Kim Kahila

Tietoturvariskien hallinta elektroniikkateollisuuden yrityksessä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tuotantotalous

Insinöörityö

5.2.2025

Tiivistelmä

Tekijä:	Kim Kahila
Otsikko:	Tietoturvariskien hallinta elektroniikkateollisuuden yrityksessä
Sivumäärä:	33 sivua + 2 liitettä
Aika:	5.2.2025
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tuotantotalous
Ammatillinen pääaine:	ICT-liiketoiminnan johtaminen
Ohjaajat:	Lehtori Thomas Rohweder Lehtori Jussi Alhorinne

Tämän insinöörityön tavoitteena on muodostaa ehdotus case-yrityksen tietoturvariskien hallinnan kehittämiseksi osana ISO/IEC 27001:2022 -sertifioitumista.

Insinöörityön tietoperustana käytetään konsulttiyrityksen yritykselle tekemää GAP-analyysiä, ISO/IEC 27000 -standardiperheen standardeja, case-yrityksen nykyistä toimintaa ja dokumentaatiota sekä projektiryhmän työpajoja. Ennen insinöörityön alkua työpajoina toteutettu GAP-analyysi tukee insinöörityön aihealueen määrittämistä, ISO/IEC 27000 -standardit tuovat toimintamallit ja suositukset toteutukselle. Projektiryhmän etäyhteyksin suoritetut tapaamiset tuovat osallistujien eri osa-alueiden vahvuudet dokumentaatioon.

Tietoperusta osoittaa, että tietoturvan dokumentaatio ei ole ISO/IEC 27001 -standardin vaatimusten tasolla. Tietoturvariskejä käsitellään yrityksen johtoryhmässä, mutta näitä ei ole arvioitu ja tuotu alemmalle, käytännön tasolle.

Tuotoksena tästä insinöörityöstä on kaksiosainen kehitysehdotus, joka sisältää tekstitiedostona olevan tietoturvariskien hallinnan kuvauksen ja Excel-tiedoston, joka pitää sisällään noin 60 tunnistetulla riskillä arvioidun riskikartan case-yritykselle.

Insinöörityön tarkoitus on kehittää case-yrityksen toimintaa vastaamaan muuttuvaa lainsäädäntöä ja asiakasvaatimuksia. Riskienhallinnan dokumentaatio ja toimintatavat on merkittävä osa NIS2 EU -direktiiviä ja ISO/IEC 27001 -sertifioitumista. Standardoidut toimintatavat osoittavat yrityksen sitoutumisen tietoturvariskien hallintaan vahvistaen turvallisuutta, laatua, luotettavuutta ja asiakastyytyväisyyttä.

Avainsanat: Tietoturva, Tietoturvariskit, ISO/IEC 27001, ISO/IEC 27005

Abstract

Author:	Kim Kahila
Title:	Information security risk management in an electronics industry company
Number of Pages:	33 pages + 2 appendices
Date:	5 February 2025
Degree:	Bachelor of Engineering
Degree Programme:	Industrial Management
Professional Major:	ICT Business Management
Supervisors:	Thomas Rohweder, Lecturer Jussi Alhorinne, Lecturer

---

Object of this thesis is to form proposal for the development of case company's information security risk management as part of the ISO/IEC 27001:2022 certification.

The thesis is based on a GAP analysis made for the company be the consulting company, the standards of the ISO/IEC 27000 standard family, case company's current operations and documentation, and the project group's workshops. The GAP analysis, carried out in workshops before the start of the thesis, supports the definition of the subject area of thesis, ISO/IEC 27000 standards provide operating models and recommendations for implementation. The remote meetings of the project group bring the strenghts of the participants' different areas to the documentation.

The knowledge base shows that the information security documentation is not at the level of the ISO/IEC 27001 standard requirements. Information security risks are processed in the company's management team, but these have not been assessed and brought to a lower, practical level.

The output of this thesis is a two-part development proposal, which includes a desription of information security risk management in a text file and an Excel file containing a risk map for case company assessed with approximately 60 identified risks.

The outcome of this thesis is to develop case company's operations to meet changing legislation and customer requirements. Risk management documentation and procedures are a significant part of the NIS2 EU directive and ISO/IEC 27001 certification. Standardized operating procedures demostrate a company's commitment to managing information security risks, strengthening safety, reliability, quality and customer satisfaction.

Keywords: Information security, Information security risks, ISO/IEC 27001, ISO/IEC 27005

Sisällys

Lyhenteet

GDPR: General Data Protection Regulation, Euroopan parlamentin ja neuvostonasetus.

NIS2: Euroopan parlamentin ja neuvoston asettama tietoturvan direktiivi.

EU-direktiivi:
Euroopan unionin alueita koskeva velvoittava tavoite, josta jäsenmaa saa itse päättää miten, ja millaisella lainsäädännöllä tavoitteet toteutetaan.

ISO: International Organization for Standardization. Kansainvälinen standardoimisorganisaatio.

IEC: International Electrotechnical Commission, kansainvälinen sähköalan standardoimisorganisaation.

ISO/IEC 27001:
Tietoturvan hallintajärjestelmän standardi.

ISO/IEC 27002:
Tietoturvallisuuden hallintakeinojen standardi.

ISO/IEC 27005:
Tietoturvariskien hallinnan standardi.

GAP-analyysi:
Prosessi, jossa verrataan liiketoiminnan nykyistä tilaa haluttuun tavoitetilaan.

HSEQ: Health, Security, Environment and Quality. ISO-standardeista 14001, 45001 ja 9001 muodostuva kokonaisuus.

1 Johdanto

Tietoturvan merkitys on kasvanut yrityksissä entisestään digitalisoitumisen ja muuttuneen maailmantilanteen vuoksi. Muutoksen pyörää liikuttaa lainsäädännön muutokset ja sitä myötä nousevat vaatimukset asiakkailta. Teollisuuden yrityksissä ennen kuluna ja pakollisena pahana koetut IT-järjestelmät ja -infra ovat muodostuneet yhdeksi toiminnan edellytykseksi. Yrityksien tiedot on siirretty toimistojen hyllyistä pilvipalveluihin, ja työntekijöiden työskentely on laajentunut yrityksen tilojen ulkopuolelle. Enää yrityksen tietojen suojaamiseen eivät riitä ainoastaan fyysiset suojaukset.

Aihealueelle kuuluvista lainsäädännöllisistä velvoitteista viimeisin merkittävämpi oli 1.1.2019 voimaan tullut henkilötietoja käsittelevä tietosuojalaki, joka tunnetaan yleisimmin Euroopan unionin asettamana yleisenä tietosuoja-asetuksena (GDPR) (Tietosuojalaki). Vuosien kuluessa on tullut aika päivittää tietoturvalait nykypäivään.

Insinöörityö suoritetaan elektroniikkateollisuuden parissa toimivalle case-yritykselle. Case-yritys on osa konsernia, joka toimii kansainvälisesti. Case-yritys lukeutuu kokonsa suhteen pk-yrityksiin, eli pieniin ja keskisuuriin yrityksiin, joka työllistää alle 250 henkilöä.

Kehityshaasteena esille nousee NIS2 EU -direktiivi, joka on Euroopan union kyberturvallisuusdirektiivi, joka täytyi toimeenpanna kansallisesti 17.10.2024 mennessä. NIS2 EU -direktiivi asettaa vaatimuksia keskeisille ja tärkeille toimijoille, joihin case-yrityksen täytyy myös vastata. Case-yrityksen tietoturvan dokumentoinnin taso ei vastaa NIS2 EU -direktiivin vaatimuksia. (Hallituksen esitys.)

Insinöörityön tavoite on muodostaa ehdotus case-yrityksen tietoturvariskien hallinnan kehittämiseksi osana ISO/IEC 27001:2022 -sertifioitumista.

Lopputuloksena insinöörityöstä on kehitysehdotus.

Insinöörityö rakentuu työpajoista, viikoittaisista projektiryhmän tapaamisista ja johtoryhmän jäsenten palautteista. Insinöörityö koostuu seitsemästä osiosta.

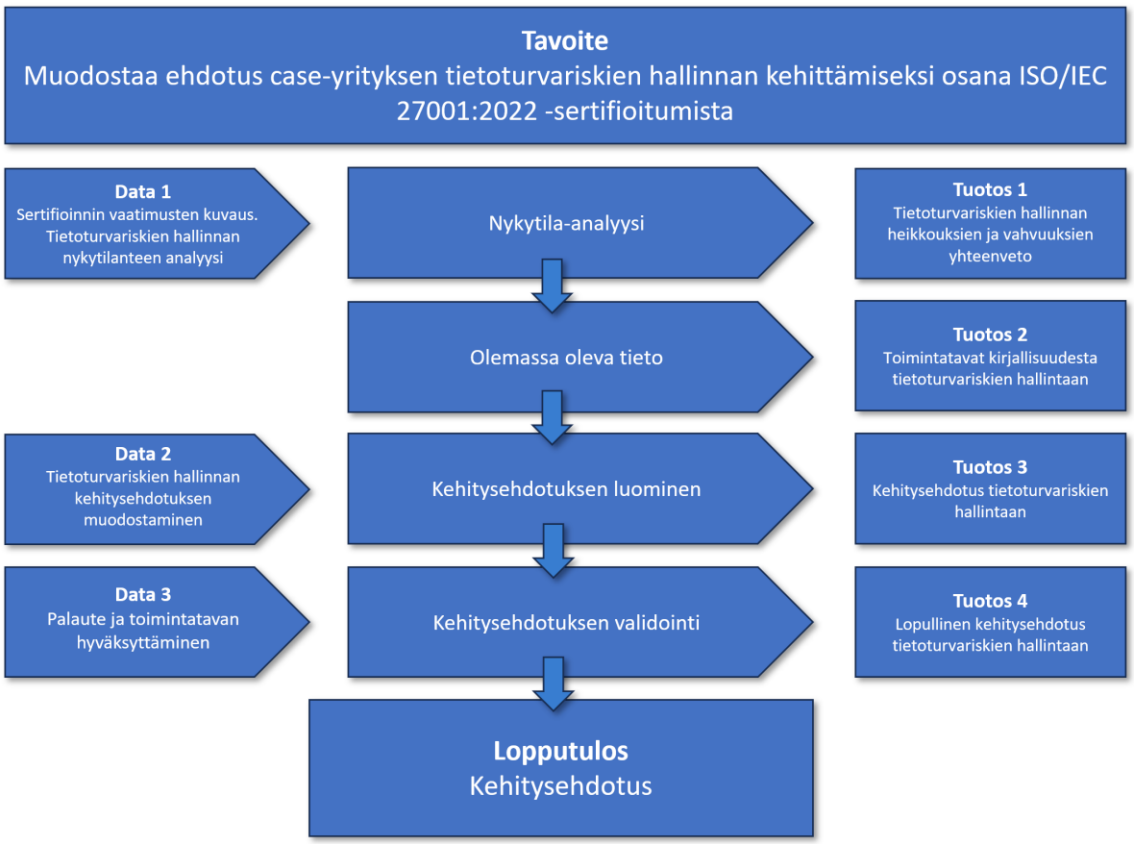
Ensimmäinen osio toimii esittelynä insinöörityön lähtökohdille. Luvussa 2 käsitellään eri vaiheista ja kenttätiedon keruusta muodostuvaa suunnitelmaa insinöörityön toteuttamiseksi. Luvussa 3 rakennetaan kuva yrityksen nykytilasta, jota seuraa nykytilan heikkouksiin vastaava teoria luvussa 4. Luvussa 5 rakennetaan kehitysehdotus yhdistämällä tuotokset luvuista 3 ja 4. Luvussa 6 validoidaan luvusta 5 luotua kehitysehdotus. Lopuksi luvussa 7 vedetään insinöörityö yhteen, tarkastellaan insinöörityön jälkeisiä toimenpiteitä ja arvioidaan insinöörityön toteuma.

2 Insinöörityön tavoite

Tässä luvussa kuvataan tapa lähestyä tutkimusta, miten tutkimus suunnitellaan ja erilaisia tapoja kerätä tietoa.

2.1 Insinöörityön vaiheet

Kuvassa 1 esitetään insinöörityön vaiheet. Insinöörityön vaiheet visualisoivat datalähteet ja vaiheiden tuotokset.



Kuva 1 Insinöörityön vaiheet

Kuten kuvassa 1 nähdään, ensimmäinen askel on kevään aikana konsultin johdolla pidettyjen työpajojen tuotoksena syntyneen raportin hyödyntäminen nykytila-analyysin luomiseksi. Työpajoissa käsiteltiin tietoturvan hallintajärjestelmän standardin (ISO/IEC 27001) vaatimuksia ja miten case-yrityksen nykyinen toiminta vastaa standardin vaatimuksia. Ensimmäisen vaiheen nykytila-analyysissa keskitytään tietoturvariskien hallinnan heikkouksiin ja vahvuuksiin.

Seuraava askel on tietoturvariskien hallinnan kehitysehdotuksen muodostaminen. Tässä vaiheessa käsitellään tietoturvariskien hallinnan standardin (ISO/IEC 27005) pohjalta luotua riskikarttaa ja arvioidaan riskit case-yrityksen kannalta.

Kolmas askel toteutuu tehdyn kehitysehdotuksen esittelyllä, palautteen keräämisellä ja toimintatavan hyväksymisellä. Saadun palautteen pohjalta kehitysehdotusta viimeistellään lopullisen kehitysehdotuksen antamiseksi.

2.2 Tiedonkeruusuunnitelma

Alla oleva taulukko pitää sisällään tiedon tiedonkeruun rakenteesta.

Taulukko 1 Kenttätiedon keruun suunnitelma

	SISÄLTÖ	LÄHDE	AVAINHENKILÖ	AJOITUS	TUOTOS
Data 1 Sertifioinnin vaatimusten kuvaus. Tietoturvariskien hallinnan nykytilanteen analyysi	- Nykyisen tietoturvariskien hallinnan kuvaus - Tietoturvariskien hallinnan analyysi	- Laatujärjestelmä - GAP-analyysi	- Talousjohtaja - Operatiivinen johtaja Projektiryhmä: - Konsultti - IT-asiantuntija - HSEQ-päällikkö	Kesäkuu	- Tietoturvariskien hallinnan heikkouksien ja vahvuuksien yhteenveto
Data 2 Tietoturvariskien hallinnan kehitysehdotuksen muodostaminen	- Ehdotukset heikkouksiin	- Avainhenkilö työpajat	- Talousjohtaja - Operatiivinen johtaja - Projektiryhmä	Kesä-marraskuu	- Kehitysehdotus tietoturvariskien hallintaan
Data 3 Palaute ja toimintatavan hyväksyttäminen	- Kehitysehdotuksen korjaaminen	- Kommentit avainhenkilöiltä	- Talousjohtaja - Operatiivinen johtaja - Projektiryhmä	Marras-tammikuu	- Lopullinen kehitysehdotus tietoturvariskien hallintaan

Kuten taulukosta 1 on nähtävissä, data 1:n pohjana toimii ISO/IEC 27000 -standardiperhe ja kevään työpajoissa muodostunut GAP-analyysi (prosessi, jossa verrataan liiketoiminnan nykyistä tilaa haluttuun tavoitetilaan).

Data 2 toteutuu projektiryhmän kesken järjestetyissä työpajoissa, joissa käsitellään tietoturvariskejä.

Data 3 kerätään avainhenkilöiden palautteella, josta muodostuu lopullinen kehitysehdotus tietoturvariskien hallintaan.

3 Tietoturvariskien hallinnan nykytilanne

Tässä luvussa tarkastellaan yrityksen nykyistä tilannetta tietoturvariskien hallinnan suhteen. Analysoidaan vahvuudet ja heikkoudet ja lopuksi vedetään asiat yhteen.

3.1 Katsaus aiheen kuvaukseen

Insinöörityön tavoite on muodostaa ehdotus case-yrityksen tietoturvariskien hallinnan kehittämiseksi osana ISO/IEC 27001:2022 -sertifioitumista. Pohjatietoina nykytilan analysoimiseksi on ennen tämän insinöörityön alkua ulkoisen konsultin johtamina toteutetut työpajat. Työpajoista muodostui GAP-analyysi, jossa case-yrityksen toimintaa peilattiin ISO/IEC 27001 -tietoturvallisuuden hallintajärjestelmään. Tämän lisäksi keskeisenä lähteenä ovat havainnot case-yrityksen toimintaan ja dokumentaatioon tutustumalla.

3.2 Yrityksen nykytilanne

Case-yrityksen nykytilanteessa liiketoiminnan riskienhallintaa toteutetaan riskien ja mahdollisuuksien kautta. Riskienhallinta ja katselmukset on johtoryhmässä toteutettu HSEQ (Health, Security, Environment and Quality, ISO-standardeista 14001, 45001 ja 9001 muodostuva kokonaisuus) -vaatimusten mukaisesti, jossa huomioidaan henkilöstö, tuote, talous, liiketoiminta, omaisuus, informaatio ja ympäristö. Johtoryhmän nimetty jäsen vastaa vastuullaan olevien riskien hallinnasta. Riskiarviointeja toteutetaan mm. asiakaskohteisiin, varaston ja tuotannon prosesseihin. Case-yrityksellä on dokumentoituna toimintajärjestelmässä toimintatavat eri prosesseihin. Prosesseille on määritetty omistajat, prosessin sisäiset tehtävät ja valtuudet.

3.3 Vahvuudet ja heikkoudet -analyysi

Case-yrityksen vahvuudet ja heikkoudet arvioidaan SWOT-analyysilla kuvan 2 mukaisesti.

Kuva 2 SWOT-analyysi

Nykytilassa vahvuuksina on nähtävissä olemassa olevan toimintajärjestelmän hyödyntäminen ISO/IEC 27001 -standardin implementoinnissa toimintaan. Toimintajärjestelmän laajentaminen mahdollistaa standardien keskitetyn hallinnan ilman merkittävää kulujen nousua. Nykyisessä toiminnassa HSEQ-vaatimusten kautta riskienhallintaa ja johdon katselmuksia toteutetaan osana liiketoimintaa.

Nykytilan heikkouksina on nähtävissä, ettei tietoturvariskejä ole tunnistettu riittävän laajasti toiminnan sisältä. Tietoturvan kannalta riskejä on käsitelty ylätasolla merkittäviksi tunnistettujen riskien kautta. Tietoturvariskit ovat läsnä läpi organisaation, joten oikeiden roolien ja riskien vastuullisten löytäminen voidaan kokea

haastavaksi. Tietoturva yleensä kuitenkin mielletään IT-osaston työksi, joka ei kuulu muille. Case-yrityksessä havaituissa puutteissa dokumentaatio ei ole riittävällä tasolla ja tämän insinöörityön kannalta merkittävänä on tietoturvariskien hallinnan kuvauksen puuttuminen.

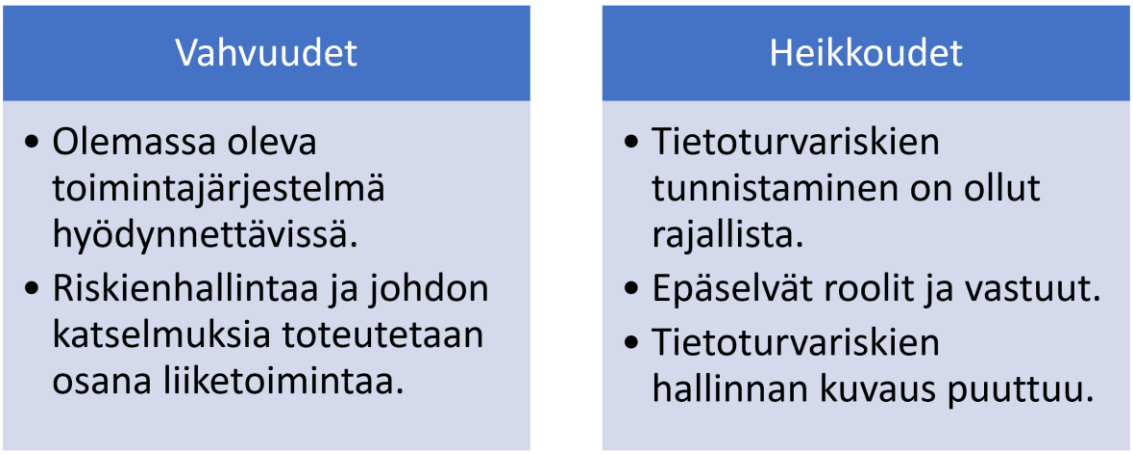
Mahdollisuutena voisi nähdä tunnistettujen riskien hallinnan viemisen Excel-taulukoista toimintajärjestelmän näkymälle. Riskienhallinta on kuvattu ja tätä tehdään HSEQ:n antamien vaatimusten mukaisesti. Nykyisen toimintamallin ja tietoturvariskienhallinnan yhdistäminen on nähtävissä mahdollisuutena.

Tunnistettuna uhkana voidaan todeta riittämätön resursointi. Uusien velvoitteiden täyttämiseksi tarvitaan nimettyjä henkilöitä, joilla on riittävät valtuudet vastata riskien hallintaan. Resursoinnissa keskiössä on myös riittävän osaamisen takaaminen, jota tulee koulutuksilla täydentää. Huomioitavana on myös nykyisten työtehtävien mahdolliset uudelleenjärjestelyt riittävän työajan takaamiseksi.

3.4 Vahvuudet ja heikkoudet -yhteenveto

Yhteenvetona tietoturvariskien hallinnan nykytilanteen vahvuuksiin ja heikkouksiin kyettiin tunnistamaan keskeiset teemat. Nämä on eritelty kuvassa 3.

Vahvuutena on tunnistettu käytössä oleva toimintajärjestelmä, jota pystytään hyödyntämään dokumentoinnin keskittämisessä. Lisäksi nykyisiin toimintatapoihin osana liiketoimintaa kuuluu riskienhallinta ja johdon katselmukset. Vahvuudet tullaan huomioimaan insinöörityön edetessä, valmiina olevat toimintamallit tarjoavat hyvän pohjan insinöörityön toteuttamiseen.



Kuva 3 Vahvuudet ja heikkoudet

Heikkoutena havaittiin, ettei tietoturvariskejä ole tunnistettu riittävän laajasti. Lisäksi epäselvyydet tulevista rooleista ja vastuista vaativat määrittelyä. Perusteena tietoturvariskien tunnistamiselle ja hallinnalle on kuvaus toimintatavasta, joka toistaiseksi puuttuu.

Tehtyjen löydösten pohjalta seuraavassa luvussa käsitellään ISO/IEC 27000 -standardisarjaa, joista teoreettisesti merkittävinä ovat tietoturvallisuuden hallintajärjestelmä ISO/IEC 27001, tietoturvallisuuden hallintakeinot ISO/IEC 27002 ja tietoturvariskien hallintaan keskittyvä ISO/IEC 27005. Valitut aiheet ovat keskeisinä tietolähteinä vastaamisessa tunnistettuihin heikkouksiin.

4 Riskienhallinnan teoreettinen viitekehys

Tässä luvussa käsitellään riskienhallinnan näkökulmasta ISO/IEC 27000 -standardisarjaa. Standardisarjasta käydään yleisesti ISO/IEC 27000 -standardin sisältö, ISO/IEC 27001 -tietoturvallisuuden hallintajärjestelmän kohdat 4-10, ISO/IEC 27002 -tietoturvallisuuden hallintakeinojen kohdat 5-8 ja ISO/IEC 27005 -tietoturvariskien hallinnan standardi.

ISO/IEC 27000 -standardisarja tarjoaa suosituksia ja ohjeita tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin. Vaatimuksien tavoitteena on suojata tiedon luottamuksellisuutta, eheyttä ja saatavuutta. ISO/IEC 27000 -standardisarjan

tietoturvallisuuden hallintajärjestelmästandardeihin kuuluvat ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004 ja ISO/IEC 27005. (SFS-EN ISO/IEC 27001:2023: 5–6.)

4.1 ISO/IEC 27001

ISO/IEC 27001 -standardi määrittelee vaatimukset tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitämiseen ja jatkuvaan parantamiseen organisaation toiminnassa (SFS-EN ISO/IEC 27001:2023: 6).

ISO/IEC 27001 -standardi pitää sisällään kuvan 4 mukaiset kohdat 4-10. Kohdissa esitettyjä vaatimuksia ei voi rajata tarkastelun ulkopuolelle, mikäli organisaatio ilmoittaa noudattavansa ISO/IEC 27001 -standardia. (SFS-EN ISO/IEC 27001:2023: 7.)

Kuva 4 ISO/IEC 27001 -standardin kohdat 4-10 (SFS-EN ISO/IEC 27001:2023: 7–16.)

Kohdassa 4 Organisaation toimintaympäristö organisaatio ymmärtää ja määrittelee toimintaympäristönsä, jossa huomioidaan myös sidosryhmien tarpeet ja odotukset. Sisältönä tästä muodostuu tietoturvallisuuden hallintajärjestelmän kuvaus, joka kuvaa rajaukset ja soveltamiset organisaation osalta.

Kohdassa 5 Johtajuus korostuu johtajuus ja sitoutuminen, joka ulottuu organisaation ylimpään johtoon. Johdon tulee varmistaa tarvittavien toimintaa ohjaavien dokumenttien toteutumisen, jotka ovat linjassa organisaation strategian kanssa. Johdon tulee laatia ja hyväksyä tietoturvapolitiikka, joka on koko organisaation tiedossa ja tarvittaessa myös saatavilla sidosryhmille. Johdon tehtäviin kuuluu myös määritellä, kenellä tai keillä on vastuut ja valtuudet toimia tietoturvallisuuden hallintajärjestelmän vaatimusten toteuttamiseksi sekä raportoida hallintajärjestelmän toteutumisesta ylimmälle johdolle. Varmistamisien lisäksi johdon roolina on viestiä tietoturvallisuuden hallinnan tärkeydestä ja edistää jatkuvaa parantamista.

Kohdassa 6 Suunnittelu määritellään vaatimuksia käsitellä tietoturvariskejä ja mahdollisuuksia. Kohdassa viitataan Liite A:n hallintakeinoihin. Liite A:ssa velvoittavat hallintakeinot ovat linjassa standardin ISO/IEC 27002:2023 kohtiin 5-8. Standardin viimeisimmässä versiossa ISO/IEC 27001:2023 Liite A:n hallintateemoja on 4: Organisaatio, Henkilöstö, Fyysinen ja Teknologia. Liite A sisältää 93 hallintakeinoa.

Kohdassa 7 Tukitoiminnot organisaation hallintajärjestelmän luomiseen, käyttöönottoon, ylläpitoon ja jatkuvaan parantamiseen on mahdollistettava riittävät resurssit. Tukitoiminnot ottavat kantaa tietoturvallisuuden tason parissa työskentelevien pätevyyteen ja tästä säilytettävään dokumentoituun näyttöön. Organisaation tulee määrittää miten sisäinen ja ulkoinen viestintä toteutetaan. Kohdassa määritetään dokumentoitavaan tietoon liittyvät käytänteet luomisesta, päivittämisestä ja hallinnasta.

Kohta 8 Toiminta määrittää käytänteet toiminnan suunnitteluun ja ohjaukseen. Toiminnassa tulee määritellä kriteerit ja prosessin ohjaus kohdan 6 tietoturvariskien hallinnan toimenpiteiden toteuttamiselle.

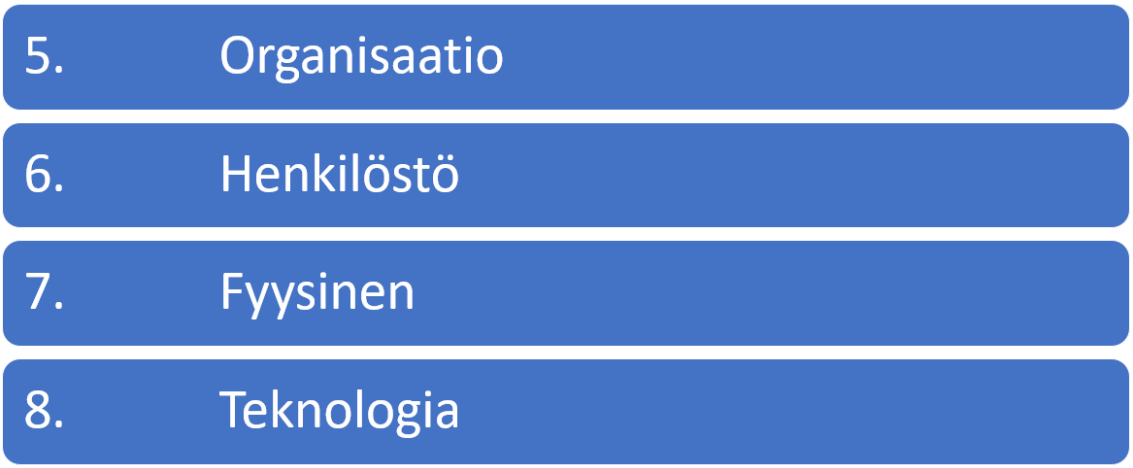
Kohdassa 9 Suorituskyvyn arviointi käsitellään organisaation tarvetta määritellä tietoturvan toteuttamiseen ja hallintajärjestelmän vaikuttavuuteen asianmukainen seuranta, mittaus, analysointi ja arviointi. Organisaation tulee toteuttaa

sisäisiä auditointeja säännöllisesti. Auditoijien tulee pystyä suorittamaan auditointi objektiivisesti ja puolueettomasti. Auditointien tulokset raportoidaan organisaation johdolle. Osana suorituskyvyn arviointia esillä on johdon katselmukset, joita tulee toteuttaa säännöllisin aikavälein. Johdon katselmuksista säilytetään dokumentoitua tietoa näyttönä tuloksista.

Kohdassa 10 Parantaminen organisaation tulee toteuttaa jatkuvaa parantamista tietoturvallisuuden hallintajärjestelmän soveltuvuuden, tarkoituksenmukaisuuden ja vaikuttavuuden eteen. Kohdassa käsitellään poikkeamia ja näiden korjaavia toimenpiteitä. Havaittuihin poikkeamiin tulee reagoida ja arvioida tarpeelliset toimenpiteet, joilla poikkeamien toistumisen ja esiintymisen saa ennaltaehkäistyä jatkossa. Poikkeamien luonteesta, tehdyistä ja korjaavista toimenpiteistä tulee säilyttää dokumentoitua tietoa. (SFS-EN ISO/IEC 27001:2023: 7–16.)

4.2 ISO/IEC 27002

ISO/IEC 27002:2022 -standardi käsittelee ISO/IEC 27001:2023 Liite A:n hallintakeinoja liitettä syvällisemmin tarjoten organisaatiolle selityksen ja ohjeistuksen hallintakeinojen toteuttamista varten. Standardi sisältää myös Liite B:n, joka kuvaa hallintakeinojen vastaavuuden standardin ISO/IEC 27002:2013 sisältäneisiin hallintakeinoihin ja tunnisteisiin. Liite B mahdollistaa organisaatioiden siirtymän yhteensopivaksi uudistuneeseen standardiin.



Kuva 5 ISO/IEC 27002 -standardin kohtien 5-8 hallintakeinot (SFS-EN ISO/IEC 27002:2022: 17.)

Hallintakeinojen teemat on numeroitu väliltä 5-8 kuvan 5 mukaisesti. Hallintakeinojen teemat määräytyvät

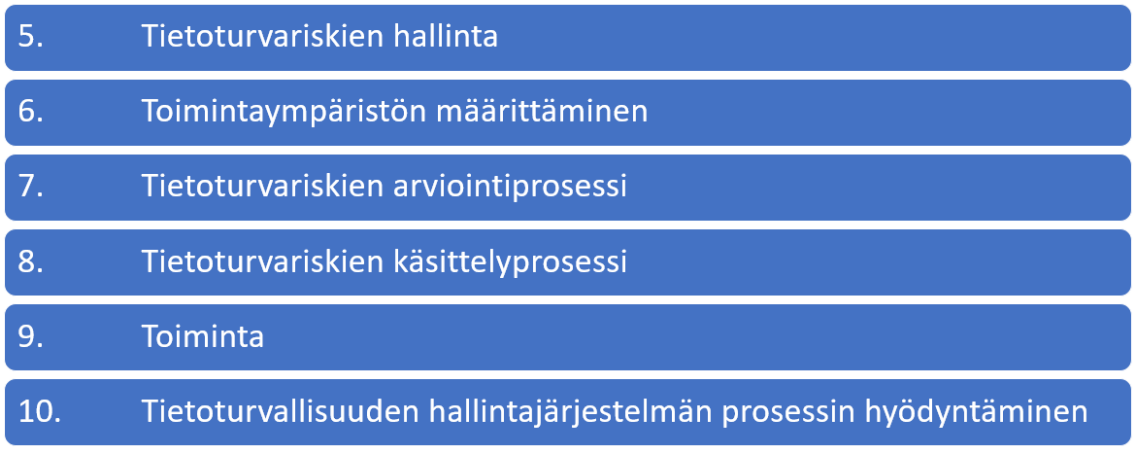
- henkilöstöön liittyviksi hallintakeinoiksi, jos ne koskevat yksittäisiä henkilöitä
- fyysisiksi hallintakeinoiksi, jos ne koskevat fyysisiä esineitä
- teknologisiksi hallintakeinoiksi, jos ne koskevat teknologiaa
- organisaatioon liittyviksi hallintakeinoiksi, jos mikään aiemmista luokista ei koske niitä.

Hallintakeinojen kuvaukset sisältävät hallintakeinon nimen, attribuuttitaulukon, hallintakeinon, tarkoituksen, ohjeistuksen ja lisätiedot. (SFS-EN ISO/IEC 27002:2022: 17–18.)

4.3 ISO/IEC 27005

ISO/IEC 27005 -standardi toimii ohjeistuksena ISO/IEC 27001:ssä määriteltyihin vaatimuksiin tietoturvariskien toteuttamiseksi. ISO/IEC 27005:2022 oleva

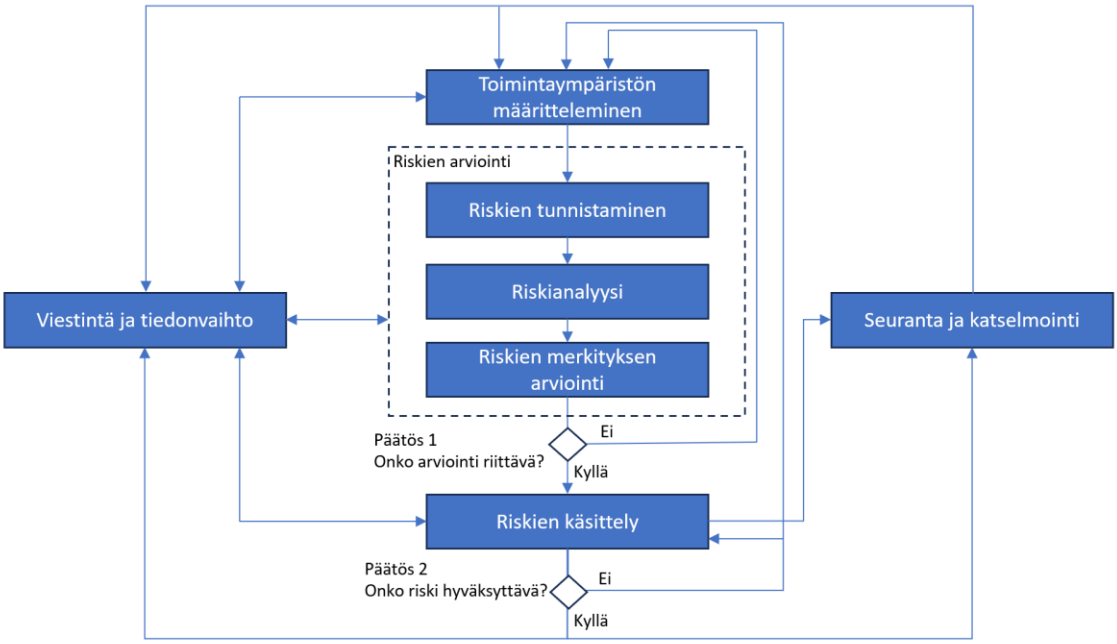
ohjeistus ja sanasto on yhdenmukainen standardien ISO/IEC 27001:2023 ja ISO 31000:2018 kanssa. (ISO/IEC 27005:2022: 4–6.)



Kuva 6 ISO/IEC 27005 -standardin rakenne (ISO/IEC 27005:2022: 3–12.)

4.3.1 Tietoturvariskien hallinta

Tietoturvariskien hallinnassa käsitellään tietoturvariskien hallintaprosessia kuvan 7 mukaisesti. Tietoturvariskien hallintaprosessi perustuu standardin ISO 31000 yleiseen riskienhallintaprosessiin. (ISO/IEC 27005:2022: 12–13.)



Kuva 7 Tietoturvariskien hallintaprosessi (ISO/IEC 27005:2022: 13.)

Tietoturvariskien hallintaprosessissa riskien arviointi- ja käsittelytoiminnot voi olla toistuvaa, jolloin iteratiivinen toimintamalli voi syventää ja tehdä riskien arvioinnista yksityiskohtaisempaa. Riskejä käsitellään, kunnes jäännösriski on saatu hyväksyttävälle tasolle. Riskin hyväksyttävälle tasolle saaminen voi vaatia riskien arviointia koskevan toimintaympäristön muuttamista ja alan asiantuntijan osallistamista.

Riskien käsittelyn iteratiiviseen prosessiin kuuluvat seuraavat vaiheet

- riskien käsittelyvaihtoehtojen kehittäminen ja valinta
- riskien käsittelyn suunnittelu ja toteuttaminen
- riskien käsittelyn vaikuttavuuden arvioiminen
- päätös siitä, onko jäljelle jäävä riski hyväksyttävissä oleva vai ei
- lisäkäsittelyn suorittamien, jos riski ei ole hyväksyttävissä oleva.

Tietoturvariskien hallinnan jaksot jakautuvat strategiseen ja operatiiviseen jaksoon. Strategisessa jaksossa liiketoiminnan omaisuuserät, riskin lähteet, uhkat, lopputavoitteet tai tietoturvatapahtumat ajavat organisaation toimintaympäristön muutoksiin. Operatiivisessa jaksossa toimintaympäristön osatekijät ovat lähtötietoina tai antamassa kriteerit riskien arviointeihin. Strategista jaksoa toteutetaan pitkällä aikavälillä, kun taas operatiivista jaksoa käsitellään lyhyemmällä aikavälillä. Molemmat jaksot voivat sisältää useita riskien arviointia erilaisilla toimintaympäristöillä ja soveltamisaloilla. (ISO/IEC 27005:2022: 13–14.)

4.3.2 Toimintaympäristön määrittäminen

Organisaation tulee määritellä ja dokumentoida riskienhallinnan toimintaympäristönsä. Toimintaympäristöä koskevat sidosryhmät tulee tunnistaa ja ymmärtää heidän vaatimuksensa. Toimintaympäristössä tulee määrittää, miten riskien arviointia sovelletaan organisaatiossa sekä laatia ja ylläpitää tietoturvariskikriteeristö. Riskien hyväksymiskriteereillä voidaan määrittää riskien käsittelyssä, onko riski hyväksyttävissä vai ei. Hyväksymiskriteerit vaihtelevat organisaation riskinottohalun mukaan. Organisaation johtotason tulee hyväksyä riskien hyväksymiskriteerit. (ISO/IEC 27005:2022: 15–20.)

4.3.3 Tietoturvariskien arviointiprosessi

Tietoturvariskien arviointiprosessissa tietoturvariskejä tunnistetaan, analysoidaan ja arvioidaan riskin merkitys. Suunniteltujen menetelmien ja työkalujen tulee olla riittävän tarkkoja, jotta voidaan todentaa tuloksien yhdenmukaisuus, pätevyys ja toistettavuus. Tietoturvariskien hallinnan toimintamallin tulee mahdollistaa vertailu organisaation muihin riskeihin.

Riskien tunnistamisen prosessissa riskit havaitaan ja kuvataan. Prosessissa tunnistetaan riskien lähteet ja tapahtumat. Tavoitteena riskien tunnistamiselle on luoda luettelo riskeistä, jotka voivat olla esteenä tietoturvatavoitteiden saavuttamiselle, vaikuttaa siihen tai viivästyttää sitä.

Yleisinä riskien tunnistamisen toimintamalleina on nostettu tapahtumakohtainen toimintamalli ja omaisuuseriin perustuva toimintamalli. Tapahtumakohtaisessa toimintamallissa tunnistetaan strategiset skenaariot riskin lähteitä tarkastelemalla. Tarkastelua voi toteuttaa esimerkiksi haastattelemalla ylintä johtoa ja muita liiketoimintaprosesseista vastaavia henkilöitä. Tapahtumakohtainen toimintamalli mahdollistaa ylätason skenaarioiden tai strategisten skenaarioiden laatimisen ilman yksityiskohtaista omaisuuserien tunnistamista.

Omaisuuseriin perustuvassa toimintamallissa omaisuuseriä, uhkia ja haavoittuvuuksia tarkastelemalla voidaan tunnistaa ja arvioida riskejä. Riskien tarkkaan arviointiin täytyy laatia tietoon ja tietojenkäsittely-ympäristöihin perustuva luettelo omaisuuseristä.

Tunnistettuja riskejä tulisi tarkastella, vaikka riskien lähde ei ole kaikissa tilanteissa organisaation hallinnan alainen tai tiedossa. Riskien arviointia tulisi toistaa varsinkin monimutkaisissa riskiskenaarioissa eri tasoilla, jotta riskien juurisyyt pystytään tunnistamaan.

Tietoturvariskien arviointiin kuuluu riskien omistajien tunnistaminen. Riskien omistajat ovat vastuussa omistamistaan riskeistä ja heillä tulee olla valtuudet hallita riskejä organisaation sisällä. Riskien omistajia tulee tunnistaa, kun sitä ei ole tehty aiemmin tai organisaation sisällä tapahtuu henkilöstömuutoksia, jolloin riskin nimetty omistaja ei pysty hallitsemaan riskiä. (ISO/IEC 27005:2022: 21–24.)

4.3.4 Tietoturvariskien käsittelyprosessi

Tietoturvariskien käsittelyprosessi toteutetaan tietoturvariskien arvioinnin pohjalta tehdystä priorisoidusta luettelosta. Riskien käsittelyvaihtoehdot tulevat tehdystä suunnitelmasta. Käsittelyvaihtoehtoja riskeille on muun muassa riskin torjunta, muokkaaminen, säilyttäminen ja jakaminen. Käsittelyvaihtoehdoilla organisaatio toteuttaa odotettavien kustannusten ja hyötyjen perusteella riskien hallintaa.

Riskeille määritettävien hallintakeinojen tulee olla riskiin vaikuttavia. Käsiteltäviin riskeihin tulee kohdistua yksi tai useampi hallintakeino. Hallintakeinoja määrittäessä tulee huomioida hallintakeinon vaikutus riskin todennäköisyyteen tai seuraukseen ja miten hallintakeino ylläpitää riskitasoa. Organisaatio voi määritellä tarvittaessa räätälöityjä hallintakeinoja. Räätälöityjen hallintakeinojen kuvauksien tulee olla merkityksellisiä organisaation henkilöille ja edistää kyseisillä hallintakeinoilla tehtävää päätöksentekoa riskien hallinnasta. Hallintakeinojen päätyypit ja näiden tarkoitukset ovat seuraavat

- Estävän hallintakeinon tarkoitus on estää tietoturvatapahtumien seurauksen tai seuraukset pienentämällä korjaavien hallintakeinojen todennäköisyyttä.

- Havaitsevan hallintakeinon tarkoitus on havaita tietoturvatapahtumat ja lieventää riskiä estävien hallintakeinojen pettäessä.

- Korjaavien hallintakeinojen tarkoitus on rajoittaa tietoturvatapahtumia lieventämällä riskiä havaitsevien hallintakeinojen pettäessä.

Organisaation määrittämiä hallintakeinoja tulee verrata ISO/IEC 27001 liite A:ssa esitettyihin hallintakeinoihin. Puuttuvia hallintakeinoja tulee verrata organisaation valitsemiin hallintakeinoihin, jotta tarvittavia hallintakeinoja ei ole poissuljettu riskien arvioinnista. Organisaatio tulee luoda liite A:n mukaisista hallintakeinoista soveltuvuuslausunto, jossa sisältyy tarvittavat hallintakeinot, perustelut hallintakeinojen sisällyttämiselle, tieto hallintakeinon toteuttamisesta ja perustelut, mikäli jokin ISO/IEC 27001 liite A:n mukaisista hallintakeinoista on jätetty pois.

Organisaation tulee laatia suunnitelma riskienkäsittelylle. Riskienkäsittelyn suunnitelma luo toimintaedellytykset riskienkäsittelyyn. Riskien hyväksymiseksi riskeille tulee määrittää omistajat, joiden tehtävä on päättää jäännöstietoturvariskien hyväksymisestä. (ISO/IEC 27005:2022: 29–36.)

4.3.5 Toiminta

Toiminta kuvaa organisaation tietoturvariskien arviointi- ja käsittelyprosessin suorittamista. Toiminnassa noudatetaan hallintajärjestelmän ja suunnitelman mukaisesti määritettyjä kriteerejä ja käytänteitä. Riskien säännöllisessä arvioinnissa tulee ottaa huomioon vuosittainen budjettikierto ja mahdolliset hankintaprosessit, joiden vaikuttavuus riskien arviointiin on merkittävä. Riskien arvioinnit tulee toteuttaa uudelleen hankintojen budjettiratkaisujen vahvistuttua. Riskejä käsitellään säännöllisin aikavälein tai muutoksia aiheuttavien tapahtumien jäljiltä. Riskien käsittelystä muodostuu säilytettävät ja hyväksytyt jäännösriskit. (ISO/IEC 27005:2022: 36–37.)

4.3.6 Hallintajärjestelmän prosessien hyödyntäminen

Tietoturvallisuuden hallintajärjestelmän prosessin osuudet täydentävät tietoturvariskien hallintaa. Riskienhallinnan standardissa ISO/IEC 27005 annetaan toteuttamisohjeita luvussa 4.2 avatun ISO/IEC 27001 -standardin kohtien 4-10 ja tämän hallintajärjestelmän hyödyntämisestä.

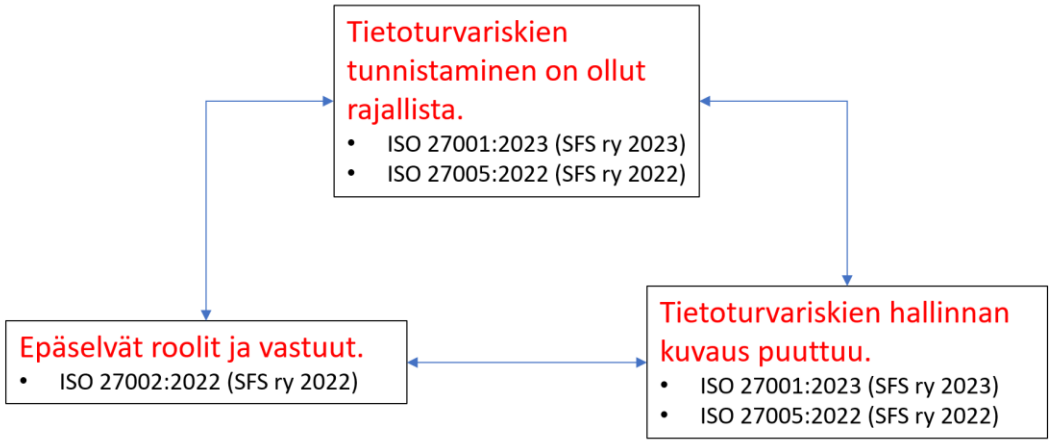
Hallintajärjestelmän hyödyntäminen tuo muun muassa perustana toimintaympäristön osalta tarpeen ymmärtää ulkoisten ja sisäisten tekijöiden vaikutukset riskeihin sekä näiden vaikutuksia hallintajärjestelmän tuloksiin. Rajoittaviakin vaikutuksia voi ilmetä tietoturvatavoitteiden osalta riskien hyväksymiskriteereille ja tietoturvapolitiikan kautta riskienkäsittelylle.

Hallintajärjestelmässä määritellyt johdon katselmukset todentavat riskienkäsittelysuunnitelman toimivuutta ja toteutumista. Sisäisten tai ulkoisten auditointien pohjalta toteutettujen korjaaviin toimenpiteisiin voidaan tarttua katselmuksissa käsitellyin aihein. Mahdollisia toteutusvaihtoehtoja tietoturvariskien käsittelysuunnitelmaa päivittämiseksi on esimerkiksi tietoturvariskien käsittelyprosessin tuloksien huomioiminen toteuttamalla suunnitelmaa asteittain ja ottaa huomioon mahdolliset tekniset tai taloudelliset vaikeudet, sisäiset ristiriidat tai ulkoisten tekijöiden vaikutukset.

Organisaation toiminnan jatkuvan parantamisen sekä seurannan ja katselmoinnin toteuttamisella toimintaa voidaan kypsyttää pitäen tietoturvariskien hallintaprosessin liiketoimintatavoitteiden kannalta olennaisena prosessia päivittäessä. Tärkeänä huomiona on muutoshallintaprosessin jatkuva palautteen anto riskienhallintaprosessille, jolloin tekniset toteutukset tietojärjestelmissä pystytään huomioimaan riskien arvioinnissa. (ISO/IEC 27005:2022: 37–45.)

4.4 Yhteenveto teoreettisesta viitekehyksestä

Insinöörityössä yrityksen nykytilan analyysissa havaittuihin heikkouksiin haettiin ratkaisuja teoreettisessa viitekehyksessä ISO/IEC 27000 -tuoteperheestä valituilla standardeilla alla olevan kuvan 8 mukaisesti.



Kuva 8 Käsitekehys heikkouksiin vastaavista aineistoista

Havaituista heikkouksista ensimmäisenä aloitetaan tietoturvariskien hallinnan kuvauksen puuttumisesta. Lähdetiedoiksi valikoitui tietoturvallisuuden hallintajärjestelmän standardi ISO/IEC 27001, joka tarjoaa reunaehdot hallintajärjestelmän kuvaukselle ja sitä myöden koskettaen riskienhallintasuunnitelmaa. Tietoturvariskien hallinnan standardin ISO/IEC 27005 kautta muodostuvat ohjeet, sisältö ja käytänteet riskienhallintasuunnitelman sisällölle.

Toisena heikkouksista olevan epäselvien roolien ja vastuiden määrittelyn lähdetietona toimii ISO/IEC 27002 -tietoturvallisuuden hallintakeinot. Valittu standardi avaa tietoturvan 93 hallintakeinon sisältöä kuvaten hallintakeinon tarkoituksen, ohjeistuksen ja mahdolliset lisätiedot. Standardissa avattu hallintakeinojen sisältö edesauttaa ymmärtämään ja kohdistamaan vastuita.

Kolmantena heikkouksista tietoturvariskien puutteellisen tunnistamisen lähteiksi valikoitui tietoturvallisuuden hallintajärjestelmän standardi ISO/IEC 27001 ja tietoturvariskien hallinnan standardi ISO/IEC 27005. Standardeista tulevat määritelmät ja ohjeet tukevat tietoturvariskien tunnistamista. Toimintaympäristön ymmärtäminen ja tietoturvariskien hallinnan prosessi ohjaavat kohti tietoturvariskien tunnistamista.

Teoreettinen pääpaino pitäytyy insinöörityön aiheen kannalta keskeisenä pidetyn tietoturvariskien hallinnan ISO/IEC 27005 -standardin ympärillä. Teoreettisessa viitekehyksessä tietoturvallisuuden hallintajärjestelmän ja hallintakeinojen standardien rooli on tietoturvariskien hallinnan standardin ympäristöä selittävä.

5 Kehitysehdotukset tietoturvariskienhallintaan

Tässä luvussa käsitellään kehitysehdotuksen muodostumista. Luvussa kuvaillaan kehitysehdotuksen rakentumista, teoreettisen viitekehyksen ja heikkouksien linkittymistä, esitetään kehitysehdotus ja lopuksi kerätään asiat yhteen muodostaen Data 2:n mukaisen kehitysehdotuksen.

5.1 Kehitysehdotuksen rakentuminen

Kehitysehdotus pohjautuu insinöörityön tähän asti käsiteltyihin aiheisiin, kuten kuvasta 9 on nähtävissä. Data 1:n pohjalta käsiteltiin nykytilan analyysiä, josta muodostui kuvaukset vahvuuksista ja heikkouksista. Insinöörityön teoreettinen osuus muodostaa toisen osuuden syventävänä tietona ohjeet ja suositukset kehitysehdotuksen rakentamiseksi. Tässä luvussa aiheina ovat työpajat ja Data 2:n mukainen kehitysehdotuksen muodostuminen.

Kuva 9 Kehitysehdotuksen vaiheet

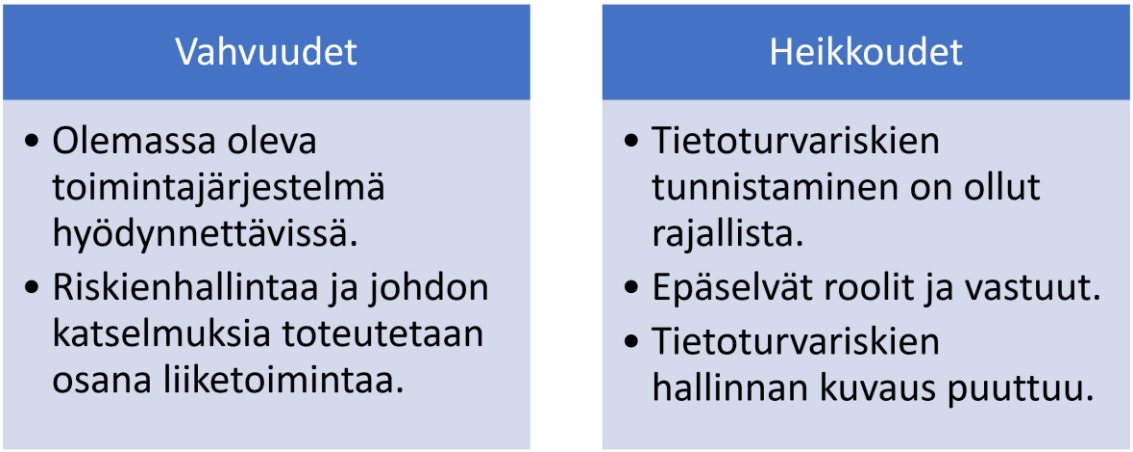
Kehitysehdotuksen rakentumisen ensimmäisen osuuden nykytilan analyysin heikkoudet ovat tietoturvariskien hallinnan kuvauksen puuttuminen, epäselvät roolit ja vastuut sekä tietoturvariskien puutteellinen tunnistaminen. Tunnistettujen heikkouksien pohjalta valittiin ISO/IEC 27000 -standardiperheen standardit ISO/IEC 27001, ISO/IEC 27002 ja ISO/IEC 27005. Valituilla standardeilla haettiin toimintatapoja ja ohjeita, jotka tarjoavat lähtötiedot Data 2:n muodostamiseen.

Data 2 muodostuu viikoittaisien projektiryhmän tapaamisien ja erillisien työpajojen pohjalta. Viikoittaisissa projektiryhmän tapaamisissa käsiteltiin insinöörityön etenemistä ja seuraavia askeleita, joista relevanttina tämän insinöörityön kannalta tietoturvariskienhallinnan työpajojen aikatauluttamista.

Työpajoihin pohjana toimi ISO/IEC 27001 -standardin liite A:n 93 hallintakeinoa, joita käsiteltiin aihealueittain ja muodostettiin case-yrityksen toimintaa kuvaava riskikartta. Projektiryhmässä toimivan ulkoisen konsultin kautta mahdollistui neuvot ja pohjaesitykset, joita sovellettiin kehitysehdotukseen. Insinöörityön kehitysehdotus on kaksiosainen. Kehitysehdotuksen muodostaa tietoturvariskienhallinnan kuvaus ja tietoturvariskeistä muodostuva riskikartta.

5.2 Avainlöydökset nykytilan analyysistä

Luvussa 3 luotu nykytila-analyysi pohjautui keväällä pidettyihin työpajoihin ja näistä muodostuneeseen GAP-analyysiin ISO/IEC 27001 -sertifioitumisen näkökulmasta. Kuvan 10 mukaisesti case-yrityksen vahvuuksina havaittiin olemassa oleva toimintajärjestelmä hyödynnettäväksi ja laajennettavaksi myös tietoturvaan perustuvaan dokumentoinnin hallintaan. Toisena vahvuuksista on HSEQ-toiminnoista käytäntö riskienhallinnasta ja johdon katselmuksista, joita toteutetaan osana liiketoimintaa.



Kuva 10 Avainlöydökset nykytilan analyysistä

Vastaavasti nykytilan analyysistä heikkouksina nousi tietoturvariskien puutteellinen tunnistaminen, epäselvyydet tulevissa rooleissa ja vastuiden määrittelyssä sekä tietoturvariskien hallinnan kuvauksen puuttuminen.

5.3 Avainlöydökset kirjallisuudesta

Luvussa 4 käsiteltiin ISO/IEC 27000 -standardisarjaa ja siihen sisältyviä standardeja, ISO/IEC 27001 -tietoturvallisuuden hallintajärjestelmä, ISO/IEC 27002 -tietoturvallisuuden hallintakeinot ja ISO/IEC 27005 -tietoturvariskien hallinnan standardi. Luku avaa ylätasolla käsiteltävien aiheiden sidonnaisuutta toisiinsa.

Luvussa 4.1 käsiteltiin ISO/IEC 27001 -tietoturvallisuuden hallintajärjestelmää, joka sisälsi hallintajärjestelmän kohtien 4–10 läpikäynnin. Luvun sisältö tarjoaa reunaehdot hallintajärjestelmän kuvaukselle ja sitä myötä koskettaen tietoturvariskien hallinnan suunnitelmaa.

Luvussa 4.2 käsiteltiin ISO/IEC 27002 -tietoturvallisuuden hallintakeinoja, joka avaa tietoturvan 93 hallintakeinon tarkoituksen, ohjeistuksen ja mahdolliset lisätiedot. Standardissa avattu hallintakeinojen sisältö edesauttaa ymmärtämään ja kohdistamaan vastuita.

Luvussa 4.3 käsiteltiin ISO/IEC 27005 -tietoturvariskien hallinnan standardia. Luvussa käsiteltiin tietoturvariskien suunnittelemista ohjaavaa sisältöä ja kuvattiin tietoturvariskien hallinnan prosessi. Luvun sisältö antaa ohjeet, sisällön ja käytänteet riskienhallintasuunnitelmaan.

5.4 Kehitysehdotus

Tässä luvussa käsitellään insinöörityöstä muodostuva kehitysehdotus. Kehitysehdotus muodostuu kahdesta kokonaisuudesta, jotka ovat tietoturvariskien hallinnan kuvaus ja riskikartta.

5.4.1 Tietoturvariskien hallinnan kuvaus

Ensimmäinen kehitysehdotus on tekstitiedostona oleva tietoturvariskien hallinnan kuvaus, joka toimii riskienhallinnan suunnitelmana. Dokumenttia luodessa on huomioitu tietoturvan standardit ISO ISO/IEC 27001 ja ISO ISO/IEC 27005 sekä NIS2 EU-direktiivin ilmoitusvelvollisuudet valvovalle viranomaiselle.

Kuvauksen toteuttamisessa on hyödynnetty jo olemassa olevia case-yrityksen käytänteitä ja kerätty ne dokumenttiin.

Riskinhallintajärjestelmä kuvaus

Sisältö

Kuva 11 Tietoturvariskien hallinnan kuvauksen sisältö

5.4.2 Riskikartta

Toisena kehitysehdotuksena on Excelissä oleva riskikartta tunnistettujen tietoturvariskien luetteloimiseksi sekä näiden arvioimiseen ja käsittelyyn. Riskikartan luomiseksi toteutettiin kesäkuussa, elokuussa ja syyskuussa yhteensä 7 kappaletta noin puolen päivän mittaisia työpajoja projektiryhmän kesken. Riskikartan toteuttamisessa keskeisenä määrittelynä toiminnalle on tietoturvariskien hallinnan kuvaus sekä ISO/IEC 27001 -standardin liite A:n 93 hallintakeinoa.

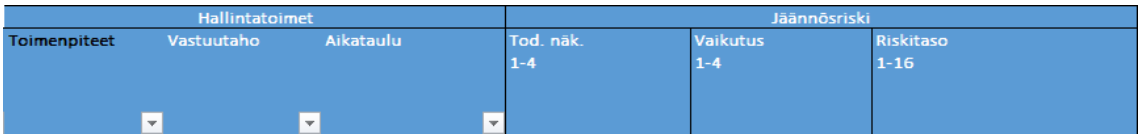
Riskit jaetaan viiteen eri kategoriaan, jotka ovat

- loppukäyttäjät
- tietojärjestelmät
- toimitusketju ja kumppanit
- fyysinen tietoturva
- tietoliikenne ja tietoturva.

Tunnistetut riskit kuvataan ja arvioidaan kuvan 12 mukaisiin sarakkeisiin. Riskien todennäköisyys ja vaikutus arvioidaan asteikolla 1-4, joiden yhteiskertoimesta muodostuu riskiluokka. Tunnistettuihin riskeihin arvioidaan uhkat jatkuvuuteen tai turvallisuuteen, henkilötietojen turvallisuuteen sekä vaatimustenmukaisuuden toteutumiseen.

Kuva 12 Riskikartta-arviointi ja kategoriat

Tunnistettuihin riskeihin voidaan antaa lisätietoja, jotka tukevat riskien hallitsemista ja jäännösriskin määrittämistä. Kuvassa 13 on nähtävissä riskikartan loput sarakkeet, joissa määritellään toimenpiteet, riskin omistaja, millaisella aikataululla hallintatoimia ollaan tekemässä ja käsittelyn lopuksi määritetään jäännösriski riskien todennäköisyyden ja vaikutuksen arvioinnin mukaisesti tehtyjen toimenpiteiden jäljiltä.



Kuva 13 Riskikartan hallintakeinot ja jäännösriski

Tunnistettuja riskejä, niiden sisältöä, arviointia tai hallintatoimia ei insinöörityössä avata riskien arkaluonteisuuden vuoksi.

5.5 Vahvuudet osana kehitysehdotusta

Kehitysehdotuksessa on huomioitu nykytilan analyysissa havaitut case-yrityksen vahvuudet. Havaitut vahvuudet ovat olemassa oleva toimintajärjestelmä hyödynnettäväksi sekä riskienhallinnan ja johdon katselmuksien toteuttaminen osana liiketoimintaa. Kehitysehdotuksien alustavat tuotokset on viety toimintajärjestelmään täydentämään HSEQ:n pohjalta olevia tiedostoja ja käytänteitä.

5.6 Kehitysehdotuksen yhteenveto

Projektiryhmän yhdessä tekemä kehitysehdotus muodostuu tietoturvariskien hallinnan kuvauksesta ja riskikartasta. Dokumentit on lisätty osaksi case-yrityksen käytössä olevaa toimintajärjestelmää.

Seuraavassa luvussa käsitellään palaute kehitysehdotuksesta ja annetaan insinöörityön kannalta lopullinen kehitysehdotus.

6 Palaute kehitysehdotuksesta

Tässä luvussa kuvataan alustavan kehitysehdotuksesta lopulliseen kehitysehdotukseen etenemistä.

6.1 Lopullisen kehitysehdotuksen toteutus

Kehitysehdotuksen muodostama kokonaisuus esitettiin case-yrityksen talousjohtajalle ja operatiiviselle johtajalle kahdessa osassa. Saatujen kommenttien perusteella kehitysehdotusta tarkasteltiin ja toteutettiin sovellettavat muutokset.

6.2 Saadut palautteet

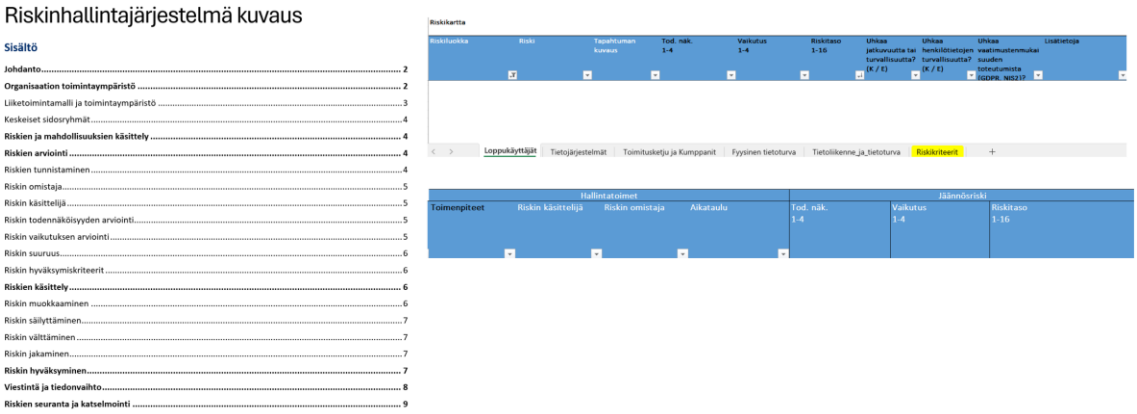
Palautteina ja havaintoina nousi kaksi erillistä nostoa. Ensimmäisenä oli riskimatriisin laajentaminen kaksiulotteisesta kolmiulotteiseen, jossa uutena attribuuttina olisi havaitseminen. Riskin toteutumisen havaitsemisen lisääminen laajentaisi nykyisen 1-16 riskimatriisin kertoimen 1-64.

Toisena havaintona nousi riskin omistajan rinnalle riskin käsittelijä. Tarkastelussa havaittiin, että tunnistetuille riskeille määritellyillä omistajilla ei ole vastuuta tai riittäviä valtuuksia riskin hallitsemiseksi. Riskin omistajat täytyi korottaa organisaation ylemmälle portaalle ja määrittää myös käytännön toteuttaja.

6.3 Lopullisen kehitysehdotuksen yhteenveto

Saatujen palautteiden pohjalta kehitysehdotusta viimeisteltiin lopulliseen versioon. Esille nousseina palautteina ja havaintoina olivat riskimatriisin laajentaminen ja riskin käsittelijän lisääminen

Havaintona noussut riskin omistajan lisäksi riskin käsittelijän huomioiminen nostettiin molempiin kehitysehdotuksen osiin kuvan 14 mukaisesti. Liitteessä 1 riskinhallintajärjestelmän kuvauksessa riskin käsittelijän rooli kuvattiin omana kohtana. Liitteessä 2 riskin käsittelijä nostettiin riskikartalle omana kolumninaan.



Kuva 14 Lopullinen kehitysehdotus

Riskimatriisin laajentaminen kaksiulotteisesta kolmiulotteiseen jätettiin insinöörityön osalta toteuttamatta. Kolmannen attribuutin lisääminen olisi tuonut lisää syvyyttä ja laajemman skaalan ymmärtämään eri näkökulmista riskin toteutumisen tasoa. Huomionarvoisena oli kuitenkin, että tämä olisi tuonut epätarkkuutta riskitason määrittelyyn riippuen riskin arvioijasta. Insinöörityössä päätettiin mennä tämän osalta linjassa ISO/IEC 27005 -standardin kanssa ja pitäytyä kaksiulotteisessa riskimatriisissa.

7 Yhteenveto

Tässä luvussa kuvataan yhteenveto ja johtopäätökset insinöörityöstä. Osion muodostaa neljä osuutta, jotka ovat insinöörityön yhteenveto, seuraavat askeleet riskienhallinnan jalostamisessa, insinöörityön arviointi ja päättävänä loppusanat.

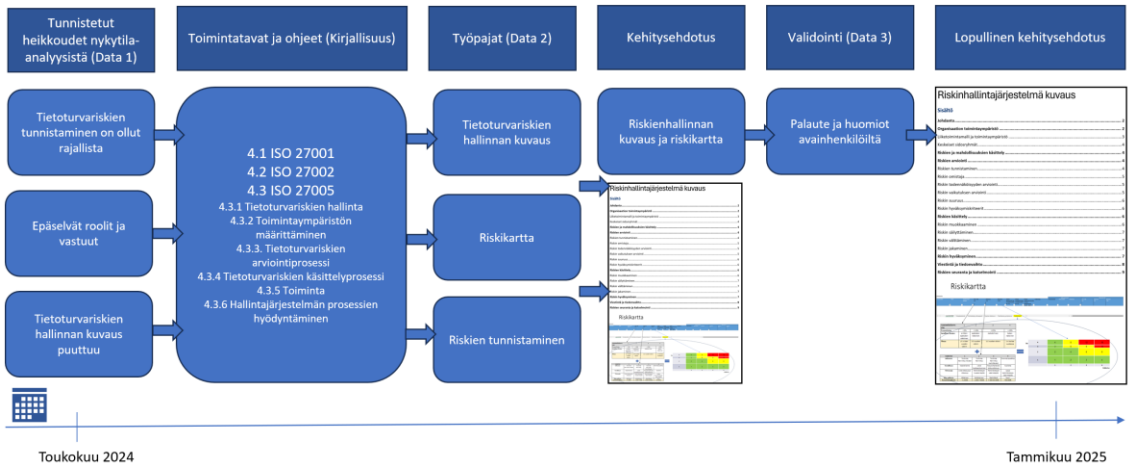
7.1 Insinöörityön yhteenveto

Tietoturva on aiheena noussut aiempaa enemmän yhteiskunnassa esille muuttuvassa ympäristössä. Tätä myöden siihen reagoidaan myös lainsäädännöllisesti. Euroopan unioni on asettanut NIS2-kyberturvallisuusdirektiivin, joka täytyi toimeenpanna kansallisesti 17.10.2024 mennessä. NIS2 EU -direktiivi asettaa vaatimuksia keskeisille ja tärkeille toimijoille, joihin case-yrityksen täytyy myös

vastata. Haasteena havaittiin, ettei elektroniikkateollisuuden parissa toimivan case-yrityksen tietoturvan dokumentoinnin taso vastaa näihin vaatimuksiin.

Insinöörityön tavoite on muodostaa ehdotus case-yrityksen tietoturvariskien hallinnan kehittämiseksi osana ISO/IEC 27001:2022 -sertifioitumista.

Insinöörityö koostuu kuudesta vaiheesta. Kuvassa 15 kuvataan yhteenveto näistä vaiheista.



Kuva 15 Insinöörityön prosessimalli

Kuvan 15 ensimmäisessä vaiheessa toteutettiin case-yrityksen nykytila-analyysi. Nykytila-analyysin pohjana toimi kevään 2024 aikana ulkoisen konsultin tekemä GAP-analyysi, jossa verrattiin case-yrityksen nykyisen liiketoiminnan suorituskykyä ISO/IEC 27001 -standardin vaatimuksiin. Avainlöydökset analyysistä on esitetty luvussa 3.4. Tunnistettuina heikkouksina olivat tietoturvariskien puutteellinen tunnistaminen verrattuna standardin vaatimuksiin, epäselvät roolit ja vastuut sekä tietoturvariskien hallinnan kuvauksen puuttuminen.

Nykytila-analyysin heikkouksien pohjalta edettiin valitsemaan tarvittava kirjallisuus. Kirjallisuus muodostui ISO/IEC 27001-, ISO/IEC 27002- ja ISO/IEC 27005 -standardeista. Keskeisimpänä insinöörityön kannalta oli ISO/IEC 27005 -standardi, joka antaa ohjeet tietoturvariskien hallintaan. Luvussa 4.4 kuvataan teoreettinen viitekehys.

Seuraavassa vaiheessa suoritettiin työpajat. Työpajoissa projektiryhmän jäsenet käsittelivät tietoturvariskien hallinnan kuvausta, joka kuvaa riskienhallinnan prosessia. Lisäksi luotiin riskien tunnistamiseen ja käsittelyyn sopiva riskikartta ja tunnistettiin keskeiset riskit case-yrityksen toiminnalle. Luvussa 5 kuvataan kehitysehdotuksen rakentumista. Luvussa tuotoksena syntyy riskienhallinnan kuvaus ja riskikartta.

Luvussa 6 validoitiin tuotoksia. Kehitysehdotus esiteltiin kahdessa osassa case-yrityksen talousjohtajalle ja operatiiviselle johtajalle. Esittelyistä nousseet palautteet ja huomiot riskienhallinnan kuvaukselle ja riskikartalle veivät kohti lopullista kehitysehdotusta. Havainnollistavat kuvat lopullisista kehitysehdotuksista on insinöörityön liitteinä 1 ja 2.

7.2 Seuraavat askeleet riskienhallinnan jalostamisessa

Seuraavina askeleina kehitysehdotukset valmistellaan johtoryhmän hyväksyttäväksi. Tietoturvariskien hallinnan kuvaukseen täydennetään avoimeksi jätetyt vastuut ja roolit organisaation sisältä. Kuvaus tulee ohjaamaan käytäntöön vientiä riskikartan osalta. Riskikarttaan tunnistettuja riskejä käsitellään riskin omistajan ja tämän määrittelemän riskin käsittelijän yhteistyöllä. Riskienhallinta ja riskikartta ovat jatkuvan kehittämisen piirissä. Näitä käydään säännöllisesti läpi, sisäiset auditoinnit tukevat riskienhallinnan vaikuttavuutta.

Tietoturvariskien käsittelyn käytäntöön tuomisen jälkeen ollaan askeleen lähempänä ISO/IEC 27001 -sertifikaatin vaatimuksia. Riskikartan täydennyttyä aloitetaan pilotti tietoturvariskien viemisestä Excel-taulukosta toimintajärjestelmään uudelle riskit-välilehdelle.

7.3 Insinöörityön arviointi

Insinöörityön kehityshaastena on, ettei case-yrityksen tietoturvan dokumentoinnin taso vastaa NIS2 EU -direktiivin vaatimuksia. NIS2 EU -direktiivin asettamat vaatimukset keskeisille ja tärkeille toimijoille koskettavat myös case-yritystä.

Insinöörityön tavoitteena on muodostaa ehdotus case-yrityksen tietoturvariskien hallinnan kehittämiseksi osana ISO/IEC 27001:2022 -sertifioitumista.

Case-yrityksen tietoturvariskien hallinnan nykytilanteen analyysin havainnoista tunnistaa puutteet suhteessa tavoitteeseen. Havaittuina puutteina nousee rajallinen tietoturvariskien tunnistaminen, epäselvät roolit ja vastuut sekä dokumentoitu kuvaus tietoturvariskien hallinnasta. Valittu kirjallisuus ISO/IEC 27000 -standardiperheestä pohjautuu vastaamaan nykytila-analyysin heikkouksiin mahdollistaen kehitysehdotuksen luomisen tietoturvariskien hallintaan.

Lopputuloksena case-yritykselle muodostuu tekstitiedosto tietoturvariskien hallinnan kuvauksesta ja Excel-tiedostona oleva riskikartta noin 60 tunnistetulla riskillä. Insinöörityön tavoite oli kehittää case-yrityksen tietoturvariskien hallintaa osana ISO/IEC 27001:2022 -sertifioitumista. Dokumentoidut käytänteet ja tunnistetut riskit ovat keskeinen alue NIS2 EU -direktiivin vaatimusten ja onnistuneen ISO/IEC 27001:2022 -sertifioitumisen näkökulmasta. Tämän perusteella insinöörityön kehitysehdotuksen lopputulos vastaa asetettua tavoitetta.

Insinöörityössä tehty suunnitelma kuvastaa totuudenmukaista etenemistä kohti asetettua tavoitetta. Luvuissa muodostuvat tuotokset vievät insinöörityötä vaiheittain eteenpäin, nämä linkittyvät toisiinsa luoden laadukkaan kokonaisuuden. Insinöörityössä sanoin ja kuvin esitetyt vaiheet ovat osoitus projektin toteutumisesta. Insinöörityössä tehdyt löydökset, ratkaisut ja tulkinnat ovat perusteltuja riittävällä tietoperustalla, joka pohjautuu kirjallisuuteen ja case-yrityksen osallistamiseen.

Insinöörityössä on otettu huomioon ja osallistutettu toimeksi antanutta case-yritystä. Kehitysehdotus luotiin yhteistyönä projektiryhmän kanssa, joka koostui itseni lisäksi ulkoisesta konsultista, IT-asiantuntijasta ja HSEQ-päälliköstä. Projektiryhmä tapasi pääsääntöisesti viikoittain. Tapaamisten tavoitteena oli seurata dokumentaation etenemistä ja tarjota mahdollisuuden kysyä kysymyksiä konsultilta. Toiminnasta raportoitiin ohjausryhmälle, jonka kokoonpanoon kuului

ulkoisen konsultin ja minun lisäksi yrityksen johdosta talousjohtaja ja operatiivinen johtaja. Ohjausryhmä tapasi 1-2 kuukauden välein.

Insinöörityötä koskeva dokumentaatio käsiteltiin talousjohtajan ja operatiivisen johtajan kanssa, josta saatujen palautteiden pohjalta tehtiin täsmennyksiä ennen dokumenttien ottamista johtoryhmän käsittelyyn ja hyväksymiseksi. Tietoturvariskien hallinnan ollessa jatkuvaa kehittämistä näitä käsitellään säännöllisesti ja toimintatapojen vaikuttavuutta todennetaan sisäisillä auditoinneilla.

Insinöörityön dokumentaatio pohjautuu standardoitujen toimintamallien soveltamiseen case-yrityksessä. Lukijalle insinöörityö mahdollistaa näkökulman saamisen tietoturvariskien hallintaan ja tähän liittyvän dokumentaation rakentamiseen. Laadukas tietoturvariskien hallinta on yksi merkittävimmistä keinoista parantaa yrityksen tietoturvaa.

7.4 Loppusanat

Insinöörityön aihe tarjosi mahdollisuuden kehittää ammattitaitoani uuteen suuntaan ja avasi oven, josta löytyy urapolku tietoturvan parissa. Aihe on ollut haastava, kärsivällisyyttä vaativa, mutta myös opettavainen. Olen kiitollinen saamastani mahdollisuudesta ja luottamuksesta työskennellä yrityksessäni kyseisen projektin parissa. Insinöörityön jälkeen pääsen jatkamaan työtäni vieden yritystä kohti ISO/IEC 27001 -sertifioitumista.

Lähteet

Tietosuojalaki. 2018. 1050/5.12.2018.

Hallituksen esitys Euroopan unionin kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. 2024. HE 57/2024.

ISO/IEC 27001:2022 – Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardoimisliitto SFS ry. Verkkoaineisto. Vaatii käyttöoikeuden. <https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1155761.html.stx>. Luettu 19.11.2024.

ISO/IEC 27002:2022 – Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. Helsinki: Suomen Standardoimisliitto SFS ry. Verkkoaineisto. Vaatii käyttöoikeuden. <https://sales.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/2/1161362.html.stx>. Luettu 19.11.2024.

ISO/IEC 27005:2022 – Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Ohjeita tietoturvariskien hallintaan. Helsinki: Suomen Standardoimisliitto SFS ry. Verkkoaineisto. Vaatii käyttöoikeuden. <https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1232324.html.stx>. Luettu 21.11.2024.

Tietoturvariskien hallinnan kuvaus

Riskinhallintajärjestelmä kuvaus

Sisältö

Riskikartta

Yritys X

Riskinarviointi Kyberriskit

Riskikartta

										Hallintatoimet				Jäännösriski		
Riskiluokka	Riski	Tapahtuman kuvaus	Tod. näk. 1-4	Vaikutus 1-4	Riskitaso 1-16	Uhkaa jatkuvuutta tai turvallisuutta? (K / E)	Uhkaa henkilötietojen turvallisuutta? (K / E)	Uhkaa vaatimustenmukaisuuden toteutumista (GDPR, NIS2)? (K / E)	Lisätietoja	Toimenpiteet	Riskin käsittelijä	Riskin omistaja	Aikataulu	Tod. näk. 1-4	Vaikutus 1-4	Riskitaso 1-16
ICT/Tiedon suojaaminen	Esimerkki riski 1. Tietovuoto	Loppukäyttäjä kirjautuu phishing-sivulle vuotaen yrityksen luottamukselliset tiedot	3	4	12	K	E	K	Loppukäyttäjä ei käsittele henkilötietoja tai laskuja työtehtävissään. Tästä huolimatta saatuja tietoja voidaan käyttää aiheuttamaan haittaa yritykselle.	Koulutetaan henkilöstöä tunnistamaan phishing hyökkäykset ja ilmoitetaan koko henkilöstölle, mikäli näitä esiintyy.	Pekka Käsittelijä	Risto Omistaja				
Kyberpuolustuksen puutteet	Esimerkki riski 2 Ohjelmistojen valvomaton lataaminen	Loppukäyttäjä asentaa sovelluksia, jotka eivät ole työtehtävien kannalta oleellisia tai luotettavia.	1	1	1	K	K	K	Loppukäyttäjillä ei ole pääkäyttäjän valtuuksia ladata sovelluksia laitteilleen.	Nykyisellä toimintamallilla ei vaadi toimenpiteitä.	Taina Käsittelijä	Risto Omistaja				
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											
					0											

Loppukäyttäjät | Toimitusketju ja Kumppanit | Tietojärjestelmät | Fyysinen tietoturva | Tietoliikenne_ja_tietoturva | Riskikriteerit