talous hallinto liitto

Huoltovarmuuskeskus

Tietoturvan arviointi – Arvioijan ohje

Sisällysluettelo

Tietoturva-arvioinnin tarkoitus ja tavoitteet

Tietoturva-arvioinnin tarkoitus ja tavoite

- Tietoturva-arvioinnin (jatkossa ’arviointi’) ja sen tueksi tehdyn arviointityökalun tarkoitus on luoda käsitys taloushallintoalalla toimivan yrityksen tietoturvan nykytilasta ja luoda arvioitavalle yritykselle selkeä kuva siitä, millä toimenpiteillä tietoturvaa voidaan kehittää jatkossa.
- Arviointi on suunniteltu suoritettavaksi yhteistyössä arvioijan ja arvioitavan yrityksen kanssa. Arviointi suoritetaan haastattelujen avulla, joissa vastaaja kertoo yrityksensä tietoturvakäytännöistä ja niiden toteutuksesta.
- Arvioinnin tavoitteena on tukea yritystä tietoturvaan liittyvien riskien tunnistamisessa ja tunnistaa yrityksen tärkeimmät tietoturvaan liittyvät kehityskohteet.

Tietoturva-arvioinnin kulku

Arviointiprosessin eteneminen

1. **Arvioinnin aloitus:** Ennen arviointityökalun lähettämistä suositellaan ns. kick-off-tilaisuutta, jossa arvioija esittelee työkalun, käy läpi sen käyttämisen ja sopii arvioitavan tahon kanssa käytännön järjestelyistä, sekä aikataulusta.
2. **Työkalun täyttö:** Arvioija lähettää arviointityökalun arviointiin osallistuvalle organisaatiolle vähintään viikkoa ennen itse arviointia, jotta arvioitavalla organisaatiolla on aikaa täyttää työkalu ennen yhteistä läpikäyntiä.
3. **Arviointityöpaja:** Arvioija käy yhdessä arvioitavan tahon kanssa läpi vastaukset ja toteutuksien kuvaukset haastattelumuotoisesti, sekä selventää mahdolliset haasteet.
4. **Yhteenveto ja kehityskohteiden tunnistaminen:** Arvioija käy läpi työkaluun täytetyt vastaukset, ja luo arvioitavalle raportin tuloksista ja tunnistetuista kehityskohteista.
5. **Arvioinnin päätöstilaisuus:** Päätöstilaisuudessa arvioija esittelee arvioinnissa esiin nousseet havainnot, kehitysehdotukset ja suosittelee seuraavat toimenpiteet arvioitavalle organisaatiolle.

Arviointiin varattavat resurssit

- Arviointiin tulee varata riittävästi aikaa ja henkilöresursseja, jotta se saadaan saatettua tavoitteeseen.
  - Esimerkki suositelluista resursseista arvioijalle:
    - Henkilöstö: 2 henkilöä (haastattelija, kirjuri)
    - Aloitustilaisuus: 30 min
    - Arviointityöpaja: 4-5 tuntia (+tauot)
    - Arvioinnin konsolidointi: 0,5 htp
    - Päätöstilaisuus: 1 tunti
- Arvioijan tulee varmistaa arvioitavan organisaation sitoutuminen arviointiin varaamalla riittävästi aikaa ja henkilöstöä.

Arvioinnin aloitus

Tavoite: Kick-off-tilaisuuden tarkoitus on varmistaa, että arviointiin osallistuvilla tahoilla on yhteinen näkemys arvioinnin tarkoituksesta, kulusta, arviointilomakkeen täytöstä ja käytännön järjestelyistä.

Kesto: 30 min

Osallistujat: Arvioija; kohdeyrityksestä arviointiin osallistuvat henkilöt

- Ennen arviointityökalun lähettämistä suositellaan ns. kick-off-tilaisuutta, jossa arvioija esittelee työkalun, käy läpi sen käyttämisen ja sopii arvioitavan tahon kanssa käytännön järjestelyistä, sekä aikataulusta.
- Kick-off-tilaisuuden esimerkkiagenda:
  - Arvioinnin tarkoitus
  - Arviointilomakkeen käyttö
  - Käytännön järjestelyistä sopiminen
- Kick-off tilaisuudessa sovitaan, täyttääkö yritys arviointilomakkeen itsenäisesti ennen arviointityöpajaa (suositeltu toimintatapa). Arviointilomakkeen saa käyttöön Taloushallintoliiton verkkosivuilta.

Työkalun täyttö

Tavoite: Työkalun esitäyttäminen ennen työpajaa antaa yritykselle tilaisuuden tutustua rauhassa tietoturvan hallintakeinoihin ja esim. keskustella niiden nykytilanteesta IT-palveluntarjoajansa tai muiden keskeisten sidosryhmien kanssa. Arviointityöpaja kulkee sujuvammin, kun tiedot on jo esikartoitettu.

Kesto: *ei määriteltyä kestoa*

Osallistujat: Kohdeyrityksestä henkilöt, jotka osaavat kuvata hallintakeinojen toteutusta (yrityksestä riippuen esim. johto, tietoturvan vastuuhenkilöt, IT-vastuuhenkilöt).

- Kohdeyritys täyttää itsenäisesti tai yhdessä IT-palveluntarjoajansa kanssa arviointityökalun.
- Yritys täyttää työkaluun kunkin hallintakeinon kohdalle tiedon sen toteuttamisesta ja kirjoittaa lyhyesti kuvauksen toteutuksesta.

Arviointityöpaja

Tavoite: Arviointityöpajan tavoitteena on luoda käsitys yrityksen tietoturvan nykytilasta käymällä läpi arviointityökalu.

Kesto: 4-5 h

Osallistujat: Arvioija; kohdeyrityksestä henkilöt, jotka osaavat kuvata hallintakeinojen toteutusta (yrityksestä riippuen esim. johto, tietoturvan vastuuhenkilöt, IT-vastuuhenkilöt)

- Arviointityöpajassa käydään läpi arviointityökalu kysymys kysymykseltä.
- Arvioija käy yhdessä arvioitavan tahon kanssa läpi vastaukset ja toteutuksien kuvaukset haastattelumuotoisesti, sekä selventää mahdolliset haasteet.
- Arvioijan rooliin kuuluu tukea vastaajaa kysymyksen ymmärtämisessä. Arvioija kirjoittaa “Toteutuksen kuvaus” sarakkeeseen lisätietoja siitä, millä tavalla käytäntöä toteutetaan arvioitavassa yrityksessä.
- Kun arvioinnin yhteydessä havaitaan selkeitä kehittämiskohteita tai erityisen hyvin toteutettuja kokonaisuuksia, sarakkeisiin I ja K voidaan tehdä näihin liittyviä merkintöjä.

Yhteenveto ja kehityskohteiden tunnistaminen

Tavoite: Tavoitteena on luoda selkeä kuva siitä, millä toimenpiteillä tietoturvaa voidaan kehittää jatkossa yrityksessä.

Kesto: noin 0,5 htp

Osallistujat: Arvioija

- Arviointityökalu luo automaattisesti prosentuaalisen ”toteutustason” Tulokset-välilehdelle. Arvioija täydentää tätä sanallisella arvioinnilla, joka perustuu arvioinnin tuloksiin ja arviointityöpajassa käytyyn keskusteluun.
- Arvioija luo arvioitavalle yhteenvedon tuloksista ja tunnistetuista kehityskohteista Kehittämissuunnitelma -välilehdelle.

Arvioinnin päätöstilaisuus

Tavoite: Päätöstilaisuuden tavoitteena on varmistaa, että kohdeyrityksellä on arvioinnin jälkeen selkeä käsitys tietoturvansa nykytilasta ja siitä, millä toimenpiteillä tietoturvaa voidaan kehittää jatkossa.

Kesto: 1 h

Osallistujat: Arvioija; kohdeyrityksestä henkilöt, jotka vastaavat tietoturvan kehittämisestä

- Päätöstilaisuudessa kohdeyritykselle esitellään arvioinnin tulokset ja tunnistetut kehityskohteet ja keskustellaan havainnoista.
- Tilaisuudessa voidaan keskustella esim. tavoista toteuttaa kehityskohteita tai priorisoida niitä.

Työkalun käyttö

Arviointimetodi

Arviointi tietoturvan toteutuksesta taloushallintoalan yrityksessä

Organisaatio	
Arvioinnin osallistujat	
Fasilitaattori	
Päivämäärä	

Arvioinnin status

Hallintakäytännöt	Status
Tietoturvan johtaminen ja riskienhallinta	Ei aloitettu
Henkilöstö ja osaaminen	Ei aloitettu
Asiakassuhteen hoito ja luottamuksellisten tietojen käsittely	Ei aloitettu
Tietosuoja	Ei aloitettu
Käyttövaltuushallinta	Ei aloitettu
Salasanojen ja tunnistautumismenetelmien hallinta	Ei aloitettu
Toimitilaturvallisuus	Ei aloitettu
Poikkeamanhallinta ja häiriöiden havaitseminen	Ei aloitettu
Tekninen ympäristö	
IT-infrastruktuurin ja järjestelmien hallinta	Ei aloitettu
Palvelimet	Ei aloitettu
Tietoverkot	Ei aloitettu
Päätelaitteet	Ei aloitettu
Siirrettävät tietovälineet	Ei aloitettu
Järjestelmät, palvelut ja kumppanit	
Sähköposti	Ei aloitettu
Pilvipalveluiden käyttö	Ei aloitettu
ICT-palveluntarjoajien hallinta	Ei aloitettu

- Arvioinnissa käytetään Taloushallintoliiton ja Huoltovarmuuskeskuksen tuottamaa Tietoturvan arviointityökalua.
- Arviointityökalu koostuu 138 hallintakeinosta, jotka on jaettu 16 aihealueeseen.

Arvioinnin osa-alueet

talous hallinto liitto

Huoltovarmuuskeskus

Hallintakäytännöt

- Tietoturvan johtaminen ja riskienhallinta
- Henkilöstö ja osaaminen
- Asiakassuhteen hoito ja luottamuksellisten tietojen käsittely
- Tietosuoja
- Käyttövaltuushallinta
- Salasanojen ja tunnistautumis-menetelmien hallinta
- Toimitilaturvallisuus
- Poikkeamanhallinta ja häiriöiden havaitseminen

Tekninen ympäristö

- IT-infrastruktuurin ja järjestelmien hallinta
- Palvelimet
- Tietoverkot
- Päätelaitteet

Järjestelmät, palvelut ja kumppanit

- Sähköposti
- Pilvipalveluiden käyttö
- Siirrettävät tietovälineet
- ICT-palveluntarjoajien hallinta

Arviointilomake -välilehti

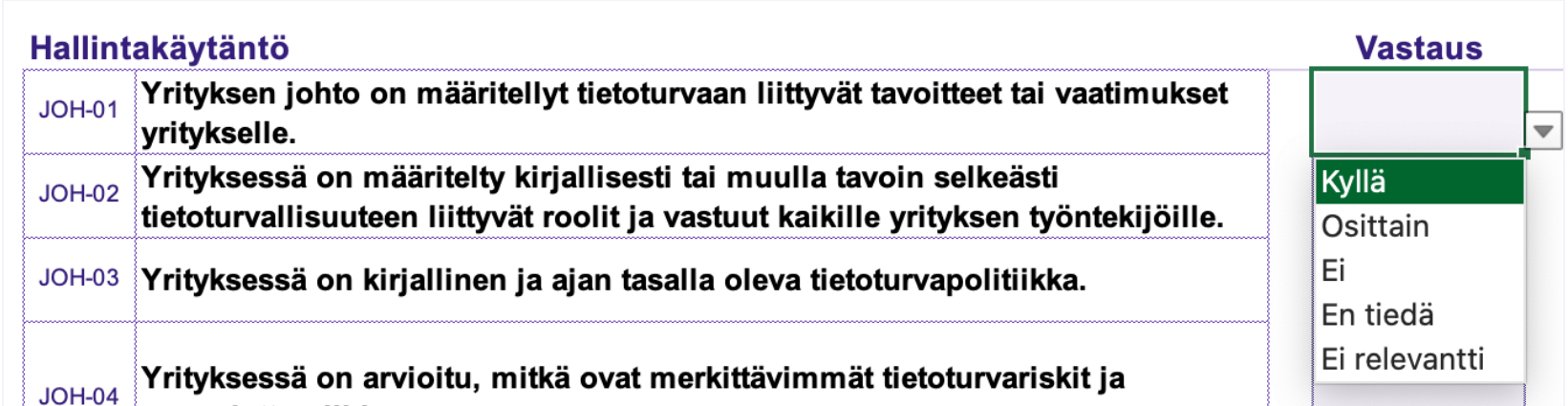
- Arviointityökalussa jokainen hallintakeino on omalla rivillään.
- Hallintakeinoon liittyville tiedoille on kuusi saraketta; Hallintakäytäntö, Vastaus, Toteutuksen kuvaus, Merkintä, Muistiinpanot, Kysymyksen kuvaus/tavoite.

- **Hallintakäytäntö**: sisältää kontrollin, johon vastataan.
- **Vastaus**: Avaa pudotusvalikon, joka sisältää vastausvaihtoehdot; Ei, Osittain, Kyllä, En tiedä, Ei relevantti.
- **Toteutuksen kuvaus**: Tähän täytetään kirjallinen kuvaus kontrollin toteutuksesta.
- **Merkintä**: Avaa pudotusvalikon, jossa voidaan korostaa havaittu kehityskohde, lisäselvitystä vaativa kontrolli, tai erityisen hyvä toteutus.
- **Muistiinpanot**: Arvioija tai yritys itse voi kirjata tähän soluun mahdollisia lisähavaintoja.
- **Tarkoitus/tavoite**: Taustoittaa kysymyksen tarkoitusta ja merkitystä.

Hallintakäytäntö		Vastaus	Toteutuksen kuvaus	Merkintä	Muistiinpanot	Tarkoitus / tavoite
JOH-01	**Yrityksen johto on määritellyt tietoturvaan liittyvät tavoitteet tai vaatimukset yritykselle.**					*Tavoitteiden määrittely kirkastaa*

Hallintakeinon toteutus

- Alasvetovalikosta valitaan vaihtoehto, joka parhaiten kuvaa hallintakeinon toteutusta yrityksessä **arviointihetkellä**.
  - Kyllä = hallintakeino on toteutettu
  - Osittain = hallintakeino on toteutettu osittain (kuvattua asiaa ei ole tehty täysin, mutta toteutusta on tehty)
  - Ei = hallintakeinoa ei ole toteutettu ollenkaan
  - En tiedä = yrityksellä ei ole tietoa siitä, onko hallintakeino toteutettu
  - Ei relevantti = hallintakeino ei ole yrityksen kontekstissa relevantti. Huom! Tätä vaihtoehtoa tulisi käyttää vain tapauksissa, joissa hallintakeinon toteuttaminen ei ole mahdollista (esim. palvelimien suojaaminen, jos yrityksellä ei ole palvelimia).



Arvioinnin valmistuminen

- Arvioinnin valmistumista voi seurata Arviointilomake-välilehdellä kohdassa Arvioinnin status.
- Kun kaikkien osa-alueiden kohdalla on tieto “Valmis”, arvioinnin tulokset voi katsoa Tulokset -välilehdeltä.

Arvioinnin status

Hallintakäytännöt	Status
Tietoturvan johtaminen ja riskienhallinta	Valmis
Henkilöstö ja osaaminen	Valmis
Asiakassuhteen hoito ja luottamuksellisten tietojen käsittely	Valmis
Tietosuoja	Valmis
Käyttövaltuushallinta	Valmis
Salasanojen ja tunnistautumismenetelmien hallinta	Valmis
Toimitilaturvallisuus	Valmis
Poikkeamanhallinta ja häiriöiden havaitseminen	Valmis
Tekninen ympäristö	
IT-infrastruktuurin ja järjestelmien hallinta	Valmis
Palvelimet	Valmis
Tietoverkot	Valmis
Päätelaitteet	Valmis
Siirrettävät tietovälineet	Valmis
Järjestelmät, palvelut ja kumppanit	
Sähköposti	Valmis
Pilvipalveluiden käyttö	Valmis
ICT-palveluntarjoajien hallinta	Valmis

Arvioinnin tulokset

Arvioinnin lopputulos	Omat pisteet	Maksimipisteet*	Toteutustaso
	226	276	82%

- Tulokset-välilehdellä näkyy ylimmäisenä *Arvioinnin lopputulos*, jossa kerrotaan koko kyselyn vastausten perusteella ansaitut pisteet, kyselyn maksimipisteet ja näiden perusteella laskettu Toteutustaso (%).
- *Osa-aluekohtaiset tulokset* -kohdassa pisteet, maksimipisteet ja toteutustaso kerrotaan osa-alueittain.
- **Arvioijan tehtävä on täydentää Tulokset-välilehdellä olevia tietoja kirjoittamalla välilehdelle Kehittämissuunnitelma luettelo suositelluista keskeisistä kehityskohteista.**

Yrityksen tavoitetason asettaminen

- Tulokset-välilehdellä yritys voi itse asettaa itselleen tavoitetason, johon haluaisi päästä esim. seuraavaan arviointiin mennessä tai muulla itse määrittämällään ajanjaksolla.
- Mikäli arvioinnin on suorittanut jo aikaisemmin, välilehdelle voi myös tuoda tiedon edellisen kierroksen toteutuksesta ja siten seurata, miten tietoturvan taso on kehittynyt.

Edellisen arvioinnin tulosten lisääminen

Tavoitetason kirjaaminen

Osa-aluekohtaiset tulokset

	Lasketaan automaattisesti vastausten perusteella			*Täytetään itse*	
Hallintakäytännöt	Pisteet	Maksimipisteet*	**Toteutustaso**	**Yrityksen asettama tavoitetaso**	**Mahdollinen edellinen toteutustaso**
Tietoturvan johtaminen ja riskienhallinta	14	22	64%	80%	50%
Henkilöstö ja osaaminen	8	18	44%	85%	44%
Asiakassuhteen hoito ja luottamuksellisten tietojen käsittely	11	24	46%	90%	40%

Taustatietoa: Pisteiden laskenta

- Tulokset-välilehdellä näkyvät pisteet lasketaan seuraavasti:
  - Vastausvaihtoehto: Kyllä = 2 pistettä
  - Vastausvaihtoehto: Osittain = 1 piste
  - Vastausvaihtoehto: Ei / En tiedä = 0 pistettä
  - Vastausvaihtoehto: Ei relevantti = laskennassa huomioidaan, että tämä kysymys ei ole relevantti yrityksen kohdalla (esim. jos kategoriassa on yritykselle 5 relevanttia kysymystä ja yksi ei-relevantti kysymys, maksimipisteet ovat 5*2=10 pistettä)
- Maksimipisteet lasketaan yritykselle relevanteista kysymyksistä. Jokaisesta toteutetusta hallintakeinosta voi saada maksimissaan 2 pistettä, joten maksimipisteet on laskettu kertomalla relevanttien kysymysten lukumäärä kahdella. Lähtökohtaisesti kyselyn maksimipisteet ovat 276 pistettä, mutta jos yritys on merkinnyt osan kysymyksistä ei-relevanteiksi, maksimipisteiden määrä on pienempi.

Tietoturvan arviointimalli on osa Huoltovarmuuskeskuksen ja Taloushallintoliiton yhdessä laatimaa tietoturva- ja tietosuojakokonaisuutta

Tietoturvan arviointimallin on tuottanut Fraktal Oy.

talous hallinto liitto

Huoltovarmuuskeskus