Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

JOONA ISOKANGAS

Tietoturva- ja tietosuojaosaamisen kehittäminen digitaalisella koulutuspolulla yritysympäristössä

Ahlström Konsernipalvelut Oy

SÄHKÖ- JA AUTOMAATIOTEKNIIKAN
TUTKINTO-OHJELMA
2026

TIIVISTELMÄ

Isokangas, Joona: Tietoturva- ja tietosuojaosaamisen kehittäminen digitaalisella koulutuspolulla yritysympäristössä: Ahlström Konsernipalvelut Oy
Opinnäytetyö, AMK
Sähkö- ja automaatiotekniikan tutkinto-ohjelma
Maaliskuu 2026
Sivumäärä: 51

Opinnäytetyössä arvioitiin organisaation tietoturva- ja tietosuojakoulutukseen liittyviä tarpeita sekä suunniteltiin ja toteutettiin koulutuskokonaisuus, joka on käyttäjän näkökulmasta helposti omaksuttava ja vaivattomasti suoritettava sekä organisaation kannalta hallittava ja ylläpidettävä. Työ toteutettiin Ahlström Konsernipalvelut Oy:n toimeksiannosta. Yhtiö on A. Ahlström Oy:n täysin omistama tytäryhtiö, joka tuottaa konserniyhtiöille keskitettyjä talous-, henkilöstöhallinto- ja ICT-palveluja. Kohderyhmänä oli henkilöstö, mukaan lukien kesä- ja kausityöntekijät. Koulutus toteutettiin organisaation sisäisenä palveluna, jonka tavoitteena on tukea turvallista päätöksentekoa arjen työtilanteissa, madaltaa kynnystä pyytää tarkennusta epäselvissä tilanteissa ja vähentää inhimillisistä virheistä aiheutuvia riskejä.

Koulutustarvetta kartoitettiin kesäkuun 2025 alkupuolella alkukyselyllä (N = 79, n = 46; vastausprosentti 58 %), ja vastausaika päättyi ennen juhannusta. Aineistoa täydennettiin sisäisillä havainnoilla sekä HR:n ja ICT:n näkemyksillä, jotta painopisteet eivät perustuisi pelkästään itsearviointiin vaan myös käytännön havaintoihin. Aineisto jäsennettiin koulutusrakenteeksi teemoittelun ja riskiperusteisen priorisoinnin avulla. Tietoturva- ja tietosuojasyistä työssä ei julkaista yksityiskohtaisia tulosjakaumia, tarkkoja kysymys- tai tehtäväkohtaisia yksityiskohtia eikä sisäistä koulutusmateriaalia paljastavia tietoja, vaan havainnot raportoidaan yleisellä tasolla.

Työn tuloksena toteutettiin mikro-oppimiseen perustuva, kymmenestä moduulista koostuva koulutusohjelma, joka kattaa keskeiset aiheet: kyberturvallisuus, salasanat ja pääsynhallinta, mobiililaitteet, fyysinen turvallisuus, etätyöskentely, internetin turvallinen käyttö, turvallinen sähköposti, tietojenkalastelu, haittaohjelmat ja kiristyshaittaohjelmat sekä sosiaalinen manipulointi. Koulutus toteutettiin MetaCompliance-ympäristössä ja integroitiin A-Learning-oppimisympäristöön (Vuolearning) koulutuspoluksi, joka tukee perehdytystä, etenemistä ja yleistason seurantaa. Lisäksi keskeiset toimintaohjeet dokumentoitiin tukemaan turvallista toimintaa tilanteissa, joissa tarvitaan harkintaa.

Johtopäätöksenä todetaan, että käyttäjälähtöinen rakenne, koulutuspolku sekä HR:n ja ICT:n selkeä roolitus parantavat koulutuksen toteutettavuutta ja ylläpidon hallittavuutta. Työssä määriteltiin seurannan periaatteet ja jatkuvan kehittämisen sykli, joiden avulla kokonaisuutta voidaan päivittää käyttöönoton aikana kertyvän palautteen ja seurantatiedon perusteella. Lisäksi ylläpidon vastuut kuvattiin yleistasolla, jotta koulutus ei jää yksittäisen henkilön varaan.

Avainsanat: tietoturva, tietosuoja, perehdytys, koulutuspolku, mikro-oppiminen, MetaCompliance, Vuolearning, käyttäjälähtöisyys

ABSTRACT

Isokangas, Joona: Developing Information Security and Data Protection Competence Through a Digital Learning Path in a Business Environment: Ahlström Konsernipalvelut Oy
Bachelor's Thesis
Degree Programme in Electrical and Automation Engineering
March 2026
Number of pages: 51

This thesis assessed the organisation's information security and data protection training needs and planned and implemented a training programme that is easy for end users to follow and manageable to maintain at organisational level. The work was commissioned by Ahlström Konsernipalvelut Oy, a wholly owned subsidiary of A. Ahlström Oy that provides centralised financial, HR and ICT services for Group companies. The target group comprised personnel, including summer and seasonal employees. The training was implemented as an internal service to support secure day-to-day decision-making, lower the threshold for seeking clarification in ambiguous situations, and reduce risks arising from human error.

Training needs were examined through a baseline survey conducted in early June 2025 (N = 79, n = 46; response rate 58%), with the response period ending before Midsummer. The dataset was complemented with internal observations and input from HR and ICT to ensure that priorities did not rely on self-assessment alone but were grounded in operational practice. The material was structured into a training framework through thematic analysis and risk-based prioritisation. For information security and data protection reasons, the thesis does not disclose detailed result distributions, item-level question or task details, or information that could reveal internal training materials; findings are therefore reported at a general level.

The outcome was a microlearning-based training programme divided into ten modules covering key topics: cybersecurity, passwords and access management, mobile devices, physical security, remote working, safe internet use, secure email, phishing, malware and ransomware, and social engineering. The programme was delivered in MetaCompliance and integrated into A-Learning (Vuolearning) as a learning pathway supporting onboarding, progression, and aggregate-level monitoring. In addition, key operational procedures were documented to support safe action where situational judgement is required.

The thesis concludes that a user-centred structure, a guided learning pathway, and clearly defined HR and ICT roles improve the programme's feasibility and maintainability. It also established monitoring principles and a continuous improvement cycle to support updates informed by deployment feedback and monitoring data. In addition, maintenance responsibilities were outlined at a high level to reduce dependence on any single individual.

Keywords: information security, data protection, onboarding, learning path, microlearning, MetaCompliance, Vuolearning, user-centred design

ALKUSANAT

Haluan kiittää Ahlström Konsernipalvelut Oy:tä saamastani toimeksiannosta, luottamuksesta työn toteuttamiseen ja mahdollisuudesta tehdä opinnäytetyö aidossa toimintaympäristössä. Samalla haluan kiittää kaikkia A. Ahlström -konsernissa työskenteleviä siitä, että sain viettää kaksi hienoa kesää osana osaavaa ja kannustavaa työyhteisöä. Erityinen kiitos kuuluu kaikille niille henkilöille, jotka osallistuivat työn valmisteluun, keskusteluihin ja käytännön toteutuksen arviointiin.

Haluan kiittää HR-tiimiä (Eija Holmi ja Jere Ahonkivi) yhteistyöstä ja tuesta työn etenemisessä. Kiitän myös esihenkilöäni, Ahlström Konsernipalvelut Oy:n toimitusjohtajaa (Pasi Koota), luottamuksesta ja tuesta työn käynnistämisessä sekä siitä, että työn toteuttaminen mahdollistui osana organisaation kehittämistä.

Lisäksi haluan osoittaa erityisen lämpimät kiitokseni ICT-tiimille (Jukka Tuominen ja Osmo Tuulensuu). Yhteistyö heidän kanssaan oli opinnäytetyön onnistumisen kannalta keskeistä, mutta samalla se oli myös henkilökohtaisesti merkityksellistä ja aidosti miellyttävää. Jukka ja Osmo jaksoivat neuvoa, opettaa ja selventää asioita arjen tilanteissa tavalla, joka kasvatti omaa ymmärrystäni ja teki työstä mielekästä. Olen siitä vilpittömästi kiitollinen.

Lopuksi kiitän opinnäytetyöni ohjaajaa joustavuudesta, tuesta ja palautteesta työn eri vaiheissa.

Porissa 06.03.2026
Joona Isokangas

SISÄLLYS

SYMBOLI- JA LYHENNELUETTELO

A-Learning	Organisaation brändätty nimi Vuolearning-oppimis-ympäristölle
ENISA	European Union Agency for Cybersecurity
HR	Henkilöstöhallinto (Human Resources)
ICT	Tieto- ja viestintätekniikka; organisaation ICT-toiminto (Information and Communication Technology)
ISO	International Organization for Standardization
ISO/IEC	ISO:n ja IEC:n yhteisstandardit (esim. ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005)
MetaCompliance	Tietoturva- ja tietosuojakoulutuksen sisältö- ja suoritusympäristö
N	Kyselyn perusjoukon koko / kyselyyn kutsutut (tässä: 79)
n	Vastaajien määrä (tässä: 46)
NIST	National Institute of Standards and Technology
TENK	Tutkimuseettinen neuvottelukunta

1 JOHDANTO

Työn lähtökohta on käytännöllinen, mutta samalla organisaation kannalta periaatteellisesti merkittävä. Tavoitteena ei ollut laatia vain yksittäistä koulutusmateriaalia, vaan rakentaa ylläpidettävä kokonaisuus, joka tukee organisaation arkea ja ohjaa käyttäjää toimimaan turvallisesti tilanteissa, joissa päätökset syntyvät nopeasti ja usein epävarmuuden keskellä. Samalla tarkoituksena oli rakentaa malli, jonka varaan tietoturva- ja tietosuojaosaamista voidaan kehittää hallitusti sekä perehdytyksessä että työssä. Tässä johdannossa jäsennetään, mihin ongelmaan työ vastaa, miksi rajaus tehtiin juuri näin ja millaisista reunaehdoista ratkaisua ryhdyttiin rakentamaan.

1.1 Tausta ja kehittämistarve

Tietoturva ja tietosuoja ovat yritysympäristössä ennen kaikkea arjen toimintakysymyksiä. Vaikka tekniset kontrollit muodostavat turvallisuuden perustan, turvallinen toiminta rakentuu myös henkilöstön käytännön valinnoista, kuten viestien tulkinnasta, tiedon jakamisesta, tunnistautumisesta ja epäselvien tilanteiden varmistamisesta (ISO/IEC 27002:2022, 2022). ENISA (2024) ja Verizon (2025) kuvaavat uhkakenttää, jossa tietojenkalastelu, tunnusten väärinkäyttö ja erilaiset sosiaalisen manipuloinnin muodot kohdistuvat juuri ihmisen toimintaan. Tässä valossa koulutuksen tehtävä ei ole vain lisätä tietoa, vaan tukea käyttäjää tunnistamaan poikkeava tilanne, pysähtymään ja toimimaan johdonmukaisesti myös ajallisen paineen ja keskeytysten alla.

Kehittämistarve ei tässä työssä liittynyt vain tiedon määrään, vaan myös siihen, miten tieto tavoittaa käyttäjän oikealla hetkellä ja sellaisessa muodossa, että sitä voidaan soveltaa arjen työtilanteissa. Organisaatiossa oli jo olemassa ohjeita, toimintaperiaatteita ja tietoa, mutta ne eivät kaikilta osin muodostaneet käyttäjän näkökulmasta helposti löydettävää, loogisesti hahmottuvaa ja työtilanteissa hyödynnettävää kokonaisuutta. Tämän vuoksi työn tavoitteena ei ollut uuden materiaalin määrällinen lisääminen, vaan koulutusratkaisun

rakentaminen siten, että olennainen tieto kokoaa hajanaiset ohjeet, painotukset ja käytännöt selkeäksi, muistettavaksi ja arjessa toimivaksi peruspoluksi.

1.2 Toimeksiantaja ja toimintaympäristö: A. Ahlström ja Ahlström Konsernipalvelut

Työ toteutettiin A. Ahlström -konsernin toimintaympäristössä, jossa konserni-rakenne, keskitetty palvelumalli ja vaihtelevat työroolit muovaavat myös tietoturva- ja tietosuojakoulutuksen ehtoja. Kyse ei ole yhden tiimin sisäisestä ohjeistuksesta, vaan kokonaisuudesta, jonka on toimittava erilaisissa tehtävissä, eri taustoista tuleville käyttäjille ja osana yhteisiä palveluprosesseja. Ahlströmin juuret ulottuvat vuoteen 1851, ja vuonna 2026 yhtiö juhlistaa 175-vuotista historiaansa (A. Ahlström, 2026), mikä tuo konserniympäristön jatkuvuudelle ja yhteisten toimintatapojen merkitykselle myös ajallista perspektiiviä.

Konserniympäristössä yhteisten periaatteiden ja prosessien merkitys korostuu, koska samoja tietoja, järjestelmiä ja palveluja käytetään erilaisissa rooleissa ja vaihtelevissa tilanteissa. Tällaista keskitettyä palvelumallia (shared services) tarkastelleet Herbert ja Seal (2012) sekä Janssen ja Joha (2006) tuovat esiin, että keskitetty palvelurakenne voi yhtenäistää toimintatapoja ja parantaa hallittavuutta, mutta samalla se edellyttää selkeää koordinaatiota, selkeästi määriteltyjä vastuita ja käytännössä toimivia yhteisiä menettelyjä.

Opinnäytetyön toimeksiantaja on Ahlström Konsernipalvelut Oy, joka tuottaa konsernille keskitettyjä tukipalveluja (A. Ahlström, 2024). Tämän vuoksi koulutuksen onnistuminen ei vaikuta vain yksittäisen työntekijän osaamiseen, vaan laajemmin siihen, miten yhdenmukaisesti turvalliset käytännöt juurtuvat organisaation arkeen. Kohderyhmään sisältyivät myös kesä- ja kausityöntekijät, mikä vahvisti tarvetta rakentaa ratkaisu, jonka aloituskynnys on matala ja eteneminen on käyttäjän näkökulmasta intuitiivista.

1.3 Tavoite ja kehittämiskysymykset

Työn tavoitteena oli arvioida organisaation tietoturva- ja tietosuojaosaamisen kehittämistarpeita sekä rakentaa digitaalinen koulutuskokonaisuus, joka on käyttäjälle ymmärrettävä, perehdytykseen soveltuva ja sujuvasti suoritettava sekä organisaatiolle hallittava. Tavoitteena ei ollut kasvattaa koulutuksen määrää sinänsä, vaan jäsentää olemassa olevat tarpeet ja käytännöt yhtenäiseksi peruspoluksi, jonka varaan turvallista toimintaa voidaan rakentaa järjestelmällisesti.

1) Millaisia tietoteknisiä ja tietoturvaan liittyviä koulutustarpeita organisaatiossa tunnistetaan alkukartoituksen ja sidosryhmähavaintojen perusteella?

2) Miten koulutuskokonaisuus voidaan suunnitella kohderyhmälle sopivaksi niin, että se tukee perehdytystä ja arjen toimintamalleja?

3) Miten MetaCompliancea ja A-Learningia voidaan hyödyntää siten, että koulutus on samanaikaisesti sujuva, seurattava ja ylläpidettävä?

Tavoitetilana oli ratkaisu, joka muuttaa hajanaiset ohjeet ja vaihtelevat käytännöt yhtenäiseksi peruspoluksi. Tällöin koulutus ei jää irralliseksi materiaaliksi, vaan siitä muodostuu osa perehdytystä, arjen toimintaa ja ylläpidon näkökulmasta hallittavaa kokonaisuutta. Samalla koulutus ei mittaa yksittäisten työntekijöiden osaamista irrallisesti, vaan tukee yhteistä toimintamallia tilanteissa, joissa epävarmuus, kiire tai rutiini voivat kasvattaa poikkeamariskiä. Tämä vastaa myös NISTin viitekehyksen ajatusta yhteisten ja hallittujen toimintatapojen merkityksestä organisaation turvallisuudessa (Joint Task Force Transformation Initiative, 2012).

1.4 Rajaukset ja tietoturvaperiaatteet raportoinnissa

Työ rajattiin tietoturva- ja tietosuojakoulutuksen suunnitteluun, toteutukseen ja käyttöönoton edellytysten varmistamiseen. Tarkastelun kohteena eivät olleet organisaation tekniset suojausratkaisut tai yksityiskohtainen riskienhallinta, vaan se, miten henkilöstölle voidaan rakentaa käytännöllinen ja ylläpidettävä koulutusmalli. Koska työ on toteutettu yritysympäristössä, myös julkisen raportoinnin tarkkuustaso on osa työn laatua, riskienhallintaa ja käytännöllisyyttä.

Työssä kuvataan ratkaisut, periaatteet, roolit ja valintojen perusteet, mutta ei sellaisia yksityiskohtia, jotka paljastaisivat organisaation sisäisiä heikkouksia, tarkkaa arviointilogiikkaa tai koulutuksen sellaista rakennetta, jonka avoin kuvaaminen ei olisi tarkoituksenmukaista. Rajaus ei heikennä työn arvioitavuutta, vaan ohjaa huomion siihen, ovatko ratkaisut johdonmukaisia, käyttökelpoisia ja ylläpidon kannalta perusteltuja.

1.5 Työn toteutus lyhyesti

Kehittämistyö eteni neljässä päävaiheessa. Ensin koulutustarvetta kartoitettiin alkukyselyllä ja täydentävillä sidosryhmähavainnoilla, jotta painotukset eivät perustuisi pelkästään itsearviointiin. Tämän jälkeen havainnot teemoiteltiin ja priorisoitiin riskiperusteisesti, minkä pohjalta suunniteltiin kymmenen jakson mikro-oppimiseen perustuva koulutuspolku. Kolmannessa vaiheessa sisältö rakennettiin MetaComplianceen ja koottiin A-Learningiin käyttäjälle helposti hahmotettavaksi kokonaisuudeksi. Lopuksi kokonaisuuden toimivuutta arvioitiin sisäisen testauksen ja pilotoinnin avulla, minkä perusteella sitä tarkennettiin ennen laajempaa käyttöönottoa. Ratkaisun suunnittelussa huomioitiin lisäksi käyttäjäpolun selkeyttä ja vaiheittaista etenemistä korostavat periaatteet Tayloria ja Hungia mukaillen (Taylor & Hung, 2022; Merritt ym., 2024; ISO 9241-210:2019, 2019).

1.6 Työn rakenne

Luku 1 kuvaa työn taustan, tavoitteet ja rajaukset. Luku 2 kokoaa työn tietoperustan, luku 3 esittää kehittämistyön menetelmällisen logiikan ja aineiston muodostumisen, luvut 4 ja 5 kuvaavat koulutuskokonaisuuden suunnittelun ja teknisen toteutuksen, luku 6 tarkastelee ylläpitoa ja riskienhallintaa, ja luku 7 kokoaa työn johtopäätökset, rajoitteet, jatkotoimet sekä oman oppimisen keskeiset havainnot.

1.7 Työn tuotokset

Työn päätuotoksena syntyi organisaation käyttöön rakennettu tietoturva- ja tietosuojakoulutuksen kokonaisuus, joka sisältää koulutuspolun, sen taustalla olevan priorisointilogiikan sekä ylläpidon ja seurannan periaatteet. Tuotos ei ole vain oppimissisältöjen kokoelma, vaan toimintamalli, jonka tarkoituksena on tehdä turvallisesta toiminnasta ennakoitavaa sekä käyttäjälle että organisaatiolle. Kokonaisuus sisältää riskiperusteisen sisältö- ja priorisointilogiikan, kymmenen jakson koulutuspolun MetaCompliance- ja A-Learning-ympäristöissä, yleistasoisen seuranta- ja raportointimallin HR:n ja ICT:n käyttöön sekä ylläpidon, palautteen ja jatkokehityksen periaatteet. Se on suunniteltu osaksi perehdytystä ja jatkuvaa osaamisen ylläpitoa, jotta koulutus ei jää irralliseksi materiaalipaketiksi vaan toimii käytännössä osana organisaation toimintamallia.

2 TAUSTA JA TEOREETTINEN VIITEKEHYS

Toisessa luvussa kootaan ne käsitteet ja näkökulmat, joihin kehittämistyön ratkaisut nojaavat. Tarkoitus ei ole kasvattaa työn teoriapainoa, vaan rajata näkyviin juuri se tietoperusta, joka auttaa perustelemaan käyttäjälähtöisen, riskiperusteisen ja organisaatiossa ylläpidettävän koulutuskokonaisuuden. Tässä

työssä teoreettisen viitekehyksen tehtävä on ennen kaikkea täsmentää ja perustella valittuja ratkaisuja, ei kasvattaa työn abstraktiotasoa tai laajuutta.

2.1 Koulutustarpeen arviointi työelämäkontekstissa

Työelämässä koulutustarve on osaamiskuilun lisäksi toimintatapojen kysymys. Goldstein ja Ford (2002) sekä Noe (2023) kuvaavat koulutustarpeen arviointia prosessina, jossa tarkastellaan paitsi osaamista myös työn vaatimuksia, toimintaympäristöä ja niitä tilanteita, joissa virheillä on käytännön seurauksia. Tässä työssä lähtökohta oli samansuuntainen: olennaista ei ollut selvittää vain, mitä käyttäjät tietävät, vaan myös sitä, missä tilanteissa turvallinen toiminta horjuu, oikean toimintatavan tunnistaminen vaikeutuu ja tuen tarve korostuu. Tästä syystä koulutustarpeen arvioinnissa yhdistettiin kyselyaineisto, sidosryhmähavainnot ja käytännön työtilanteet, mikä on perusteltua silloin, kun samaa ilmiötä tarkastellaan useasta näkökulmasta eikä yhden aineistolähteen varassa (Patton, 1999; Heale & Forbes, 2013). Valittua näkökulmaa täydentävät Puhakainen ja Siponen (2010), jotka korostavat, että tietoturvakoulutuksessa huomio kannattaa kohdistaa erityisesti niihin tilanteisiin, joissa käyttäjän toiminta vaikuttaa aidosti lopputulokseen.

2.2 Digitaalinen oppiminen ja oppimisympäristö yrityksessä

Digitaalinen oppiminen toimii yritysympäristössä parhaiten silloin, kun sen vahvuudet sidotaan työn arkeen. Saavutettavuus, ajasta ja paikasta riippumaton suorittaminen sekä mahdollisuus rakentaa sisältö vaiheittain tukevat koulutusta, jota suoritetaan pääsääntöisesti työtehtävien rinnalla. Samalla oppimisympäristöltä edellytetään selkeää rakennetta ja käyttäjälle näkyvää etenemislogiikkaa, jotta se ei itsessään lisää kuormitusta. Järjestelmän on näyttäydyttävä käyttäjälle sekä hyödyllisenä että riittävän helppokäyttöisenä, ja etenemisen tulee olla ymmärrettävää sekä tehtävän suorittamista tukevaa (Davis, 1989; Venkatesh ym., 2003; ISO 9241-210:2019, 2019). Tästä syystä alustavalinnassa ei tarkasteltu vain sisältöjen jakamista, vaan myös sitä, miten

käyttäjä löytää seuraavan oikean vaiheen ilman tarpeetonta kognitiivista kuormitusta.

2.3 Palveluhenkinen ja käyttäjälähtöinen tietoturvakoulutus

Palveluhenkinen ja käyttäjälähtöinen lähestymistapa tarkoittaa tässä työssä sitä, että koulutus suunnitellaan työntekijän näkökulmasta mahdollisimman selkeäksi, ennakoitavaksi ja helposti lähestyttäväksi siten, että se tukee toimintaa myös tilanteissa, joissa oma varmuus ei riitä. Sen sijaan, että käyttäjä nähtäisiin ensisijaisesti riskinä, hänet nähdään toimijana, jota voidaan tukea oikea-aikaisella ohjauksella, näkyvillä tukikanavilla ja ymmärrettävillä toimintamalleilla. Turvallisuuskulttuuri vahvistuu, kun turvallinen toiminta rakentuu osaksi arjen käytäntöjä eikä irralliseksi velvoitteeksi, ja käyttäjää tukeva palveluhenkisyys lisää samalla koulutuksen hyväksyttävyyttä ja käytännön vaikuttavuutta (ENISA, 2017; Roer & Carpenter, 2022). Käyttäjää tukeva tietoturvakoulutus ei perustu vain sääntöjen esittämiseen, vaan myös siihen, että turvallinen toimintatapa ja avun hakemisen reitti tehdään arjessa näkyväksi (Kyberturvallisuuskeskus, 2023). Tätä näkökulmaa syventää Edmondsonin (1999) psykologista turvallisuutta koskeva ajattelu: jos virheiden tai epävarmuuden esiin tuominen vaikeutuu, turvallisen toiminnan edellytykset heikkenevät juuri kriittisimmissä tilanteissa.

2.4 Tietoturva- ja tietosuojakoulutus henkilöstölle

Tietoturva- ja tietosuojakoulutuksen erityispiirre on siinä, ettei sen tavoitteena ole vain lisätä tietoisuutta, vaan ohjata toimintaa käytännön tilanteissa. Pelkkä yleinen tietoisuus ei siis riitä, jos työntekijä ei tunnista tilanteen olennaista riskiä tai jos organisaation odotukset jäävät käytännössä epäselviksi. Siksi koulutuksen painopiste siirtyi pois laajoista taustaselityksistä kohti konkreettisia toimintamalleja, jotka tukevat pysähtymistä, varmistamista ja turvallista valintaa juuri ratkaisevalla hetkellä (Puhakainen & Siponen, 2010; Herath & Rao, 2009; Butavicius ym., 2022). Samalla koulutuksessa erotettiin yhteinen peruskerros ja organisaatiokohtainen toimintatapakerros: ensin vahvistetaan kaikille

olennaiset periaatteet, minkä jälkeen täsmennetään, miten toimitaan juuri omassa ympäristössä. Sama perusajatus näkyy myös Joint Task Forcen (2020) sekä Whitmanin ja Mattordin (2016) näkemyksissä: turvallinen käyttäytyminen edellyttää sekä yleistä ymmärrystä että organisaatiokohtaisia käytäntöjä.

2.5 Vaikuttavuuden ja toimivuuden arviointi

Yritysympäristössä koulutuksen arviointia on tarkoituksenmukaista jäsentää kerroksittain. Baldwinin ja Fordin (1988) sekä Kirkpatrickin ja Kirkpatrickin (2016) mukaan koulutuksen arvo ei palaudu pelkkään suoritukseen, vaan siihen, siirtyykö oppiminen käytännön toiminnaksi. Tässä työssä vaikuttavuuden tarkastelu kytkettiin toteutumiseen, käyttäjäkokemukseen ja ylläpidon näkökulmasta hyödylliseen seurantaan. Käytännössä tarkastelu kohdistui kolmeen kysymykseen: tavoittaako koulutus kohderyhmän, auttaako se korjaamaan puutteellista tai virheellistä ymmärrystä ja tuottaako se sellaista palautetta ja seurantatietoa, jonka avulla kokonaisuutta voidaan kehittää. Hattie ja Timperley (2007) korostavat palautteen merkitystä ymmärryksen täsmentymisessä, ja Merritt ym. (2024) sekä Spitzner (2023) painottavat, että tietoturvakoulutuksessa arvioinnin tulee tukea kehittämistä eikä muuttua itsetarkoitukseksi. Tavoitteena ei siten ollut rakentaa raskasta arviointijärjestelmää, vaan malli, joka tuottaa riittävän kuvan koulutuksen toimivuudesta ja kehittämistarpeista.

3 TUTKIMUSMENETELMÄT JA AINEISTONKERUU

Kehittämistyön uskottavuus rakentuu siitä, ettei ratkaisu synny irrallisena ideana vaan aineiston, rajauksen ja vaiheittaisen päätöksenteon kautta. Tässä luvussa tehdään näkyväksi, miten koulutustarve tunnistettiin, miten havaintoja tulkittiin ja millä perusteilla ne muunnettiin käyttöön otettavaksi koulutuskokonaisuudeksi. Samalla kuvataan työn luotettavuuteen, eettisyyteen ja tietoturvalliseen raportointiin liittyvät ratkaisut.

3.1 Kehittämistyön lähestymistapa ja peruslogiikka

Työ toteutettiin toiminnallisena kehittämistyönä, jossa tavoitteena ei ollut vain kuvata ilmiötä, vaan tuottaa organisaation käyttöön konkreettinen ja hyödynnettävä ratkaisu. Lähestymistapa on lähellä suunnittelutieteellistä ajattelua (design science), jossa ongelman ymmärtäminen, ratkaisun rakentaminen ja sen käytännöllinen arviointi kytkeytyvät toisiinsa (Hevner ym., 2004; Peffers ym., 2007). Tämä logiikka sopi työhön hyvin, koska tavoitteena oli rakentaa koulutusmalli, ei pelkästään analysoida koulutustarvetta.

Kehittämistyön peruslogiikka oli käyttäjälähtöinen, palveluhenkinen ja iteratiivinen. Koulutusta ei suunniteltu teoriasta käsin irrallisena kokonaisuutena, vaan havaituista tarpeista, käytännön työtilanteista ja organisaation toimintaympäristöstä. Kokonaisuus hahmotettiin sosioteknisenä ratkaisuna, jossa järjestelmäympäristö, ohjeistus ja käyttäjän toiminta vaikuttavat toisiinsa. Ratkaisua tarkennettiin vaiheittain sen mukaan, mitä aineisto, pilotointi ja sidosryhmäkeskustelut toivat näkyviin.

Työn aikana vahvistui näkemys siitä, että tietoturvan käytännön haaste ei useinkaan liity käsitteiden puuttumiseen, vaan siihen, ettei käyttäjä kiireessä tunnista seuraavaa sopivaa oikeaa toimintatapaa. Siksi menetelmällinen tavoite ei ollut kerätä mahdollisimman paljon aineistoa, vaan rakentaa aineiston pohjalta rakenne, joka vähentää epävarmuutta, tukee tilannesidonnaista päätöksentekoa ja ohjaa turvalliseen toimintaan juuri ratkaisevalla hetkellä.

3.2 Toteutusvaiheet ja aikajana

Kehittämistyö eteni vaiheittain keväästä 2025 alkuvuoteen 2026. Ensin täsmennettiin työn tavoitteet, rajaukset ja tietoturvallisen raportoinnin periaatteet. Tämän jälkeen toteutettiin alkukysely, jota täydennettiin HR:n ja ICT:n näkemyksillä sekä arjen käytännön havainnoilla. Seuraavassa vaiheessa aineisto teemoiteltiin ja priorisoitiin, minkä pohjalta suunniteltiin koulutuksen sisältörakenne, suorituslogiikka ja kahden ympäristön työnjako. Viimeisessä vaiheessa kokonaisuus testattiin sisäisesti, sitä tarkennettiin pilotoinnin perusteella ja sille

määriteltiin käyttöönottoa sekä ylläpitoa tukevat toimintatavat. Vaiheistus oli tärkeä, koska se teki kehittämistyöstä hallittavan ja mahdollisti ratkaisujen perustelemisen vaihe vaiheelta. Ojasalo ym. (2015) kuvaavat toiminnallisen kehittämistyön etenevän vaiheittain tavoitteiden täsmentämisestä toteutukseen ja arviointiin. Myös tässä kehittämisprosessissa ratkaisu rakentui iteratiivisesti ja tarkentui työn edetessä.

3.3 Aineistot ja aineiston muodostaminen

Kehittämistyön aineisto muodostui kolmesta toisiaan täydentävästä lähteestä: alkukyselystä, HR- ja ICT-sidosryhmien havainnoista sekä toteutuksen aikana kertyneestä kehittämisaineistosta. Näin koulutustarvetta ei tarkasteltu vain käyttäjien itsearviointina, vaan osana organisaation käytäntöjä ja tukitoimintojen kokemusta. Aineiston koostaminen useasta lähteestä vahvisti tulkintaa erityisesti silloin, kun eri lähteet osoittivat samansuuntaisesti. Tämänkaltaista aineistonmuodostusta on perusteltu sillä, että samaa ilmiötä tarkastellaan useasta suunnasta eikä yhden lähteen varassa (Patton, 1999; Carter ym., 2014). Alkukysely tarjosi yleiskuvan epävarmuusalueista, sidosryhmät varmistivat organisaation käytännöt ja toteutuksen aikana kertyneet havainnot osoittivat, missä kohdissa käyttäjäpolku tai sisältö vaati täsmennystä. Sidosryhmille välitetyn täsmennyspyynnön esimerkki on esitetty liitteessä 1.

3.4 Aineiston muodostumisen käytännön toteutus ja vinoumien hallinta

Aineiston muodostamisessa huomioitiin sekä käytännöllisyys että vinoumien riski. Alkukysely lähetettiin koko kohderyhmälle, ja sitä tulkittiin kehittämisen suuntaa antavana lähtökuvana, ei yksilötason osaamisen mittarina. Aineistoa täydennettiin myös muilla havainnoilla, jotta itsearviointiin, vastauskatoon ja sosiaaliseen toivottavuuteen liittyviä vinoumia ei ylitulkittaisi (Groves, 2006; van de Mortel, 2008; Tourangeau & Yan, 2007). Tämän vuoksi kyselyä ei pidetty yksinään riittävänä perustana koulutusratkaisulle, vaan sitä täydennettiin HR:n ja ICT:n havainnoilla. Näin aineisto jäsentyi lähemmäs käytännön todellisuutta eikä jäänyt vain vastaajien kokemusten varaan.

3.5 Aineiston käsittely ja analyysin käytännön toteutus

Aineiston analyysin tavoitteena oli jäsentää hajanaisista havainnoista johdonmukainen koulutusrakenne. Käytännössä tämä tarkoitti havaintojen teemoittelua, niiden vaikutusten arviointia sekä sen tarkastelua, millaisissa tilanteissa käyttäjä voi omalla toiminnallaan vähentää riskiä. Tätä lähestymistapaa tukee Braunin ja Clarken (2006) näkemys siitä, että aineistosta voidaan tunnistaa toistuvia merkityksiä ja rakentaa niiden varaan tulkinnallinen kokonaisuus, kun taas ISO/IEC 27005:2022 (2022) tarjoaa riskiperusteiselle priorisoinnille luontevan viitekehyksen. Analyysin tuloksena ei muodostunut irrallisten aiheiden luetteloa, vaan rakenne, jossa jokainen jakso perusteltiin havaintojen, riskitason ja käytännön tarpeen kautta.

3.6 Tekijän rooli, työn luotettavuus ja rajoitteet

Tekijä vastasi koulutuskokonaisuuden suunnittelusta, koordinoinnista ja raportoinnista, mikä toi työhön vahvan käytäntölähtöisen näkökulman mutta edellytti samalla tietoista reflektiota oman roolin vaikutuksesta tulkintaan. Berger (2015) ja Finlay (2002) korostavat, että kehittämistyössä tekijän asema on syytä tehdä näkyväksi, jotta lukija voi arvioida työn rajauksia ja tulkintoja avoimesti. Samaa läpinäkyvyyden vaatimusta painottaa Tracy (2010), jonka mukaan laadullisen työn uskottavuus rakentuu perustelluista tulkinnoista, tutkimusprosessin näkyväksi tekemisestä ja arvioinnin jäljitettävyydestä. Tässä työssä tämä näkyi siinä, että ratkaisut perusteltiin vaiheittain, keskeiset valinnat dokumentoitiin ja aineistoa tarkasteltiin useasta lähteestä, jotta tulkinta ei kaventuisi pelkästään tekijän ennakko-oletuksiin vaan säilyisi analyyttisesti perusteltuna. Työn luotettavuus rakentui ennen kaikkea päätöksenteon jäljitettävyydestä ja siitä, ettei koulutuksen sisältöä johdettu yhden aineistolähteen varaan. Samalla on kuitenkin tunnistettava työn rajoitteet: aineisto ei ole tilastollisesti yleistettävä, osa arvioinnista perustuu itsearviointiin ja julkinen raportointitaso on tietoturvasyistä tietoisesti pidetty yleistasoisena.

3.7 Priorisointikriteerit ja analyysin jäljitettävyys

Koulutuksen painopisteet priorisoitiin kolmen käytännöllisen kriteerin avulla: virheen mahdollinen vaikutus, tilanteen toistuvuus arjessa sekä se, voiko käyttäjä omalla toiminnallaan aidosti vaikuttaa lopputulokseen. Näin koulutuksen sisältö ei rakentunut vain kiinnostavien aiheiden ympärille, vaan sellaisten käyttäjätilanteiden ympärille, joissa oikea toimintamalli vähentää riskiä käytännössä ja joissa käyttäjälle voidaan tarjota vaikuttavaa ja käyttökelpoista tukea (Merritt ym., 2024). Vaikutuksen, toistuvuuden ja käyttäjän vaikutusmahdollisuuden huomioiminen on lähellä myös riskiperusteista arviointiajattelua, jossa huomio kohdistetaan niihin teemoihin, joissa ohjeistettu käyttäytyminen toimii aidosti merkityksellisenä kontrollina (ISO/IEC 27005:2022, 2022). Priorisointi vastaa laadullisen analyysin logiikkaa, jossa toistuvista havainnoista muodostetaan päätöksentekoa ohjaavia teemoja (Braun & Clarke, 2006).

Taulukko 1. Päätöspolku tarvehavainnoista koulutusjaksoiksi (koontitaso)

Havaittu tarve / epävarmuus (teemataso)	**Riskitilanne (esimerkkitaso)**	**Tavoiteltu toimintamalli (tiivis)**	**Koulutusjakso**	**Perustelu ja aineistolähde (koontitaso)**
Yhteisen käsitteistön puute ja epäselvyys poikkeamatilanteissa	Käyttäjä ei tiedä, milloin tilanne on tietoturvapoikkeama ja mihin ilmoitetaan	Pysähdy, varmista ja ohjaa tilanne oikeaan tukikanavaan	1) Kyberturvallisuus	Alkukyselyn epävarmuusteemat + HR/ICT:n prosessikuvaus ja perehdytyksen vaatimukset
Tunnistautumiseen liittyvä epävarmuus (salasana/MFA/tiliepäily)	Yllättävä kirjautumispyyntö tai epäily tilin vaarantumisesta	Älä hyväksy yllättävää pyyntöä; vaihda tunnisteet ohjeistuksen mukaan, tarvittaessa yhteys ICT:hen	2) Salasanat	Kyselyssä korostuneet tunnistautumisen riskit + tietoturvaohjeistus
Mobiililaitteiden käyttö vaihtelevissa ympäristöissä	Laite katoaa tai sitä käytetään julkisessa tilassa tai verkossa	Suojaa laite, käytä lukitusta ja ilmoita poikkeamista viipymättä	3) Mobiililaitteet	Arjen työtilanteiden yleisyys + riskiperusteinen priorisointi

Havaittu tarve / epävarmuus (teemataso)	**Riskitilanne (esimerkkitaso)**	**Tavoiteltu toimintamalli (tiivis)**	**Koulutusjakso**	**Perustelu ja aineistolähde (koontitaso)**
Fyysisen turvallisuuden peruskäytännöt arjessa	Vierailija tai sivullinen näkee luottamuksellista tietoa	Pidä työtila hallinnassa ja estä tietojen näkyminen sivullisille	4) Fyysinen turvallisuus	Organisaation turvallisuuskäytännöt + yleiset arjen riskitilanteet
Etätyön suojaus ja työskentelytapa	Kotona tai matkalla työskentely ilman kontrolloitua ympäristöä	Varmista työympäristö, näytön suojaus ja yhteydet; pyydä apua epäselvissä tilanteissa	5) Etätyöskentely	Toimintaympäristön muutos (etätyö) + käyttäjän päätökset ratkaisevat riskin
Verkkoselailun ja latausten turvallisuus	Käyttäjä lataa ohjelman/asiakirjan epävarmasta lähteestä	Vältä tarpeettomia latauksia, käytä vain hyväksyttyjä kanavia ja keskeytä epäilyttävä toiminta	6) Internetin turvallisuus	Tyypilliset “käynnistävät tekijät” (linkit/lataukset) + riskienhallinnan peruslogiikka
Sähköpostin turvallinen käyttö ja virheiden ehkäisy	Luottamuksellinen tieto lähtee väärälle vastaanottajalle tai liite on epäilyttävä	Tarkista vastaanottajat ja sisältö; epäilyssä älä avaa tai jatka käsittelyä, ja ohjaa tarvittaessa ICT:lle	7) Turvallinen sähköposti	Kysely- ja tukikanavahavainnot + ohjeistuksen ydin muotoiltuna toimintamalliksi
Tietojenkalastelun tunnistaminen ja toiminta	Sähköposti/viesti ohjaa linkkiin tai pyytää tunnuksia	Tunnista merkit, älä toimi kiireessä; ilmoita viestistä ja toimi ohjeistuksen mukaisesti.	8) Tietojenkalastelu (phishing)	Korkea vaikutus ja todennäköisyys + henkilöstön epävarmuusalueet

Havaittu tarve / epävarmuus (teemataso)	**Riskitilanne (esimerkkitaso)**	**Tavoiteltu toimintamalli (tiivis)**	**Koulutusjakso**	**Perustelu ja aineistolähde (koontitaso)**
Haitta- ja kiristyshaittaohjelmien “varhainen katkaisu”	Liite/lataus käynnistää poikkeavan toiminnan	Katkaise toiminta, irrota tarvittaessa verkosta ja ilmoita viipymättä	9) Haitta- ja lunnasohjelmat	Riskin seuraukset merkittävät + nopean toiminnan arvo (vahingon rajaaminen)
Sosiaalisen manipuloinnin tilanteet ja varmistaminen	Puhelu/viesti painostaa tekemään poikkeavan toimenpiteen (esim. kiire, auktoriteetti)	Varmista pyyntö toisesta kanavasta; älä toimi kiireessä ja ota tarvittaessa tuki mukaan	10) Sosiaalinen manipulointi	Inhimilliset tekijät ja paineen vaikutus päätöksiin + käyttäjän toimintamalli keskiössä

Taulukko 1 havainnollistaa, miten tarvehavainnot muunnettiin koulutusjaksoiksi vaiheittaisen priorisoinnin kautta. Koulutuksen rakenne ei siis muodostunut yksittäisten aiheiden luetteloksi, vaan havaintojen, riskitilanteiden ja tavoiteltujen toimintamallien varaan rakentuvaksi kokonaisuudeksi. Tämä oli työn kannalta olennainen ratkaisu, koska tavoitteena ei ollut vain tunnistaa epävarmuusalueita, vaan jäsentää ne käyttäjän arjessa sovellettavaksi peruspoluksi.

Painopiste siirtyi samalla yleisestä tietoisuuden lisäämisestä niihin tilanteisiin, joissa oikea toimintamalli vähentää riskiä käytännössä. Tämän perusteella koulutuspolkua voidaan pitää toimivana ratkaisuna, koska se kokoaa hajanaiset tarpeet yhdeksi kokonaisuudeksi, jossa käyttäjän kannalta olennainen seuraava toimintatapa voidaan tunnistaa ilman tarpeetonta tulkintakuormaa.

3.8 Tietoturvallinen raportointi, aineistonhallinta ja laadunvarmistus

Työssä noudatettiin koko kehittämisprosessin ajan tiedon minimoinnin ja tietoturvallisen raportoinnin periaatteita. Aineistoa käsiteltiin vain siinä laajuudessa kuin kehittämistyön toteuttaminen edellytti, eikä raporttiin sisällytetty sellaisia

yksityiskohtia, jotka paljastaisivat organisaation sisäisiä arviointitapoja, tarkkoja tulosjakaumia tai koulutusmateriaalin kriittisiä sisältöjä. Ratkaisu on linjassa sekä yleisen tietosuoja-asetuksen (Euroopan parlamentti ja neuvosto, 2016, art. 5(1)(c), 5(1)(f), 32) että ISO/IEC 27002:2022-standardin (2022) kanssa, sillä molemmat korostavat tiedon käsittelyn lähtökohtina tarpeellisuutta, minimointia ja asianmukaista suojaamista. Laadunvarmistus toteutui sekä sisällöllisesti että teknisesti: ratkaisuja tarkennettiin HR:n ja ICT:n näkökulmista, koulutuspolkua käytiin läpi suorittajan näkökulmasta ja samalla varmistettiin, että julkiseen raporttiin jäi vain työn arvioinnin kannalta olennainen tieto. Tietoturvallinen rajaus ei siten ollut raportoinnin heikkous, vaan osa työn ammattimaista toteutustapaa.

3.9 Eettinen arviointi, tutkimusluvat ja henkilötietojen käsittely

Eettisessä tarkastelussa keskeistä oli varmistaa, että kehittämistyö tukee organisaation oppimista ilman, että seuranta tai raportointi kohdistuu tarpeettomasti yksittäisiin henkilöihin. TENK:n (2023) hyvän tieteellisen käytännön periaatteet sekä tietosuojan minimointivaatimus ohjasivat sitä, miten aineistoa kerättiin, käsiteltiin ja raportoitiin. Eettisyys näkyi tässä työssä ennen kaikkea rajauksena: kaikkea tietoa ei kerätty, eikä kaikkea kerättyä tietoa myöskään ollut tarkoituksenmukaista julkaista.

4 KOULUTUSKOKONAISUUDEN SUUNNITTELU

Koulutuskokonaisuuden suunnittelun lähtökohtana oli tehdä turvallisesta toiminnasta mahdollisimman helposti omaksuttava osa arkea. Tavoitteena ei ollut rakentaa kattavinta mahdollista sisältöpakettia, vaan muodostaa rajattu ja johdonmukainen peruspolku, joka tukee käyttäjää tavallisimmissa ja vaikutuksiltaan merkittävimmissä tilanteissa. Samalla koulutuksen tuli tukea perehdytystä, olla nykyiselle henkilöstölle kohtuullinen suorittaa sekä muodostaa organisaation näkökulmasta hallinnoitava ja ylläpidettävä rakenne. Tämä vastaa

myös käyttäjälähtöisen suunnittelun periaatteita, joiden mukaan turvallisen toiminnan on näyttäydyttävä tarkoituksenmukaisena osana käyttäjän omaa käyttöympäristöä (ISO 9241-210:2019, 2019). Myös Cabinet Office (2022) ja Merritt ym. (2024) korostavat, että käyttäjää tulee tukea selkeillä, arkeen sidotuilla toimintamalleilla.

4.1 Koulutuksen tavoitteet ja kohderyhmä

Koulutuksen kohderyhmäksi määriteltiin henkilöstö, joka käyttää digitaalisia välineitä ja käsittelee organisaation tietoja osana päivittäistä työtään. Ratkaisun tuli toimia sekä pidempään organisaatiossa olleille työntekijöille että uusille, kesä- ja kausityöntekijöille, joiden perehdytykseen liittyvä kuormitus on usein jo valmiiksi suuri. Tämän vuoksi kokonaisuuden tuli olla sisällöltään selkeä, toteutukseltaan hallittava ja myös uudelle käyttäjälle realistinen omaksua.

4.1.1 Perustason löytäminen

Perustason määrittelyssä ratkaisevaa ei ollut sisällön mahdollisimman laaja kattavuus, vaan sen tarkoituksenmukainen rajaus. Koulutuksen tuli ohjata toimintaa tavallisimmissa riskitilanteissa, mutta samalla sen oli oltava mahdollista suorittaa perehdytyksen ja työn ohessa. Liian suppea kokonaisuus olisi jättänyt epävarmuuden ennalleen, kun taas liian laaja koulutus olisi lisännyt kuormitusta ja heikentänyt käyttöönotettavuutta. Tämän vuoksi perustaso muotoiltiin kurinalaiseksi yhteiseksi poluksi, jonka tarkoituksena oli määritellä koko henkilöstölle realistinen minimitaso. Perustasoksi määriteltiin kyky tunnistaa tyypilliset riskitilanteet, toimia niissä organisaation toimintamallin mukaisesti, ymmärtää ratkaisujen taustalla oleva peruslogiikka ja löytää tarvittaessa tuki. Osa teemoista jätettiin myöhempään roolikohtaiseen syventämiseen, jotta yhteinen peruspolku säilyisi selkeänä ja hallittavana.

4.1.2 Koulutustarpeista johdetut painotukset

Tarvehavaintojen perusteella painopisteet kohdistuivat tilanteisiin, joissa väärä oletus syntyy helposti ja joissa päätöksentekoon liittyy tulkinnallista epävarmuutta. Näitä olivat esimerkiksi sähköpostin käyttö, tunnusten hallinta, mobiililaitteet, etätyö, sosiaalinen manipulointi ja tilanteet, joissa epäselvä toimintamalli voi lisätä virheen todennäköisyyttä. Valintaa tukee myös Traficomin (2026) yhteenveto vuoden 2025 keskeisistä kyberilmiöistä, jossa korostuvat huijaukset, kalastelu, organisaatioiden välillä levinneet tilimurrot sekä haavoittuvien reunalaitteiden hyväksikäyttö. Painotukset eivät siis nousseet yleisestä teoriasta, vaan siitä, missä organisaation arjessa esiintyi eniten epävarmuutta tai vaihtelua. Kiire, keskeytykset ja kognitiivinen kuormitus lisäävät taipumusta nopeisiin mutta virhealttiisiin oletuksiin, mikä tekee juuri näistä tilanteista koulutuksen kannalta keskeisiä (Kahneman, 2011). Olennaista oli myös havaita, ettei osaamisen vaihtelu selity vain työroolilla, vaan samat epävarmuudet voivat koskea sekä uusia että kokeneempia työntekijöitä. Tästä syystä koulutus rakennettiin yhteisen peruspolun varaan, jota voidaan tarvittaessa täydentää roolikohtaisesti myöhemmässä vaiheessa.

4.2 Sisältörakenne: 10 jaksoa ja niiden sisällöllinen logiikka

Koulutus jaettiin kymmeneen jaksoon, jotka etenevät perustason ymmärryksestä kohti tavallisimpia riskitilanteita ja muodostavat käyttäjälle selkeästi jäsentyvän kokonaisuuden. Jaksotus mahdollisti sen, että kokonaisuus avautuu käyttäjälle vaiheittain eikä suurena sisältömääränä kerralla. Pienempiin ja rajattuihin kokonaisuuksiin jaettu sisältö tukee työn ohessa tapahtuvaa oppimista ja helpottaa samalla koulutuksen päivittämistä ilman, että koko koulutuspolkua tarvitsee uudistaa (Bruck ym., 2012). Jaksojen aiheet ovat kyberturvallisuus, salasanat ja tunnistautuminen, mobiililaitteet, fyysinen turvallisuus, etätyö, internetin turvallinen käyttö, turvallinen sähköposti, tietojenkalastelu, haitta- ja kiristyshaittaohjelmat sekä sosiaalinen manipulointi. Rakenteessa vältettiin myös tarpeetonta päällekkäisyyttä siten, että sama perusperiaate toistuu eri konteksteissa: pysähdy, tarkista, varmista ja toimi sovitun mallin mukaisesti.

Kokonaisuutta ohjasi myös käytännön havainto siitä, että organisaatiossa ohjeistusta oli jo olemassa, mutta se ei aina tavoittanut käyttäjää oikealla hetkellä tai oikeassa muodossa. Koulutuspolun tehtäväksi tuli paitsi opettaa myös jäsentää, missä järjestyksessä asiat kannattaa kohdata ja mitä toimintatapaa käyttäjältä kulloinkin edellytetään. Siksi ohjeistuksen ydin koottiin rajatuiksi tilannelähtöisiksi jaksoiksi, joista käyttäjälle jää mieleen seuraava oikea teko. Tämä on linjassa myös koetun hyödyllisyyden ja helppokäyttöisyyden periaatteiden kanssa, jotka vaikuttavat siihen, otetaanko ratkaisu arjessa todella käyttöön (Davis, 1989; Venkatesh ym., 2003).

4.3 Koulutuspolun logiikka ja suoritusvaatimukset

Koulutuspolun eteneminen suunniteltiin käyttäjän näkökulmasta mahdollisimman ennakoitavaksi. A-Learning toimii polun kotinäkymänä, jossa käyttäjä voi seurata etenemistään, vaikka yksittäiset sisällöt suoritetaan MetaCompliance-ympäristössä. Lähtökohtana oli, että eteneminen on käyttäjälle ymmärrettävää, rakenteeltaan hallittavaa eikä aiheuta tarpeetonta muistikuormaa. Suunnittelussa painotettiin etenemisen selkeyttä, vaiheittaisuutta ja kokonaisuuden hahmottumista aiemman tutkimuskirjallisuuden ja standardin perusteella (ISO 9241-210:2019, 2019; Kupias & Peltola, 2009; Merritt ym., 2024). Myös Vuolearningin oma kuvaus tukee sen käyttöä koulutuspolun kokoavana näkymänä (Vuolearning, n.d.). Tällainen rakenne vähentää muistamisen tarvetta ja tekee palaamisesta sujuvaa myös keskeytysten jälkeen, mikä on erityisen tärkeää perehdytyksessä ja työn ohessa suoritettavassa koulutuksessa. Koulutuspolun käyttäjänäkymän teknistä toteutusta käsitellään tarkemmin luvussa 5.2, ja näkymä on esitetty kuvassa 3.

4.4 Oppimistavoitteet ja pedagogiset periaatteet

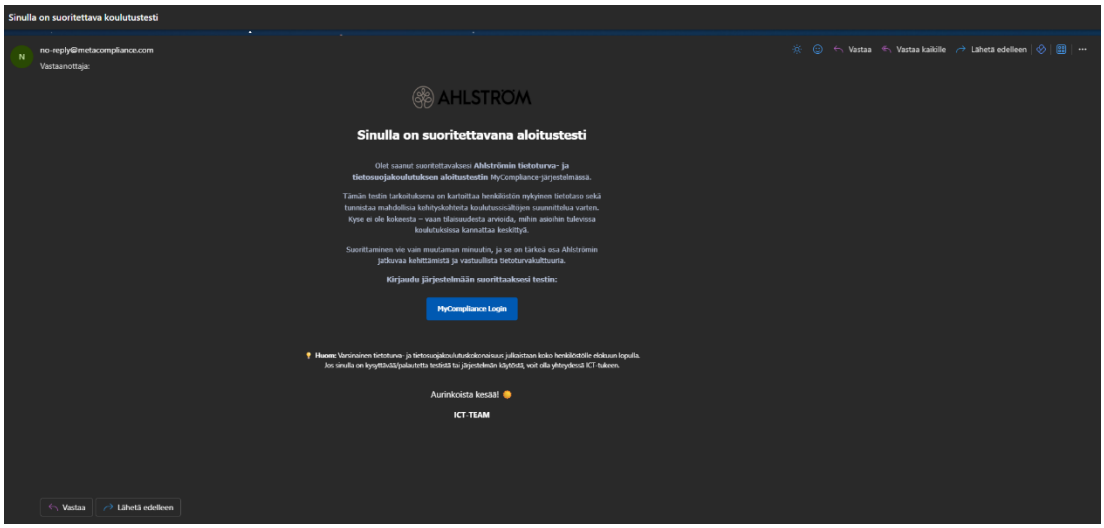
Pedagogisesti kokonaisuus rakennettiin lyhyiden, rajattujen oppimistavoitteiden varaan. Jokaisessa jaksossa pyrittiin siirtämään painopiste tiedon tunnistamisesta toiminnan kannalta olennaiseen tekemiseen, kuten pysähtymiseen, tarkistamiseen, ilmoittamiseen tai varmistamiseen. Anderson ja Krathwohl

(2001) tukevat oppimistavoitteiden jäsentämistä aktiivisten verbien ympärille, ja Hattie sekä Timperley (2007) osoittavat, että palautteen vaikuttavuus vahvistuu, kun oppija ymmärtää, mitä hänen seuraavaksi tulisi tehdä. Tavoitteena oli, että käyttäjälle jää jokaisesta jaksosta mieleen rajattu ydinsanoma ja sitä tukeva minimitoimintamalli. Aikuisoppimisen näkökulmasta juuri työn arkeen kytkeyvä ja välittömästi sovellettava sisältö on erityisen tarkoituksenmukaista (Knowles ym., 2015). Aktivoinnit ja välitön palaute valittiin aiemman tutkimuskirjallisuuden perusteella, koska ne ohjaavat käyttäjää arvioimaan tilannetta ja korjaavat väärää tulkintaa heti (Shute, 2007; Taylor & Hung, 2022; Merritt ym., 2024).

4.5 Viestintä ja käyttöönoton valmistelu

Käyttöönoton valmistelussa painotettiin viestinnän selkeyttä, matalaa aloituskynnystä ja yhden polun mallia. Ennen varsinaista käyttöönottoa oli tärkeää varmistaa, että käyttäjälle on heti selvää, mistä koulutus alkaa, missä järjestyksessä se etenee ja miten apua saa tarvittaessa. Käyttöönoton onnistuminen ei siten rakentunut vain teknisestä toimivuudesta, vaan myös siitä, että kokonaisuus näyttäytyy käyttäjälle ymmärrettävänä ja työn kannalta perusteltuna. Varsinaisessa käyttöönotossa viestinnän tehtävä oli täsmentää, miksi koulutus tehdään, miten se suoritetaan, mitä se käytännössä edellyttää ja mistä saa apua. Tällainen viestintä kytkee koulutuksen suoraan työn arkeen ja vähentää epävarmuutta jo ennen ensimmäistä suoritusta (Kotter, 1996; Merritt ym., 2024).

Kuva 1. Aloitustestin kutsuviesti sähköpostissa (linkki MetaCompliance-ympäristöön, MyCompliance).



Kuva: Tekijä, kuvakaappaus sähköpostiviestistä, 2025 (tekijän muokkaama).

Esimerkkikutsu koulutuspolkuun lähetetystä viestistä on liitteessä 2.

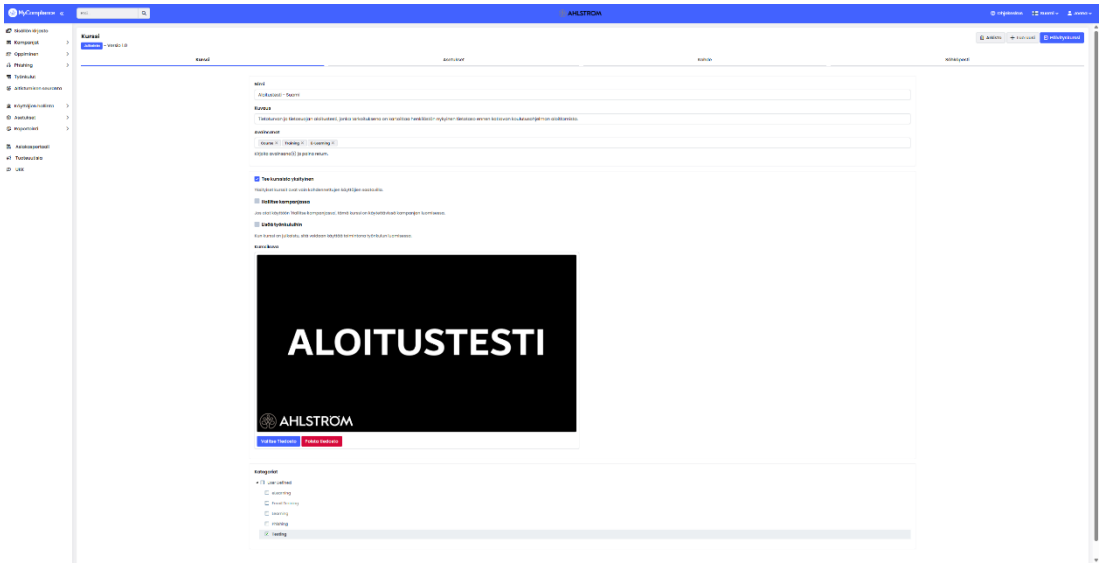
5 TEKNINEN TOTEUTUS JA OPPIMISYMPÄRISTÖ

Teknisen toteutuksen lähtökohtana oli hyödyntää organisaatiossa jo käytössä olevia ympäristöjä siten, että koulutuspolusta muodostuu käyttäjälle mahdollisimman helposti jäsentyvä kokonaisuus. Ratkaisun toimivuus ei riippunut vain siitä, missä ympäristössä sisältö suoritetaan, vaan siitä, miten kokonaisuuden eri osat kytkeytyvät toisiinsa ja ohjaavat käyttäjää eteenpäin. Tavoitteena ei ollut rakentaa uutta järjestelmää, vaan yhdistää sisällön suorittaminen, seuranta ja perehdytyskytkentä hallittavaksi malliksi. Tämä on yhdenmukaista myös sen kanssa, että turvallisuuteen liittyvien käytäntöjen tulee olla organisaation rakenteisiin kytkeytyviä, hallittavia ja käyttäjälle selkeitä (ISO/IEC 27001:2022, 2022; Joint Task Force, 2020; NIST, 2024).

5.1 MetaCompliance koulutussisällön toteutusalustana

MetaCompliance valittiin koulutussisällön toteutusalustaksi, koska se mahdollistaa lyhyiden moduulien, arviointien, aktivointien ja tietoturvakoulutukseen soveltuvan sisältörakenteen yhdistämisen samaan ympäristöön (MetaCompliance, n.d.). Tässä työssä MetaCompliancea ei kuitenkaan tarkasteltu irrallisena koulutuskanavana, vaan osana laajempaa käyttäjäpolkua, jossa teknine toteutus jäsentää kokonaisuutta eikä lisää hajanaisuutta. Kehittämistyön kannalta tärkeää oli myös mahdollisuus rakentaa sisältöjä elementeistä, jolloin yksittäisiä jaksoja voidaan myöhemmin päivittää kohdennetusti ilman koko kokonaisuuden uusimista. Tämä vastaa lyhyiden, helposti päivitettävien ja käyttäjää aktivoivien sisältöjen periaatetta (ENISA, 2025; Merritt ym., 2024).

Kuva 2. Aloitustestin määritys MetaCompliance-ympäristössä (kurssin asetukset).



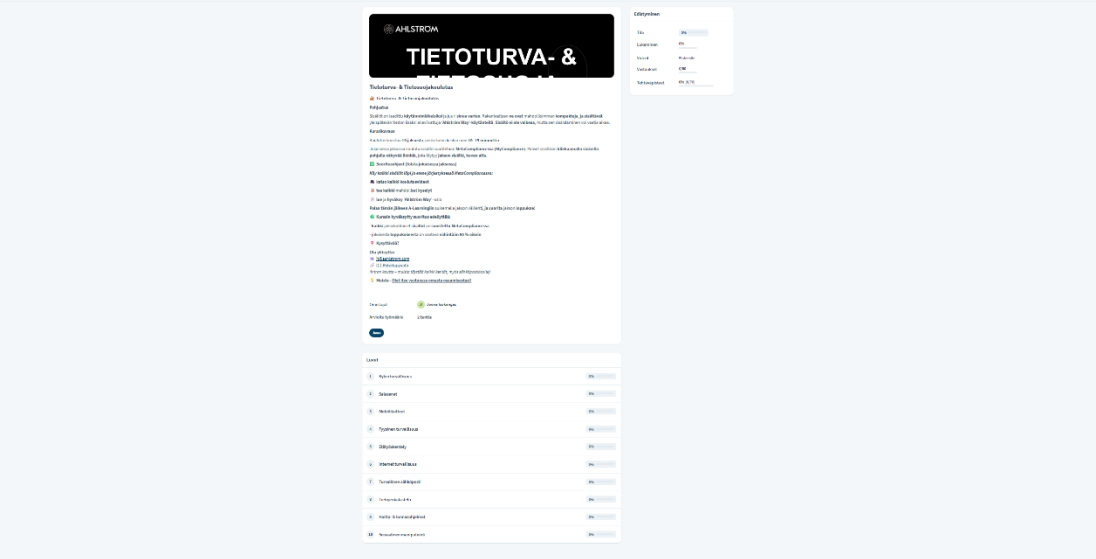
Kuva: Tekijä, kuvakaappaus MetaCompliance-ympäristöstä, 2025 (tekijän muokkaama).

Rajattu esimerkki MyCompliance-ympäristössä käytetystä jakson elementtirakenteesta on esitetty liitteessä 3.

5.2 A-Learning (Vuolearning) koulutuspohjan ja seurannan ympäristönä

A-Learningin rooli oli toimia koulutuspolun kotinäkymänä ja käyttäjän etenemisen selkeänä ohjauspintana. Ratkaisun vahvuus oli siinä, että käyttäjä näkee yhdestä paikasta, missä vaiheessa polkua hän on, mitä seuraavaksi tehdään ja miten kokonaisuus etenee, vaikka yksittäiset sisällöt suoritetaan toisessa ympäristössä. Tavoitteena oli, että käyttäjä hahmottaa etenemisen helposti, pystyy palaamaan polkuun keskeytysten jälkeen ja tunnistaa vaivatta seuraavan vaiheen, mikä tukee kokonaisuuden sujuvaa omaksumista perehdytyksessä (ISO 9241-210:2019, 2019; Kupias & Peltola, 2009; Merritt ym., 2024). Kuvassa 3 esitetään koulutuspolun käyttäjänäkymä A-Learningissa.

Kuva 3. Koulutuspolun käyttäjänäkymä A-Learningissa (10 jaksoa).



Kuva: Tekijä, kuvakaappaus A-Learning (Vuolearning) -oppimisympäristöstä, 2025 (tekijän muokkaama).

5.3 Seuranta, roolit ja raportoinnin käytännöt (HR / ICT)

Seuranta ja raportointi rakennettiin palvelemaan kolmea tarkoitusta: koulutuksen toteutumisen varmistamista, käyttäjien etenemisen tukemista ja kokonaisuuden kehittämistä. HR:n rooli painottuu koulutuksen kytkemiseen perehdytykseen ja suoritusten yleistasoiseen hallintaan, kun taas ICT:n tehtävänä on varmistaa, että koulutuksen sisältö ja poikkeamatilanteiden toimintamallit

vastaavat organisaation käytäntöjä. Tämä vastaa Joint Task Forcen (2020) näkemystä siitä, että seurannan tulee tukea turvallisuuden johtamista eikä jäädä irralliseksi mittaamisen välineeksi. ENISA (2017) tarkastelee tietoturvakulttuurin kehittämistä jatkuvana organisaatiotason toimintana, ja myös Merritt ym. (2024) painottavat, että seurannan tulisi tukea käyttäjää ja kehittämistyötä sen sijaan, että se lisäisi kitkaa. Seurantatiedon rajaaminen käyttötarkoituksen kannalta tarpeelliseen on samalla linjassa yleisen tietosuoja-asetuksen käyttötarkoitussidonnaisuuden ja tietojen minimoinnin periaatteiden kanssa (Euroopan parlamentti ja neuvosto, 2016, art. 5(1)(b), 5(1)(c)).

Raportoinnissa pidettiin tietoisesti kiinni tietoturvallisesta rajauksesta: seurannan logiikka ja vastuut kuvataan julkisesti, mutta yksityiskohtainen tulosdata rajataan organisaation sisäiseen käyttöön. Näin seuranta tukee toimintaa ja kehittämistä ilman, että se muuttuu henkilötason arvottamiseksi (NIST, 2010).

5.4 Pilotointi ja sisäinen testaus (käyttöönoton varmistaminen)

Pilotoinnin tarkoitus oli varmistaa, että koulutus toimii aidosti käyttäjän näkökulmasta ennen laajempaa käyttöönottoa. Testauksessa tarkasteltiin siirtymiä ympäristöjen välillä, suorituslogiikan selkeyttä, arviointien toimivuutta, seurannan koontinäkymää sekä sitä, onko käyttäjälle heti selvää, mitä tehdä seuraavaksi ja mistä apua saa. Käyttäjätestaus kohdistettiin juuri siirtymiin, selkeyteen ja käytön sujuvuuteen, mikä on linjassa käyttäjälähtöisen suunnittelun periaatteiden kanssa (ISO 9241-210:2019, 2019).

Pilottivaiheeseen osallistui myös kesä- ja kausityöntekijöitä, mikä vahvisti arvioinnin kattavuutta tuomalla esiin ne kohdat, joissa ohjeistus nojasi liiaksi organisaation hiljaiseen tietoon. Keskeinen havainto oli, että kitka syntyy usein pienistä asioista, jotka nostavat aloituskynnystä ja heikentävät käyttäjän tilannehahmotusta: otsikosta, etenemisjärjestyksestä, näkyvästä painikkeesta tai siitä, ettei tukikanava avaudu oikealla hetkellä. Tämän vuoksi koulutuksen käytettävyyttä ei tarkasteltu erillisenä lisätekijänä, vaan osana tietoturvaa.

Pilotoinnin perusteella koulutuksen kieltä, etenemislogiikkaa ja viestintää täsmennettiin kohdennetusti, ja keskeiset muutokset on koottu taulukkoon 2.

Taulukko 2. Pilotoinnin muutosloki (koontitaso)

Tarkistuskohde	**Havainto (koontitaso)**	**Korjaustoimi / täsmennys**	**Miksi muutos oli olennainen**
Polun aloitus ja jatkaminen	Keskeytyksen jälkeen seuraava askel ei ollut käyttäjälle täysin itsestään selvä	Lisättiin täsmällinen ohjaus takaisin polkuun ja yhdenmukaistettiin etenemisen näkyvyys	Vähentää keskeytyksiä ja madaltaa kynnystä jatkaa
Jaksojen löydettävyys	Oikea jakso ei löytynyt kaikissa tilanteissa nopeasti	Selkeytettiin nimeämistä ja sijoittelua sekä lisättiin tarvittaessa suoria linkkejä	Vähentää järjestelmän käytön kitkaa ja tukipyyntöjä
Hyväksymiskriteerit	Hyväksymisen logiikka tulkittiin eri tavoin eri jaksoissa	Yhdenmukaistettiin hyväksymisen ehdot ja tarkistettiin läpivienti	Parantaa oikeudenmukaisuutta ja vähentää epävarmuutta
Raportointinäkymä (HR/ICT)	Koontitason seurannasta puuttui joitakin ohjauksen kannalta olennaisia näkymiä	Täsmennettiin koontitaso ja roolirajaukset; rajattiin pois tarpeettomat yksityiskohdat	Mahdollistaa ohjauksen ilman yksityiskohtaista henkilötason valvontaa
Ohjeistusten linkitys	Kaikissa kohdissa ei ollut yksiselitteistä polkua	Lisättiin ohjaus intranet-ohjeeseen niissä	Yhdistää koulutuksen ja arjen

Tarkis-tuskohde	Havainto (koontitaso)	Korjaustoimi / täsmennys	Miksi muutos oli olennainen
	alkuperäiseen ohjeeseen	kohdissa, joissa käyttäjä tarvitsee lisätietoa	ohjeistuksen toimivaksi kokonaisuudeksi

Taulukko 2 osoittaa, että pilotoinnissa esiin nousseet täsmennystarpeet liittyivät ennen kaikkea koulutuksen käytettävyyteen, etenemisen selkeyteen ja ohjeistusten saavutettavuuteen. Havainnot eivät siten koskeneet vain yksittäisiä teknisiä yksityiskohtia, vaan sitä, kuinka johdonmukaisesti käyttäjä hahmottaa polun, hyväksymisen ehdot ja tuen löytämisen eri vaiheissa.

Pilotoinnin perusteella vahvistui näkemys siitä, että käytettävyys on myös tietoturvakoulutuksen toimivuuden ehto. Jos eteneminen, jaksojen löydettävyys tai ohjeistusten linkittyminen jää epäselväksi, myös oikean toimintatavan omaksuminen vaikeutuu. Tämän vuoksi taulukossa kuvatut muutokset olivat koulutuksen käytännön toimivuuden kannalta olennaisia, eivät vain teknisiä tarkennuksia.

6 YLLÄPITO, JATKOKEHITYS JA RISKIENHALLINTA

Pelkkä käyttöönotto ei vielä tee kokonaisuudesta kestävää ratkaisua. Jotta koulutuspolku pysyy hyödyllisenä, sen ylläpidolle on oltava selkeä omistajuus, toimiva palautemekanismi, kohtuullinen tarkastelurytmi ja toimintamalli sille, miten muuttuva uhkakenttä sekä organisaation käytännöt huomioidaan koulutussisällöissä. Tässä luvussa koulutusta tarkastellaan elinkaaren näkökulmasta: miten kokonaisuus pidetään toimivana myös ensimmäisen toteutuskierroksen jälkeen ja miten sitä kehitetään hallitusti ilman, että ratkaisu alkaa

pirstoutua. ISO/IEC 27001:2022 (2022) ja Joint Task Force (2020) korostavat jatkuvan parantamisen ja hallittavuuden merkitystä osana turvallisuuden johtamista. Sama ajatus ulottuu myös käyttäjille suunnattuun koulutukseen: Merritt ym. (2024) painottavat, että kokonaisuuden on pysyttävä ajan myötä selkeänä, käyttökelpoisena ja arjessa toimivana.

6.1 Omistajuus ja vastuunjako (HR ja ICT)

Ylläpidon perusedellytys on selkeästi määritelty ja dokumentoitu omistajuus. Tässä työssä vastuunjako jäsennettiin siten, että HR vastaa koulutuksesta perehdytys- ja koulutusprosessin näkökulmasta, kun taas ICT vastaa sisällön ajantasaisuudesta, poikkeamatilanteiden toimintamalleista ja tietoturvan asiantuntijanäkökulmasta. Jaettu vastuu on tarkoituksenmukainen, koska koulutus on samanaikaisesti henkilöstön oppimisen väline ja osa organisaation turvallista toimintatapaa. Turvallisuuden johtamisen näkökulmasta vastuiden selkeys on keskeinen osa hallintajärjestelmää (ISO/IEC 27001:2022, 2022). Joint Task Force (2020) korostaa organisaation vastuiden ja toimintatapojen selkeyttä, ja Merritt ym. (2024) ulottavat saman periaatteen myös käyttäjäkoulutuksen ylläpitoon, jossa omistajuuden tulee olla selkeä ja jatkuva. Olennaista on, ettei koulutus jää yhden henkilön varaan, vaan omistajuus ja vastuut säilyvät toimivina myös henkilövaihdosten yli.

6.2 Päivitystarpeen tunnistaminen ja ylläpitokäytännöt

Päivitystarpeita ei tule tarkastella vain kalenterin perusteella, vaan niiden on noustava sekä toimintaympäristön muutoksista että käyttäjiltä ja ylläpidosta saaduista signaaleista. Koulutuksen rungon tulee pysyä riittävän vakaana, mutta yksittäisiä jaksoja on voitava päivittää nopeasti, jos uhkakenttä, työvälineet, organisaation käytännöt tai palautteessa toistuvat epäselvyydet sitä edellyttävät. Tämä vastaa myös jatkuvan arvioinnin ja parantamisen periaatetta, jota Joint Task Force (2020) pitää osana turvallisuustoimintojen hallintaa. Samalla ENISA (2025) ja Merritt ym. (2024) korostavat, että loppukäyttäjille suunnatun koulutuksen on mukauduttava muuttuvaan uhkakenttään ja

havaittuihin epäselvyyksiin ilman, että perusrakenne menettää selkeyttään. Käytännöllinen ylläpitomalli perustuu siksi kevyisiin mutta säännöllisiin tarkastelupisteisiin, joissa arvioidaan, onko sisältö edelleen ajantasainen, ymmärrettävä ja työn arkeen sopiva.

6.3 Palautekanavat ja kehityssykli (A-Learning, HR, ICT/tiketit)

Palautekanavan tehtävänä ei ole kerätä mahdollisimman paljon hajanaisia havaintoja, vaan tuottaa kehittämisen kannalta käyttökelpoista tietoa. Tässä ylläpitomallissa tietoa voi kertyä useaa reittiä: oppimisympäristön kautta, HR:n perehdytyshavaintojen pohjalta sekä ICT:n tukipyyntöjen ja poikkeamatilanteiden yhteydessä. Tämä vastaa myös Hattien ja Timperleyn (2007) näkemystä palautteesta toiminnan ohjaamisen välineenä, ei vain jälkikäteisenä arviointina. Merritt ym. (2024) korostavat tietoturvakoulutuksessa käyttäjän näkökulmasta samaa periaatetta, ja Spitzner (2023) tarkastelee turvallisuustietoisuuden kehittämistä jatkuvana ohjelmana, jossa havainnot ja palaute kytkeytyvät samaan ylläpitosykliin. Näin havaintotieto tulee osaksi yhteistä kehityssykliä eikä jää yksittäisiksi huomioiksi. Kun palaute liitetään osaksi sovittua omistajuusmallia, siitä tulee osa ylläpitoa eikä vain käyttöönoton jälkeinen lisä.

6.4 Riskienhallinta koulutuskokonaisuuden elinkaaressa

Koulutuskokonaisuuden elinkaaren riskit liittyvät harvoin vain sisältöön. Käytännössä riskejä syntyy myös siitä, että koulutus vanhenee, omistajuus hämärtyy, käyttäjäpolkuun kertyy kitkaa tai seuranta muuttuu liian raskaaksi. Riskienhallinnan näkökulmasta huomio kohdistuu tällöin vaikutuksiin, todennäköisyyksiin ja tarkoituksenmukaisiin käsittelytapoihin, kuten ISO/IEC 27005:2022 (2022) jäsentää. Joint Task Force Transformation Initiative (2012) korostaa vastaavasti turvallisuustyössä hallittujen ja jatkuvien toimintamallien merkitystä, ja Merritt ym. (2024) ulottavat saman ajatuksen käyttäjille suunnattuun koulutukseen painottamalla, että kokonaisuuden on oltava riittävän kevyt, ylläpidettävä ja käytännössä toteutuva. Tässä työssä riskienhallinta tarkoittaa ennen kaikkea hallittavuutta: sisältöjä on voitava päivittää, vastuut on

määriteltävä selkeästi ja kokonaisuuden on pysyttävä riittävän kevyenä, jotta koulutus säilyy arjessa käytettävänä. Hyvä koulutus ei siis ole vain sisällöllisesti toimiva, vaan myös sellainen, joka kestää muutoksia ja ylläpitoa ilman, että sen toimivuus alkaa heikentyä.

6.5 Tietoturvallinen raportointi ja julkisen opinnäytetyön rajaus

Raportoinnissa noudatettiin samaa periaatetta kuin työn muussakin rajauksessa: julkisen version tuli olla arvioitava, mutta samalla tietoturvan kannalta tarkoituksenmukaisesti rajattu. Tämä vastaa tietojen minimoinnin ja asianmukaisen suojauksen periaatteita (Euroopan parlamentti ja neuvosto, 2016, art. 5(1)(c), 5(1)(f), 32). Samaa linjaa tukevat myös ISO/IEC 27002:2022 (2022) sekä Whitman ja Mattord (2016), jotka korostavat, että tiedon käsittely ja julkaiseminen on rajattava tarpeelliseen ja että turvallisuustyön raportoinnin tulee olla samanaikaisesti hyödyllistä ja hallitusti rajattua. Julkisessa versiossa voidaan siksi kuvata koulutuksen rakenne, periaatteet, roolit ja keskeiset johtopäätökset, mutta ei sellaisia yksityiskohtia, jotka helpottaisivat organisaation toimintatapojen väärinkäyttöä tai tekisivät sisäisestä arviointilogiikasta liian läpinäkyvän. Tämän vuoksi yksityiskohtainen seuranta- ja kehitystieto rajattiin organisaation sisäiseen käyttöön, jossa sitä käsitellään vain käyttötarkoituksen kannalta tarpeellisessa laajuudessa (Euroopan parlamentti ja neuvosto, 2016, art. 5(1)(b), 5(1)(c)).

7 JOHTOPÄÄTÖKSET

Tämän työn keskeinen johtopäätös on, että tietoturva- ja tietosuojakoulutuksen vaikuttavuus perustuu ennen kaikkea siihen, miten luontevasti koulutus kytkeytyy käyttäjän arkeen. Pelkkä oikea sisältö ei riitä, jos eteneminen on epäselvää, tukikanavat jäävät näkymättömiksi tai koulutus näyttäytyy organisaatiossa irrallisena velvoitteena. Kun koulutus sidotaan perehdytykseen, jäsennetään käyttäjälle selkeäksi poluksi ja tehdään organisaatiolle ylläpidettäväksi

kokonaisuudeksi, siitä tulee todennäköisemmin pysyvä osa toimintatapaa eikä vain kertaluonteinen kampanja.

7.1 Vastaukset kehittämiskysymyksiin

Kehittämiskysymyksiin vastaaminen tiivistyy neljään kokonaisuuteen: koulutustarpeen tunnistamiseen, koulutusrakenteen valintaan, tekniseen toteutukseen ja palveluhenkisen toimintamallin täsmentämiseen. Näitä kaikkia yhdisti sama perusajatus: ratkaisun piti toimia yhtä aikaa käyttäjän näkökulmasta sujuvasti ja organisaation näkökulmasta hallittavasti.

7.1.1 Miten koulutustarve tunnistettiin ja mihin se perustui?

Koulutustarve tunnistettiin yhdistämällä alkukysely, HR:n ja ICT:n käytännön havainnot sekä toteutuksen aikana kertynyt kehittämisaineisto. Näin voitiin osoittaa, ettei keskeinen puute ollut yksittäinen tietovaje, vaan toimintatapojen vaihtelu ja tulkinnallinen epävarmuus tilanteissa, joissa päätös on tehtävä nopeasti. Tarvekartoituksen vahvuus oli siinä, että se siirsi huomion yleisestä tietoisuuden lisäämisestä niihin käytännön tilanteisiin, joissa pysähtyminen, varmistaminen ja yhteinen toimintamalli ratkaisevat eniten.

7.1.2 Millainen koulutuskokonaisuus suunniteltiin ja miksi?

Suunniteltu koulutuskokonaisuus on kymmenen jakson modulaarinen polku, jossa yhteinen perustaso yhdistyy työtilanteisiin sidottuihin minimitoimintamalleihin. Tällainen rakenne osoittautui perustelluksi, koska sen avulla koulutus pysyy perehdytyksessä kohtuullisena, ylläpidossa hallittavana ja käyttäjälle riittävän selkeänä. Samalla rakenne jättää tilaa myöhemmälle syventämiselle ilman, että peruspolku hajoaa liian varhain erillisiksi ja raskaiksi kokonaisuuksiksi.

7.1.3 Miten koulutus toteutettiin teknisesti ja miten seurattavuus varmistettiin?

Tekninen toteutus rakennettiin mallilla, jossa MetaCompliance toimii sisältöjen ja osaamisen varmistamisen ympäristönä ja A-Learning kokoaa ne käyttäjälle yhdeksi selkeäksi poluksi. Tällä työnjaolla käyttäjäkokemus säilyi selkeänä, mutta organisaatio sai silti riittävän seurattavuuden koulutuksen toteutumiseen. Seuranta rakennettiin tietoisesti ohjaavaksi eikä kontrolloivaksi: sen tehtävänä on tukea etenemistä, tunnistaa kitkakohdat ja tuottaa ylläpidolle päätöksenteon kannalta hyödyllistä tietoa.

7.1.4 Miten koulutuksessa näkyy palveluhenkinen, käyttäjää tukeva lähestymistapa?

Palveluhenkinen lähestymistapa näkyy siinä, että koulutus ei kehystä käyttäjää riskiksi vaan tuen tarvitsijaksi ja turvallisen toiminnan mahdollistajaksi. Käyttäjälle täsmennetään, mitä häneltä odotetaan, mistä tukea on saatavissa ja miten toimia silloin, kun oma varmuus ei riitä. Pidän tätä tärkeänä, koska turvallinen toiminta ei vahvistu pelkällä ohjeistuksella, vaan vasta silloin, kun varmistaminen on aidosti sallittua ja käytännössä helppoa.

7.2 Hyödyt ja rajoitteet

Kokonaisuuden keskeinen hyöty on siinä, että se tuotti organisaation käyttöön valmiin, käyttöönotettavan ja ylläpidettävän koulutusmallin. Samalla on kuitenkin tunnistettava, että työn tulkintaa rajaavat aineiston luonne, julkisen raportoinnin tietoturvasyyt ja se, että pitkän aikavälin vaikutuksia voidaan arvioida luotettavasti vasta käyttöönoton jälkeen. Näistä rajoitteista huolimatta pidän työn tulosta vahvana, koska ratkaisu perustuu todelliseen tarpeeseen ja sen toimivuutta tarkennettiin jo kehittämisvaiheessa.

7.2.1 Keskeiset hyödyt organisaatiolle ja käyttäjälle

Organisaatiolle suurin hyöty on se, että koulutus muuttuu irrallisesta materiaalista johdettavaksi toimintamalliksi. Käyttäjän näkökulmasta hyöty näyttäytyy selkeytenä: odotukset, eteneminen ja tukikanavat ovat näkyvissä samassa kokonaisuudessa. Tämä vähentää tilanteita, joissa toiminta jää yksittäisen työntekijän oman tulkinnan, muistin tai oma-aloitteisuuden varaan.

Pidän merkittävänä myös sitä, että ratkaisu sidottiin suoraan perehdytykseen ja ylläpitoon. Tämä tekee kokonaisuudesta uskottavamman kuin kertaluonteinen koulutuskampanja. Käyttäjän kannalta hyöty ei ole vain tiedon lisääntyminen, vaan se, että epäselvään tilanteeseen on olemassa tunnistettava toimintamalli ja selkeä tukikanava, josta varmistus saadaan.

7.2.2 Työn rajoitteet ja niiden vaikutus tulkintaan

Työn keskeiset rajoitteet liittyvät aineiston luonteeseen ja julkisen raportoinnin rajauksiin. Alkukysely soveltui hyvin koulutustarpeen jäsentämiseen, mutta sitä ei ole tarkoituksenmukaista tulkita tarkaksi mittariksi yksilö- tai ryhmätasolla. Sen tehtävänä oli ennen kaikkea tunnistaa epävarmuusalueita ja ohjata kehittämistyön suuntaamista, ei tuottaa täsmällistä vertailutietoa eri vastaajaryhmistä.

Toinen rajoite liittyy raportin tietoisesti tiivistettyyn muotoon sekä julkisen opinnäytetyön ja käytännön turvallisuustyön väliseen suhteeseen. Arviointikysymyksiä, tulosjakaumia ja organisaation sisäisiä riskikohtia ei ole tarkoituksenmukaista avata yksityiskohtaisesti julkisessa raportissa, koska tällainen tarkkuustaso voisi paljastaa turvallisuustyön kannalta tarpeettomia yksityiskohtia. Tästä syystä työssä valittu koontitasoinen raportointi ei ole vain esitystekninen ratkaisu, vaan osa työn tietoturvallista toteutusta. Olennaista ei tällöin ole näkyvän taustamateriaalin määrä, vaan se, ovatko tehdyt ratkaisut perusteltuja, johdonmukaisia ja käytännössä toimivia. Tämän vuoksi kokonaisuuden vahvuutta on luontevaa arvioida ennen kaikkea sen selkeyden, käyttöönotettavuuden ja organisaation arkeen kiinnittyvän toteutuslogiikan kautta.

7.2.3 Kehittämistyö ja oma oppiminen

Oman oppimiseni kannalta tärkein havainto oli, että toimiva tietoturvakoulutus syntyy vasta silloin, kun teoria, käytännön työtilanteet ja organisaation toimintamallit muodostavat käyttäjän näkökulmasta toimivan kokonaisuuden. Työn aikana jouduin luopumaan ajatuksesta, että lisäohjeistus yksin ratkaisisi ongelman, sillä vähitellen kävi selväksi, että ratkaisevaa on se, miten helposti käyttäjä tunnistaa tilanteen, löytää seuraavan oikean teon, säilyttää päätöksentekovalmiutensa ja uskaltaa varmistaa silloin, kun oma varmuus ei riitä. Tässä mielessä koulutuksen vaikuttavuus on yhtä paljon käyttäjän kognitiivisen kuormituksen hallintaa kuin sisällöllistä oikeellisuutta.

Työn vaativin mutta samalla opettavaisin osa oli tasapainottaa samaan ratkaisuun kolme näkökulmaa: tietoturvavaatimusten riittävä jämäkkyys, käyttäjän kuormituksen kohtuullisuus ja organisaation käytännön hallittavuus. Liian yleinen koulutus ei ohjaa toimintaa, mutta liian yksityiskohtainen koulutus ei enää elä työarjessa eikä tue päätöksentekoa silloin, kun aikaa ja huomiota on vähän. Työn aikana vahvistui ymmärrys siitä, että toimiva ratkaisu syntyy useammin kurinalaisesta rajaamisesta ja priorisoinnista kuin sisällön kasvattamisesta. Näin kehittämistyö näyttäytyi enemmän käyttökelpoisen kokonaisuuden jäsentämisenä kuin pelkkänä sisällöntuotantona tai oikeiden asioiden listaamisena.

Kehittämisprosessin aikana täsmentyi myös oma käsitykseni siitä, mikä koulutuksessa on lopulta vaikeinta. Alkuvaiheessa painotin enemmän sisältöjen kattavuutta ja oikeellisuutta, mutta työn edetessä yhä selvemmin korostuivat rakenteen selkeys, oikea-aikainen ohjaus ja mahdollisuus varmistaa epäselvä tilanne matalalla kynnyksellä. Tämä vahvisti näkemystä siitä, että toimiva tietoturva- ja tietosuojakoulutus ei ole vain tiedon välittämistä, vaan myös käyttäjän päätöksenteon tukemista.

7.3 Jatkotoimenpiteet ja suositukset

Työn perusteella koulutuspolun seuraava kehitysvaihe ei ole kokonaisuuden uudelleenrakentaminen, vaan hallittu vakiinnuttaminen. Olennaisinta on varmistaa selkeästi määritelty omistajuus, käytännössä toimiva palautesykli, kevyt mutta riittävä seuranta sekä rytmi, jolla sisältöjä tarkastetaan. Kun nämä perusrakenteet ovat kunnossa, koulutus voi kehittyä vaiheittain ilman, että sen peruspolku hajoaa tai menettää hallittavuuttaan.

7.3.1 Ylläpito ja päivitysrytmi

Ylläpidossa kannattaa välttää kahta ääripäätä: liian tiheää, käyttäjää kuormittavaa muokkaamista ja toisaalta liian hidasta päivityssykliä, jossa sisältö alkaa huomaamatta menettää ajantasaisuuttaan. Käytännöllinen ratkaisu on säännöllinen, ennalta sovittu tarkastelu, jota täydennetään tarvittaessa nopeilla kohdennetuilla päivityksillä. Näin koulutuksen runko säilyy vakaana, mutta olennaiset muutokset saadaan tuotua käyttäjille riittävän ajoissa.

7.3.2 Omistajuuden ja roolien täsmentäminen

Omistajuus kannattaa määritellä selkeästi sekä prosessissa että arjen käytännöissä. Kun HR:n ja ICT:n roolit määritellään selkeästi, koulutus ei jää kahden vastuun väliin. Myös käyttäjän näkökulmasta on tärkeää, ettei polku näyttäydy nimettömänä järjestelmäkokonaisuutena, vaan siihen liittyvät ihmiset, vastuut ja tukikanavat ovat tunnistettavia. Tämä lisää koulutuksen uskottavuutta, vahvistaa toiminnan psykologista turvallisuutta ja helpottaa ylläpidon jatkuvuutta henkilövaihdoksissa.

7.3.3 Palautekanava osaksi kokonaisuutta

Palautekanavan tulisi olla koulutuksen normaali osa eikä erillinen lisätoiminto. Kun käyttäjällä on helppo tapa kertoa epäselvistä kohdista ja palaute käsitellään osana ylläpitoa, koulutus pysyy paremmin kiinni todellisissa

käyttötilanteissa. Samalla palaute auttaa tunnistamaan kohdat, joissa sisältö on sinänsä oikea, mutta esitystapa liian raskas tai tulkinnanvarainen.

7.3.4 Seuranta käytännön ohjaukseen, ei numeron vuoksi

Seurannassa olennaista ei ole mahdollisimman suuri mittarimäärä vaan se, tuottaako seuranta päätöksenteon kannalta käyttökelpoista tietoa. Paras seuranta ohjaa tukemaan käyttäjiä, tunnistaa koulutuspolun kitkakohdat ja auttaa priorisoimaan päivityksiä. Jos seuranta muuttuu numerokeskeiseksi tai liian yksityiskohtaiseksi, se voi alkaa syödä juuri sitä luottamusta ja käytännöllisyyttä, jota koulutuksella tavoitellaan.

7.3.5 Onnistumisen arviointi käytännössä

Onnistumista voidaan arvioida kolmen käytännöllisen kysymyksen avulla: toteutuuko koulutus suunnitellusti, onko sen suorittaminen käyttäjälle aidosti sujuvaa ja tuottaako se ylläpidolle riittävän kuvan siitä, mitä tulisi kehittää seuraavaksi. Näiden kysymysten etuna on, että ne sitovat arvioinnin käytännön toimintaan eivätkä jätä sitä irralliseksi mittaamiseksi. Koulutus on onnistunut silloin, kun se ei jää rakenteellisesti kesken, käyttäjä ei joudu arvailemaan etenemistään ja kehitystarpeet voidaan tunnistaa ilman yliraskasta seurantaa.

7.3.6 Roolikohtainen syventäminen myöhemmässä vaiheessa

Yhteinen peruspolku kannattaa säilyttää koulutuksen ytimenä, mutta sen rinnalle on järkevää rakentaa myöhemmin roolikohtaisia syventäviä osuuksia. Tämä on perusteltua erityisesti niissä tehtävissä, joissa altistus, vastuu tai käsiteltävän tiedon luonne poikkeaa olennaisesti peruskäyttäjästä. Syventämisen tulee kuitenkin tapahtua vasta sen jälkeen, kun yhteinen perustaso toimii luotettavasti, jotta kokonaisuus ei kasva tarpeettoman raskaaksi liian varhain.

7.3.7 Palveluhenkinen sävy pidettävä tietoisena valintana

Palveluhenkinen sävy ei säily itsestään, vaan sitä on vaalittava tietoisesti myös käyttöönoton jälkeen. Jos viestintä, muistutukset ja tukikanavat alkavat korostaa vain valvontaa, koulutuksen perusajatus heikkenee nopeasti. Käyttäjän näkökulmasta sävyn merkitys on suuri: sama sisältö voi tuntua joko työtä tukevan tai kuormitusta lisäävän riippuen siitä, miten se kehystetään. Siksi palveluhenkisyys kannattaa nähdä ylläpidettävänä laatutekijänä, ei pelkkänä alkuvaiheen viestintäratkaisuna.

7.4 Yhteenveto

Työn tuloksena syntyi organisaation käyttöön rakennettu tietoturva- ja tietosuojakoulutuksen kokonaisuus, jonka keskeinen vahvuus on käytännöllisyydessä. Sen arvo ei perustu vain siihen, että se käsittelee oikeita teemoja, vaan siihen, että sisältö, koulutuspolku, seuranta ja käyttäjän tukeminen on koottu hallittavaksi kokonaisuudeksi. Koulutus on sidottu perehdytykseen, tehty käyttäjälle ymmärrettäväksi ja rakennettu ylläpidettäväksi, joten kyse ei ole vain opinnäytetyön tuotoksesta vaan toimintamallista, joka voi jäädä elämään organisaation arkeen.

Työ vahvisti samalla käsitystäni siitä, että tietoturva- ja tietosuojakoulutuksen keskeinen haaste ei yleensä ole tiedon puute, vaan tiedon muuttaminen arjen valinnoiksi. Yritysympäristössä koulutus on uskottava vasta silloin, kun se jäsentää oikean toimintatavan käyttäjälle ymmärrettäväksi, tekee varmistamisesta luontevaa ja tuesta helposti saavutettavaa. Koulutuksen arvo mitataan siinä hetkessä, kun käyttäjä pysähtyy epäselvässä tilanteessa, tunnistaa riskin ja tietää, miten toimia turvallisesti. Siksi onnistunut koulutus ei ole organisaation laajin mahdollinen sisältöpaketti, vaan sellainen, joka karsii käyttäjän kannalta turhaa monimutkaisuutta ja jättää näkyviin toiminnan kannalta olennaisen.

Yritysympäristössä toimiva tietoturva- ja tietosuojakoulutus on enemmän kuin sisältökokonaisuus. Sen on oltava käyttäjälle selkeä, organisaatiolle

ylläpidettävä ja käytännön työtilanteisiin kiinnittyvä ratkaisu, joka tukee toimintaa myös epävarmuuden, kiireen ja keskeytysten keskellä. Tästä näkökulmasta työn tuloksena syntynyt kokonaisuus ei vastaa vain yksittäiseen koulutustarpeeseen, vaan toimii perustana, jota voidaan hyödyntää sekä perehdytyksessä että jatkuvan osaamisen ylläpidossa.

Käytännössä koulutus palvelee samanaikaisesti sekä perehdytystä että jatkuvaa osaamisen ylläpitoa. Uusi työntekijä saa selkeän peruspolun ja yhteisen vähimmäistason, kun taas olemassa olevalle henkilöstölle se tarjoaa kerrattavan, kohtuullisesti kuormittavan ja tarvittaessa päivitettävän rakenteen. Kun palautekanava, tukipolku ja omistajuus on rakennettu näkyväksi osaksi kokonaisuutta, koulutus ei jää irralliseksi materiaaliksi, vaan toimii sisäisenä palveluna, joka tukee arjen päätöksentekoa ja helpottaa oikeaa toimintaa myös silloin, kun aikaa on vähän tai tilanne on epäselvä.

Ohjeet auttavat vasta, kun ne muuttuvat toiminnaksi.

LÄHTEET

A. Ahlström Oy. (2024). Annual Report 2024. Haettu 14.7.2025 osoitteesta https://aahlstrom.com/wp-content/uploads/2025/04/A.Ahlstrom_Annual-Report-2024.pdf

A. Ahlström Oy. (2026). Kestävää arvonluontia: Historiamme alkaa vuodesta 1851. Haettu 2.2.2026 osoitteesta https://aahlstrom.com/ahlstromin-historia/

Anderson, L. W., & Krathwohl, D. R. (Toim.). (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. Longman.

Baldwin, T. T., & Ford, J. K. (1988). Transfer of training: A review and directions for future research. Personnel Psychology, 41(1), 63–105. https://doi.org/10.1111/j.1744-6570.1988.tb00632.x

Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. Qualitative Research, 15(2), 219-234. https://doi.org/10.1177/1468794112468475

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bruck, P. A., Motiwalla, L., & Foerster, F. (2012). Mobile learning with micro-content: A framework and evaluation. In BLED 2012 Proceedings (Paper 2). Association for Information Systems. https://aisel.aisnet.org/bled2012/2

Butavicius, M. A., Taib, R., & Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. Computers & Security, 123, 102937. https://doi.org/10.1016/j.cose.2022.102937

Cabinet Office. (2022). Government Cyber Security Strategy 2022 to 2030. Yhdistyneen kuningaskunnan hallitus. Haettu 12.12.2025 osoitteesta https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030/government-cyber-security-strategy-2022-to-2030-html

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. Oncology Nursing Forum, 41(5), 545–547. https://doi.org/10.1188/14.ONF.545-547

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340. https://doi.org/10.2307/249008

Edmondson, A. C. (1999). Psychological safety and learning behavior in work teams. Administrative Science Quarterly, 44(2), 350–383. https://doi.org/10.2307/2666999

ENISA. (2017). European Union Agency for Cybersecurity. ENISA Threat Landscape 2017. Haettu 2.9.2025 osoitteesta https://op.europa.eu/en/publication-detail/-/publication/69539d46-113b-11e8-9253-01aa75ed71a1/language-en

ENISA. (2024). European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. Haettu 22.1.2026 osoitteesta https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

ENISA. (2025). European Union Agency for Cybersecurity. ENISA Threat Landscape 2025. Haettu 15.2.2026 osoitteesta https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

Euroopan parlamentti ja neuvosto. (2016). Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 (yleinen tietosuoja-asetus). Haettu 22.8.2025 osoitteesta http://data.europa.eu/eli/reg/2016/679/oj

Finlay, L. (2002). "Outing" the Researcher: The Provenance, Process, and Practice of Reflexivity. Qualitative Health Research, 12(4), 531–545. https://doi.org/10.1177/104973202129120052

Goldstein, I. L., & Ford, J. K. (2002). Training in organizations: Needs assessment, development, and evaluation (4. painos). Wadsworth.

Groves, R. M. (2006). Nonresponse Rates and Nonresponse Bias in Household Surveys. Public Opinion Quarterly, 70(5), 646–675. https://doi.org/10.1093/poq/nfl033

Hattie, J., & Timperley, H. (2007). The Power of Feedback. Review of Educational Research, 77(1), 81–112. https://doi.org/10.3102/003465430298487

Heale, R., & Forbes, D. (2013). Understanding triangulation in research. Evidence-Based Nursing, 16(4), 98. https://doi.org/10.1136/eb-2013-101494

Herath, T. C., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Herbert, I. P., & Seal, W. B. (2012). Shared services as a new organisational form: Some implications for management accounting. The British Accounting Review, 44(2), 83–97. https://doi.org/10.1016/j.bar.2012.03.006

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105. https://doi.org/10.2307/25148625

ISO 9241-210:2019. (2019). Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems. International Organization for Standardization. Haettu 2.8.2025 osoitteesta https://www.iso.org/obp/ui/en/#iso:std:iso:9241:-210:ed-2:v1:en

ISO/IEC 27001:2022. (2022). Information security, cybersecurity and privacy protection - Information security management systems - Requirements. International Organization for Standardization & International Electrotechnical Commission. Haettu 15.8.2025 osoitteesta https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

ISO/IEC 27002:2022. (2022). Information security, cybersecurity and privacy protection - Information security controls. International Organization for Standardization & International Electrotechnical Commission. Haettu 18.8.2025 osoitteesta https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en

ISO/IEC 27005:2022. (2022). Information security, cybersecurity and privacy protection - Guidance on managing information security risks. International Organization for Standardization & International Electrotechnical Commission. Haettu 20.8.2025 osoitteesta https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en

Janssen, M., & Joha, A. (2006). Motives for establishing shared service centers in public administrations. International Journal of Information Management, 26(2), 102–115. https://doi.org/10.1016/j.ijinfomgt.2005.11.006

Joint Task Force Transformation Initiative. (2012). Guide for Applying the Risk Management Framework to Federal Information Systems and Organizations: A Security Life Cycle Approach (NIST SP 800-37 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r1

Joint Task Force. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Kahneman, D. (2011). Thinking, Fast and Slow. Farrar, Straus and Giroux.

Kirkpatrick, J. D., & Kirkpatrick, W. K. (2016). Kirkpatrick's four levels of training evaluation. ATD Press.

Knowles, M. S., Holton, E. F., & Swanson, R. A. (2015). The adult learner: The definitive classic in adult education and human resource development (8. painos). Routledge.

Kotter, J. P. (1996). Leading Change. Harvard Business School Press.

Kupias, P., & Peltola, R. (2009). Perehdyttämisen pelikenttä. Palmenia.

Kyberturvallisuuskeskus. (2023). Tietoturva on koko organisaation asia – vinkkejä henkilöstön kouluttamiseen. Haettu 18.1.2026 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/tietoturva-koko-organisaation-asia-vinkkeja-henkiloston

Merritt, M., Hansche, S., Ellis, B., Nethery Snyder, J., Sanchez-Cherry, K., & Walden, D. (2024). Building a Cybersecurity and Privacy Learning Program

(NIST SP 800-50r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50r1

MetaCompliance. (n.d.). Advanced Cyber Security Training for Employees: Engaging, multilingual eLearning solutions (Content Library / Nano library). Haettu 15.6.2025 osoitteesta https://www.metacompliance.com/content-library

NIST. (2010). National Institute of Standards and Technology. Guide to protecting the confidentiality of personally identifiable information (PII) (NIST SP 800-122). https://doi.org/10.6028/NIST.SP.800-122

NIST. (2024). National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Noe, R. A. (2023). Employee Training and Development (9. painos). McGraw Hill.

Ojasalo, K., Moilanen, T., & Ritalahti, J. (2015). Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. Sanoma Pro.

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. Health Services Research, 34(5 Pt 2), 1189–1208. https://pmc.ncbi.nlm.nih.gov/articles/PMC1089059/

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757-778.

Roer, K., & Carpenter, P. (2022). The Security Culture Playbook: An Executive Guide To Reducing Risk and Developing Your Human Defense Layer. Wiley.

Shute, V. J. (2007). Focus on formative feedback. ETS Research Report Series, 2007(1), i–47. https://doi.org/10.1002/j.2333-8504.2007.tb02053.x

Spitzner, L. (2023). 2023 Report: Managing Human Risk. SANS Institute. Haettu 28.9.2025 osoitteesta https://www.sans.org/white-papers/2023-report-managing-human-risk

Taylor, A., & Hung, W. (2022). The Effects of Microlearning: A Scoping Review. Educational Technology Research and Development, 70(2), 363–395. https://doi.org/10.1007/s11423-022-10084-1

TENK. (2023). Tutkimuseettinen neuvottelukunta. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa: Tutkimuseettisen

neuvottelukunnan HTK-ohje 2023. https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf

Tourangeau, R., & Yan, T. (2007). Sensitive questions in surveys. Psychological Bulletin, 133(5), 859-883. https://doi.org/10.1037/0033-2909.133.5.859

Tracy, S. J. (2010). Qualitative quality: Eight "big-tent" criteria for excellent qualitative research. Qualitative Inquiry, 16(10), 837-851. https://doi.org/10.1177/1077800410383121

Traficom. (2026). Huijauksia, kalastelua, sääntelyn ja teknologioiden kehitystä - videokoosteessa vuoden 2025 merkittävimmät kyberilmiöt ja kehityskulut sekä vinkit kansalaisille ja organisaatioille kyberturvalliseen vuoteen 2026. Haettu 20.2.2026 osoitteesta https://www.traficom.fi/fi/ajankohtaista/huijauksia-kalastelua-saantelyn-ja-teknologioiden-kehitysta-videokoosteessa-vuoden

van de Mortel, T. F. (2008). Faking it: Social desirability response bias in self-report research. Australian Journal of Advanced Nursing, 25(4), 40–48. https://www.ajan.com.au/archive/Vol25/Vol_25-4_vandeMortel.pdf

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478. https://doi.org/10.2307/30036540

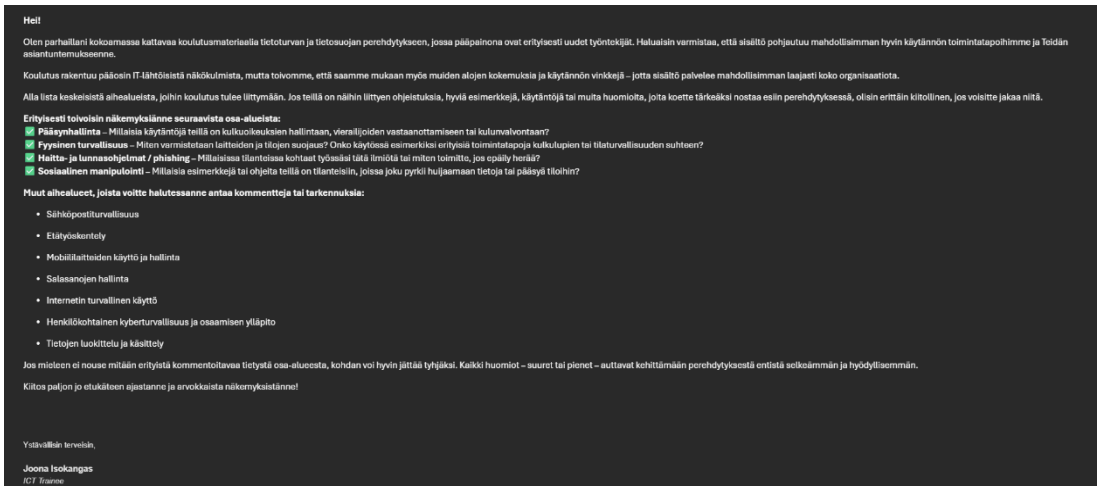
Verizon. (2025). Data Breach Investigations Report (DBIR) 2025. Haettu 19.1.2026 osoitteesta https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

Vuolearning. (n.d.). Learning paths and onboarding task lists. Haettu 2.11.2025 osoitteesta https://www.vuolearning.com/en/

Whitman, M. E., & Mattord, H. J. (2016). Management of information security (5. painos). Cengage Learning.

LIITTEET

Liite 1. Sähköpostitse välitetty esimerkkiviesti sidosryhmille koulutussisältöjen täsmentämiseksi.



Hei!

Olen parhaillani kokoamassa kattavaa koulutusmateriaalia tietoturvan ja tietosuojan perehdytykseen, jossa pääpainona ovat erityisesti uudet työntekijät. Haluaisin varmistaa, että sisältö pohjautuu mahdollisimman hyvin käytännön toimintatapoihimme ja Teidän asiantuntemukseenne.

Koulutus rakentuu pääosin IT-lähtöisistä näkökulmista, mutta toivomme, että saamme mukaan myös muiden alojen kokemuksia ja käytännön vinkkejä – jotta sisältö palvelee mahdollisimman laajasti koko organisaatiota.

Alla lista keskeisistä aihealueista, joihin koulutus tulee liittymään. Jos teillä on näihin liittyen ohjeistuksia, hyviä esimerkkejä, käytäntöjä tai muita huomioita, joita koette tärkeäksi nostaa esiin perehdytyksessä, olisin erittäin kiitollinen, jos voisitte jakaa niitä.

Erityisesti toivoisin näkemyksiänne seuraavista osa-alueista:

- ☑ **Pääsynhallinta** – Millaisia käytäntöjä teillä on kulkuoikeuksien hallintaan, vierailijoiden vastaanottamiseen tai kulunvalvontaan?
- ☑ **Fyysinen turvallisuus** – Miten varmistetaan laitteiden ja tilojen suojaus? Onko käytössä esimerkiksi erityisiä toimintatapoja kulkulupien tai tilaturvallisuuden suhteen?
- ☑ **Haitta- ja lunnasohjelmat / phishing** – Millaisissa tilanteissa kohtaat työssäsi tätä ilmiötä tai miten toimitte, jos epäily herää?
- ☑ **Sosiaalinen manipulointi** – Millaisia esimerkkejä tai ohjeita teillä on tilanteisiin, joissa joku pyrkii huijaamaan tietoja tai pääsyä tiloihin?

Muut aihealueet, joista voitte halutessanne antaa kommentteja tai tarkennuksia:

- Sähköpostiturvallisuus
- Etätyöskentely
- Mobiililaitteiden käyttö ja hallinta
- Salasanojen hallinta
- Internetin turvallinen käyttö
- Henkilökohtainen kyberturvallisuus ja osaamisen ylläpito
- Tietojen luokittelu ja käsittely

Jos mieleen ei nouse mitään erityistä kommentoitavaa tietystä osa-alueesta, kohdan voi hyvin jättää tyhjäksi. Kaikki huomiot – suuret tai pienet – auttavat kehittämään perehdytyksestä entistä selkeämmän ja hyödyllisemmän.

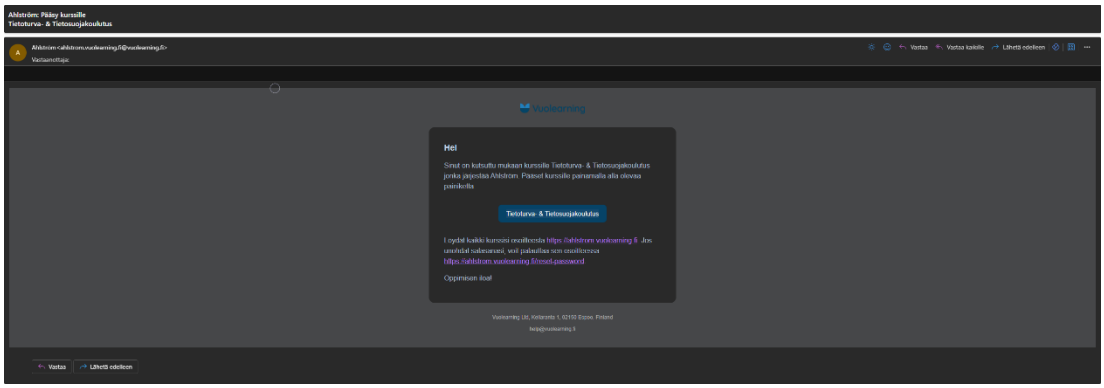
Kiitos paljon jo etukäteen ajastanne ja arvokkaista näkemyksistänne!

Ystävällisin terveisin,

Joona Isokangas
ICT Trainee

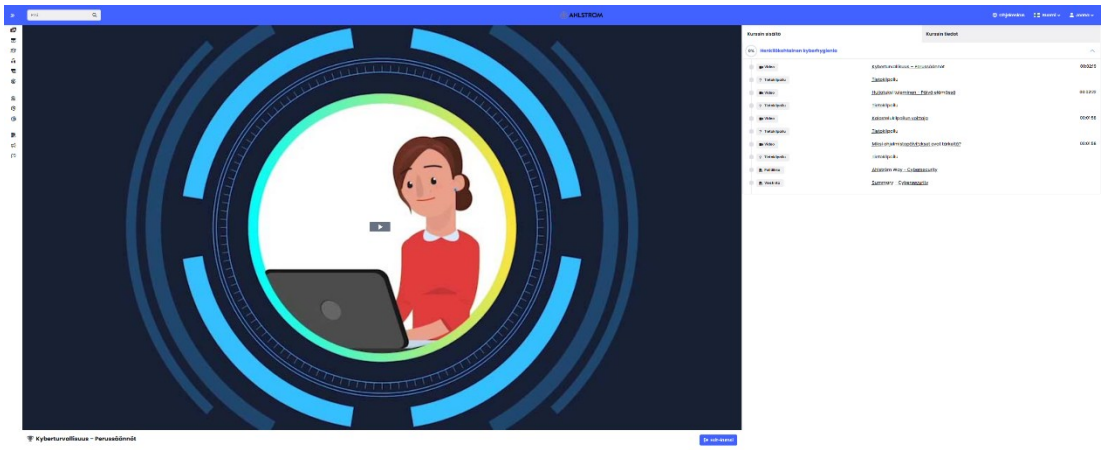
Lähde: Tekijä, kuvakaappaus sähköpostiviestistä, 2025 (tekijän muokkaama).

Liite 2. Esimerkkikutsu koulutuspolkuun (A-Learning/Vuolearning), sähköpostitse.



Lähde: Tekijä, kuvakaappaus sähköpostiviestistä, 2025 (tekijän muokkaama).

Liite 3. MyCompliance (MetaCompliance): esimerkki jakson elementtirakenteesta (rajattu).



Lähde: Tekijä, kuvakaappaus MyCompliance (MetaCompliance), 2025 (tekijän muokkaama).