
# TIETOTURVALLISUUS-JOHTAMISJÄRJESTELMÄN RAKENTAMISEN VAIHEET

12/2016

Artikkelin on kirjoittanut Arterin perustaja ja QF-kouluttaja Jussi Moisio.

# TIETOTURVALLISUUSJOHTAMISJÄRJESTELMÄN RAKENTAMISEN VAIHEET

**Vaihe**

| Vaihe | |
|---|---|
| 1 | Johto on määritellyt liiketoiminnalliset perustelut sille, miksi TT-turvallisuusjohtamisjärjestelmää lähdetään ylipäätään rakentamaan? Mitä liiketoiminnallista ym. hyötyä sitoutumisesta jatkuvaan parantamiseen tietoturvallisuuden parantamiseen yritys saa? |
| 2 | Johto on hyväksynyt TT-hallintajärjestelmäprojektin ja antanut sen aloittamiselle hyväksynnän. |
| 3 | Projektin avainhenkilöstölle on annettu peruskoulutus TT-järjestelmään: mistä on kyse ja millaista tekemistä, rakenteita, selvityksiä, riskien ja mahdollisuuksien hallintaa TT-järjestelmä edellyttää. Tehdäänkö työ omin voimin? Missä määrin ulkoista asiantuntijaa tarvittaessa käyttäen? |
| 4 | Projektiryhmä on määritelty ja projektipäällikkö nimetty (usein tietoturvapäällikkö) sekä edustajat on nimetty keskeisistä toiminnoista tai osastoilta tai prosesseilta (IT, ICT-ammattilaisia ja muita yrityksen eri toimintojen osaajia. |
| 5 | Projektiryhmä on määritellyt, milloin ja missä asioissa tullaan käyttämään ulkopuolista asiantuntemusta. |
| 6 | TT-ohjausryhmä nimetty (tai voi olla suoraan johtoryhmä), jossa projektipäällikkö mukana ja johdon edustajat on nimetty. |
| 7 | Projektiryhmä on määritellyt vastuuhenkilöt, joiden tehtävänä on tunnistaa yrityksen toimintaan liittyvät soveltuvat TT-lait, -asetukset, viranomaisvaatimukset ja muut sitoumukset, joihin yritys on TT-mielessä sitoutunut suojatakseen tieto-omaisuuttaan. |

**Vaihe**

| | |
|---|---|
| 8 | Projektiryhmä on määritellyt TT-hallintajärjestelmän rakentamisessa sovellettavat ohjauskokoukset ja raportointitavat. |
| 9 | Projektiryhmä on määritellyt vastuut ja menettelyn, kuinka tietoturvaan liittyvien lakisääteisten ym. vaatimusten tunnistuslistaa tullaan jatkossa päivittämään. |
| 10 | Projektiryhmä on määritellyt TT-hallintajärjestelmän kattavuuden (suojattavat kohteet) ja ohjausryhmä on hyväksynyt sen. |
| 11 | Projektiryhmä on määritellyt TT-hallintajärjestelmän rakenteen, mm. mistä tasoista järjestelmä koostuu ja miten järjestelmässä toteutuu Plan-Do-Check-Act. |
| 12 | TT-hallintajärjestelmäprojektisuunnitelmassa on otettu huomioon tietoturvahallinnan olennaiset avainasiat, kuten tietoturvapolitiikka, viestintä, operatiivinen johtaminen, pääsynhallinta, tietojärjestelmien hankinta, kehittäminen ja ylläpito, organisointi, omaisuudenhallinta, TT-poikkeamien hallinta, jatkuvuudenhallinta, henkilöturvallisuus, fyysinen ja ympäristön turvallisuus, vaatimustenmukaisuus jne. |
| 13 | Projektiryhmä on määritellyt riskien ja mahdollisuuksien tunnistamistavan (tietoturvariskien arviointiprosessi), tunnistamisessa käytettävät työpohjalomakkeet ja tietoturvariskien merkittävyyden arvioinnissa käytettävän todennäköisyyksien ja seurausten vakavuuksien pisteytysasteikon. |
| 14 | Projektiryhmä on määritellyt, miten usein TT-riskit ja mahdollisuudet päivitetään koko soveltamislaajuudessa ml. että aina merkittävien muutosten yhteydessä päivitetään ko. kohteen TT-riskit ja mahdollisuudet. |

**Vaihe**

**15** Uhkien ja riskien peruskartoitus on tehty. Tunnistetaan kattavasti yrityksen toiminnassa ilmenevät tietoturvahaavoittuvuudet ja niihin liittyvät uhkatekijät ja aiheuttajat systemaattisesti TT-hallinta-järjestelmään kuuluvien kohteiden osalta. Henkilöstön edustus on otettu mukaan kartoitukseen.

**16** Merkittävät TT-riskit on määritelty käyttäen sovittua riskien merkittävyyden arvottamismenettelyä systemaattisesti koko TT-hallintajärjestelmään sisällytetyssä laajuudessa.

**17** Johto tai ohjausryhmä on määritellyt tietoturvariskien hyväksymis-kriteerit. Hyväksyttäviä riskien tasoja katselmoidaan sovituin väliajoin

**18** Projektiryhmä on määritellyt riskeille käsittelyvaihtoehdot ja määritellyt hallintakeinot kullekin riskille päätetyn käsittelyvaihtoehdon mukaan

**19** Projektiryhmä on käynyt läpi ISO 27001 -liitteen A hallintatavoitteet ja keinot ja laatinut ns. Soveltuvuuslausunnon, joka sisältää kaikki vaaditut hallintakeinot sekä perustelut liitteen A hallintakeinojen käyttämiselle tai käyttämättä jättämiselle.

**20** Projektiryhmä on koostanut eo. pohjalta riskien käsittelysuunnitelman ja hankkinut kunkin riskin omistajalta hyväksynnän ko. riskin käsittelylle ja jäljelle jääville tietoturvariskeille.

**21** Johto tai ohjausryhmä on laatinut organisaatiolle TT-politiikan, jossa sitoudutaan jatkuvaan parantamiseen, lakien, viranomais- ja muiden TT-vaatimusten noudattamiseen, kehittämistavoitteiden asettamiseen. TT-politiikka on dokumentoitu ja siitä viestitään koko organisaatiolle. TT-politiikka on sidosryhmien saatavissa.

## Vaihe

22 Johto tai TT-ohjausryhmä on laatinut tietoturvatavoitteet TT hallintajärjestelmän asiaankuuluville toiminnoille ja tasoille. Tavoitteet ovat mahdollisuuksien mukaan mitattavissa. Tavoitteiden asettamisessa on otettu huomioon soveltuvat TT-vaatimukset ja riskien arvioinnin ja käsittelyn tulokset.

23 Johto tai TT-ohjausryhmä yhdessä projektiryhmän kanssa on laatinut TT-tavoitteiden saavuttamiseksi toimenpiteet, resurssitarpeet, vastuut, aikataulun ja tavat, miten arvioida tavoitteiden saavuttamista.

24 Koko henkilöstölle annetaan TT-asioista peruskoulutusta painottaen sitä, mitä TT-asiat itse kunkin työssä tarkoittavat normaali-, häiriö- ja poikkeustilanteissa ja kuinka tulee toimia. Koulutuksessa kiinnitetään huomiota siihen, millaisiin parannustavoitteisiin koko yritys on sitoutunut ja otetaan esille yrityksen TT-tavoitteet ja mitä ne merkitsevät toiminnoissa / osastoilla/ prosesseissa. Lisäksi korostetaan, mihin itse kunkin tulee reagoida ja ryhtyä joko itse välittömiin toimenpiteisiin tai ilmoittaa eteenpäin (uhka- tai läheltä piti -tilanne, -ongelma, -häiriö- tai poikkeustilanne).

25 Projektiryhmä on määritellyt TT-järjestelmän ylläpitoon liittyvien menettelyiden työstämisen: TT-käsikirjan laatiminen (vapaaehtoinen), kaikille yhteisten TT-ohjeiden laatiminen, asiakirjojen valvontaohjeen laatiminen, TT-tiedostojen valvontaohjeen laatiminen, toimintokohtaisten erityisohjeiden laatiminen, TT-järjestelmän auditointiohjeen laatiminen tai yhdistäminen yleiseen auditointiohjeeseen, samoin on määritelty TT-poikkeamien ja niihin liittyvien korjaavien ja ehkäisevien toimenpiteiden menettelyt jne.

**Vaihe**

26 Projektiryhmä on määritellyt, mitä tulee seurata ja mitata ml. TT-hallintajärjestelmään liittyvät tietoturvaprosessit (tietoturvariskien arviointiprosessi, tietoturvariskien käsittelyprosessi) ja hallintakeinot. Mittaamiseen ja seurantaan on määritelty taajuus, kuinka usein mitataan tai seurataan, ketkä mittaavat tai seuraavat, milloin ja miten kertynyttä tietoa analysoidaan ja miten tulokset dokumentoidaan.

27 Projektiryhmä on määritellyt TT-häiriöiden, -tapahtumien ja -poikkeamien käsittelytavan ja niiden käsittelyssä kirjattavat seikat mm. häiriöihin vastaamisen menettelyt, seurannan ja raportoinnin menettelyt, TT-häiriöiden havaitsemiselle ja raportoinnille nimetty yhteydenottopiste, lomakepohjat, tietoturvarikkomusten käsittely jne.

28 Projektiryhmä on määritellyt toimintojen / osastojen / prosessien edustajat tarkistamaan yksiköissään, mitä muutoksia vastuissa ja valtuuksissa mahdollisesti tarvitaan TT-asioiden takia. Samoin heitä on pyydetty tarkistamaan tiedonkulun valmiudet oikean tiedonkulun varmistamiseksi TT-asioissa

29 Projektiryhmä on määritellyt toimintojen / osastojen / prosessien edustajat arvioimaan, mitä tarkistuksia koulutustarpeiden ja pätevyyksien tunnistamisessa ja valmiuksien luomisessa mahdollisesti tarvitaan TT-asioissa. Erityispätevyyksien (viranomaisten ja / tai sovelletun teknologian hallinnan edellyttämät) osalta tarkistetaan, että ne ovat asianmukaisessa kunnossa.

## Vaihe

30 Projektiryhmä on määritellyt, mitä TT-hallintajärjestelmään liittyviltä ulkoisilta palvelutoimittajilta vaaditaan TT-hallinnassa, sopimuksissa, viestinnässä jne. Esimerkiksi palvelutasot, palveluraportit, seuranta-kokoukset, auditoinnit, tietoturvahäiriöiden hallinta, kirjattavat tiedot, ongelmien ratkaisu, palvelukapasiteetti, jatkuvuus, toimittajan puolelta nimetty vastuuhenkilö, tietoturva arkaluonteisissa tiedoissa, joihin toimittajalla pääsy, tilaajan ja toimittajien tekemät muutokset palveluihin mm. parannukset sovittuun palveluun, uusien sovellusten kehittäminen, TT-turvallisuusparannukset, verkkomuutokset, uusien versioiden käyttöönotot, uudet kehitystyökalut, fyysiset palvelutilojen muutokset, toimittajan muutokset, alihankinnan siirto toiselle alihankkijalle jne

31 Projektiryhmä on määritellyt TT-vaatimukset, joita noudatetaan organisaation projektitoiminnoissa ja järjestelmäkehittämisessä.

32 Johto ja projektiryhmä ovat suunnitelleet TT-auditointien vuosiohjelman ja laatineet sisäisen TT-auditoinnin ohjeen ja lomakkeet.

33 TT-hallintajärjestelmän sisäiset auditoijat on valittu niin IT-, ICT ammattilaisten kuin eri toimintojen asiantuntijoiden joukosta huomioiden työkokemus, koulutustausta, toimialatuntemus, tietoturvatuntemus jne.

34 TT-hallintajärjestelmän sisäisille auditoijille on järjestetty ISO 27001- ja oman TT-hallintajärjestelmän sisältökoulutusta ja auditointiprosessin koulutusta.

35 Ensimmäinen toimintojen / osastojen / prosessien TT-auditointi on suoritettu ja raportoitu.

**Vaihe**

36 Johto yhdessä tietoturvapäällikön ja projektiryhmän kanssa on määritellyt TT-järjestelmän johdon katselmuksen sisällön.

37 Tietoturvapäällikkö on valmistellut ja pyytänyt johdon katselmukseen osallistujia ennakolta valmistelemaan omat osuutensa ensimmäiseen johdon katselmukseen. Katselmus on pidetty ja johtopäätökset on kirjattu katselmuspöytäkirjaan.

38 Johto tai ohjausryhmä on todennut, että TT-järjestelmä on toiminnassa ja on siirrytty ylläpitoon ja järjestelmän edellyttämään jatkuvaan parantamiseen sekä tarvittaessa on luotu valmiudet pyytää ulkoista sertifiointiauditointia.

## TULE OPPIMAAN LISÄÄ KOULUTUKSIIMME!

Ilmoittaudu mukaan osoitteessa: https://www.arter.fi/course_category/qf-koulutukset/

## TAI OTA YHTEYTTÄ

qf@arter.fi

ARTER

www.arter.fi