017. JHS 179 Kokonaisarkkitehtuurin suunnittelu ja kehittäminen 2017. Luettavissa: https://dvv.fi/documents/16079645/202143806/JHS179.doc/62b572fa-0a4f-f247-8beb-73c7501be68c?t=1707472969099. Luettu 15.9.2022

Hosiaisluoma, E. 2022a. ArchiMate Cookbook. Luettavissa: https://www.hosiaisluoma.fi/ArchiMate-Cookbook.pdf Luettu 18.9.2022

Hosiaisluoma, E. 2022b. ArchiMate käsikirja. Luettavissa: http://www.hosiaisluoma.fi/ArchiMate-ka%CC%88sikirja.pdf Luettu 18.9.2022

Kansallinen turvallisuusviranomainen. 2020. Katakri 2020, Tietoturvallisuuden auditointityökalu viranomaisille. Luettavissa: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246. Luettu 20.12.2021

Kyberturvallisuuskeskus 2020. Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri). Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri Luettu 15.7.2022

Kyberturvallisuuskeskus 2021. Katakri 2020 -arviointityökalu. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Katakri-2020-arviointityokalu.xlsx Luettu 20.12.2021

Laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906. Luettavissa https://www.finlex.fi/fi/laki/alkup/2019/20190906. Luettu 11.5.2023

Lankhorst, M et al. 2013. Enterprise Architecture at Work Modelling, Communication and Analysis, Third Edition. Springer. Heidelberg. Luettu 18.12.2023

Mayer, M. & Feltus, C. 2017. Evaluation of the Risk and Security Overlay of ArchiMate to model Information System Security Risks. Luxembourg Institute of Science and Technology. Luxemburg. Luettavissa: https://ieeexplore.ieee.org/document/8089840 Luettu 14.9.2023

Sparx Systems 2023. Enterprise Architect ArchiMate -mallinnustyökalu. Luettavissa: https://sparxsystems.com/products/ea/. Luettu 16.10.2023

The Open Group 2019a. How to Model Enterprise Risk Management and Security with the ArchiMate® Language. Luettavissa: https://publications.opengroup.org/w172. Luettu 15.9.2022

The Open Group 2019b. ArchiMate® Model Exchange File Format for the ArchiMate Modeling Language, Version 3.1. Luettavissa: https://publications.opengroup.org/c19c Luettu 15.9.2022

The Open Group 2022a. The TOGAF Standard. Luettavissa: https://pubs.opengroup.org/togaf-standard/index.html Luettu 10.9.2023

The Open Group 2022b. How to Use the ArchiMate Modelling Language to Support the TOGAF Standard. Luettavissa: https://publications.opengroup.org/g21e Luettu 10.9.2023

The Open Group 2023. ArchiMate 3.2 Specification. Luettavissa: https://pubs.opengroup.org/architecture/archimate3-doc/. Luettu 14.9.2023.

The Open Group s.a. ArchiMate Tool Certification. Luettavissa: https://www.opengroup.org/certifications/archimate/tool Luettu 14.9.2023

Valtionvarainministeriö 2020. Suositus tiedonhallintamallista. Luettavissa: http://urn.fi/URN:ISBN:978-952-367-328-1 Luettu 10.11.2023

Valtiovarainministeriö 2023. Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö. Luettavissa: http://urn.fi/URN:ISBN:978-952-367-275-8. Luettu 30.7.2023

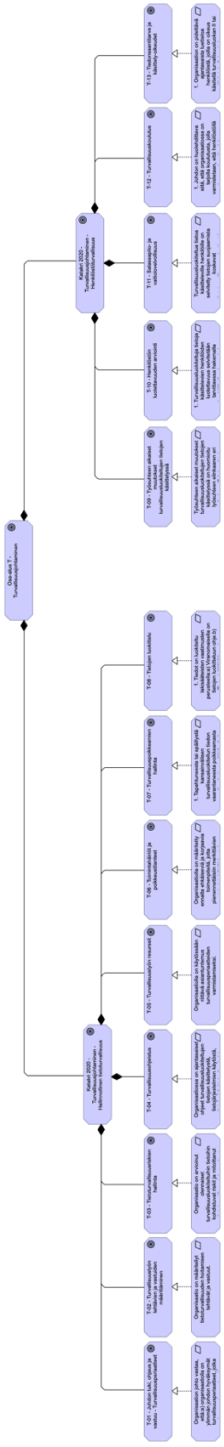
Wierda, G. 2021. Mastering ArchiMate, Edition 3.1. R&A IT Strategy & Architecture. Netherlands. Luettu 22.3.2021

Liitteet

Liite 1. Toiminnallisen työn tuotos: https://github.com/h4nu/Katakri-2020-ArchiMate

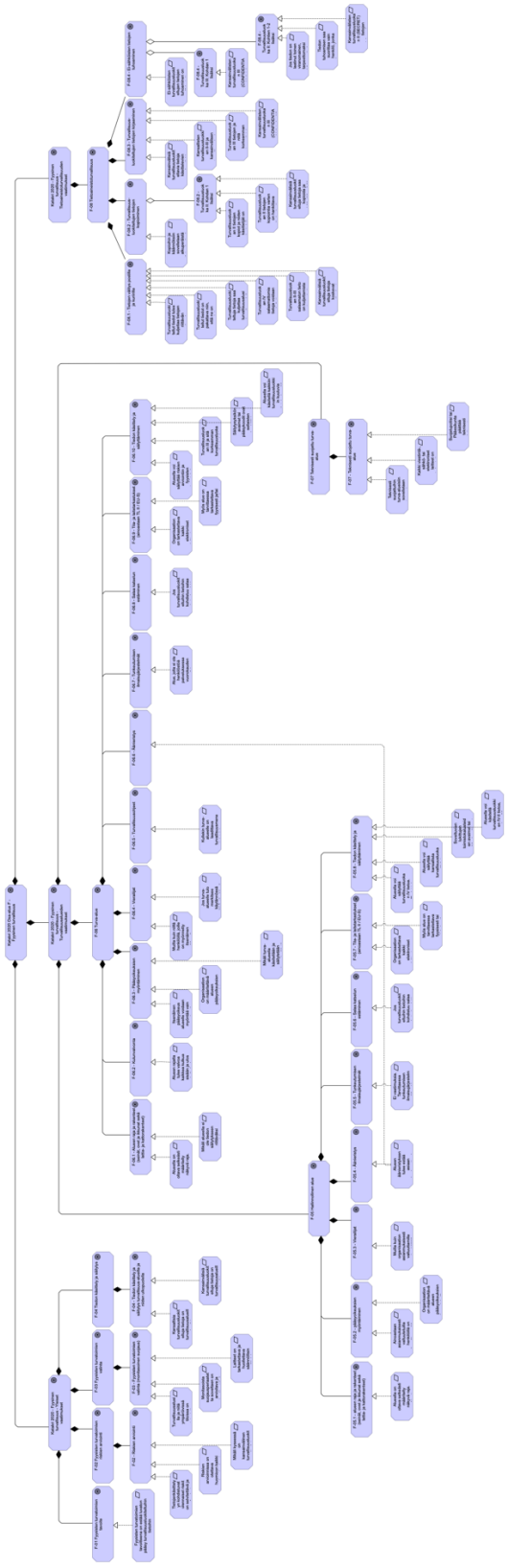
Liite 2. Katakri 2020 osa-alueiden Archimate mallinnukset vaatimuksineen

Turvallisuusjohtamisen osa-alue vaatimuksineen esitettynä kuvassa 27.



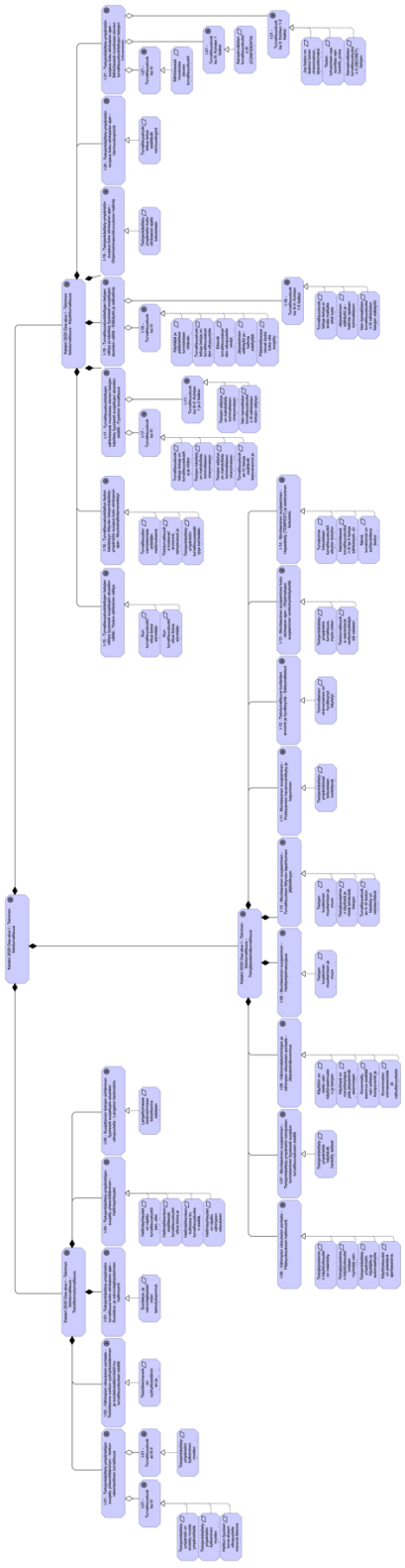
Kuva 27. Katakri 2020 Osa-alue T - Turvallisuusjohtaminen vaatimuksineen

Fyysisen turvallisuuden osa-alue vaatimuksineen esitettynä kuvassa 28.



Kuva 28. Katakri 2020 Osa-alue F - Fyysinen turvallisuus vaatimuksineen

Teknisen tietoturvallisuuden osa-alue vaatimuksineen esitettynä kuvassa 29.



Kuva 29. Katakri 2020 Osa-alue I - Tekninen tietoturvallisuus vaatimuksineen