Muistutus: Tallenna tiedosto ennen täyttämistä.

| | |
|---|---|
| Yrityksen nimi | |
| Y-tunnus | |
| Toimiala | |
| Arviointipäivä | |
| Arvioija | |

**Arviointiasteikko (arviointiväittämä 0-4)**

0 Ei arvioitu

1 Ei toteutettu

2 Osittain toteutettu

3 Pääosin toteutettu

4 Täysin toteutettu

**Raportin kypsyystaso (yritys 0-5)**

0 Ei arvioitu

1 Alkuvaihe

2 Kehittyvä

3 Hallittu

4 Edistynyt

5 Optimoitu

Tunniste: ACCESS-1a

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Identiteettien luominen ja hallinta

**Vaatimus**

Työntekijöille ja muille entiteeteille (kuten prosesseille tai laitteille, jotka tarvitsevat pääsyn toimintoon kuuluviin laitteisiin, ohjelmistoihin tai tietovarantoihin) osoitetaan erilliset identiteetit. (Huom. tällä vaatimuksella ei kuitenkaan rajoiteta jaettujen identiteettien käyttöä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-1b

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Identiteettien luominen ja hallinta

**Vaatimus**

Työntekijöille ja muille entiteeteille jaetaan pääsyvaltuustiedot (kuten salasanat, älykortit tai avaimet). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-1c

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Identiteettien luominen ja hallinta

**Vaatimus**

Identiteetit poistetaan käytöstä, kun niitä ei enää tarvita. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-1d

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Identiteettien luominen ja hallinta

**Vaatimus**

Salasanojen vahvuusvaatimukset ja uudelleenkäytön rajoitukset on määritelty ja niiden noudattaminen on pakollista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-1e

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Identiteettien luominen ja hallinta

**Vaatimus**

Identiteettien ajantasaisuudesta huolehditaan tarkastamalla ja päivittämällä ne määrätellyin väliajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten yhteydessä tai yritysrakenteen muuttuessa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-1f

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Identiteettien luominen ja hallinta

**Vaatimus**

Identiteetit poistetaan käytöstä yrityksen määrittelemien enimmäismääräaikojen puitteissa, kun niitä ei enää tarvita.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-1g

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Identiteettien luominen ja hallinta

**Vaatimus**

Hallintatunnusten käyttö on rajoitettu vain niihin prosesseihin, joihin ne on luotu.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-1h

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Identiteettien luominen ja hallinta

**Vaatimus**

Vahvempaa tai monivaiheista tunnistautumista tai kertakäyttötunnuksia vaaditaan käyttö- ja pääsyoikeuksille, joihin liittyy korkeampi riski (tällaisia voivat olla esimerkiksi hallinta- tai ylläpitotunnukset, jaetut tunnukset tai etäyhteyden käyttö).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-1i

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Identiteettien luominen ja hallinta

**Vaatimus**

Monivaiheista tunnistautumista vaaditaan

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-1j

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Identiteettien luominen ja hallinta

**Vaatimus**

Identiteetit, joilla ei ole kirjauduttu määritellyn ajanjakson kuluessa, poistetaan käytöstä mikäli mahdollista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-2a

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Looginen pääsynhallinta

**Vaatimus**

Loogisten käyttöoikeuksien hallinnan valvontakeinoja on käytössä. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-2b

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Looginen pääsynhallinta

**Vaatimus**

Käyttöoikeudet poistetaan, kun niitä ei enää tarvita. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-2c

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Looginen pääsynhallinta

**Vaatimus**

Käyttöoikeuksille on asetettu vaatimuksia, joita myös ylläpidetään (esimerkiksi sääntöjä siitä, millaisille entiteeteille voidaan myöntää pääsy, missä rajoissa pääsy voidaan myöntää, rajoitetaanko etäyhteyksiä tai onko valtuustiedoille kuten salasanoille asetettu erityisiä vaatimuksia).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-2d

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Looginen pääsynhallinta

**Vaatimus**

Käyttöoikeuksien vaatimuksissa on huomioitu pienimmän valtuuden periaate (ref. "principle of least privilege").

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-2e

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Looginen pääsynhallinta

**Vaatimus**

Käyttöoikeuksien vaatimukset sisältävät tehtävien eriyttämisen periaatteet (ref. "separation of duties").

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-2f

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Looginen pääsynhallinta

**Vaatimus**

Käyttöoikeuspyynnöt tarkastaa ja hyväksyy kyseisen laitteen, ohjelmiston tai tietovarannon omistaja.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-2g

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Looginen pääsynhallinta

**Vaatimus**

Käyttöoikeudet, joihin liittyy korkeampi riski toiminnalle, tarkastetaan perusteellisemmin ja niiden käyttöä valvotaan tarkemmin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-2h

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Looginen pääsynhallinta

**Vaatimus**

Käyttöoikeudet tarkastetaan ja päivitetään aika ajoin ja määriteltyjen tilanteiden kuten yritysrakenteen muuttuessa tai tilapäisen käyttöoikeuksien korotuksen jälkeen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-2i

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Looginen pääsynhallinta

**Vaatimus**

Kirjautumis- ja yhteydenmuodostusyrityksiä seurataan ja niissä havaitut poikkeavuudet toimivat kybertapahtumien indikaattoreina.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-3a

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Fyysinen pääsynhallinta

**Vaatimus**

Fyysisen pääsynhallinnan valvontakeinoja on käytössä (kuten aitoja, lukkoja tai kylttejä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-3b

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Fyysinen pääsynhallinta

**Vaatimus**

Pääsyoikeudet poistetaan, kun niitä ei enää tarvita. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-3c

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Fyysinen pääsynhallinta

**Vaatimus**

Pääsyoikeuksien käytöstä pidetään lokia. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-3d

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Fyysinen pääsynhallinta

**Vaatimus**

Pääsyoikeuksille on asetettu vaatimukset, joita myös ylläpidetään (esimerkiksi sääntöjä siitä, kenelle pääsy voidaan myöntää, millä tavoin pääsyoikeudet myönnetään tai missä rajoissa pääsy sallitaan).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-3e

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Fyysinen pääsynhallinta

**Vaatimus**

Pääsyoikeuksien vaatimuksissa on huomioitu pienimmän valtuuden periaate (ref. "principle of least privilege").

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-3f

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Fyysinen pääsynhallinta

**Vaatimus**

Pääsynhallinnan vaatimuksissa on huomioitu tehtävien eriyttämisen periaatteet (ref. "separation of duties").

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-3g

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Fyysinen pääsynhallinta

**Vaatimus**

Pääsyoikeuspyynnöt tarkastaa ja hyväksyy kyseisen tilan, laitteen, ohjelmiston tai tietovarannon omistaja.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-3h

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Fyysinen pääsynhallinta

**Vaatimus**

Pääsyoikeudet, joihin liittyy korkeampi riski, tarkastetaan perusteellisemmin ja niiden käyttöä valvotaan tarkemmin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-3i

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Fyysinen pääsynhallinta

**Vaatimus**

Pääsyoikeudet tarkastetaan ja päivitetään aika ajoin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-3j

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Fyysinen pääsynhallinta

**Vaatimus**

Pääsyoikeuksien käyttöä seurataan ja niistä pyritään tunnistamaan mahdollisia kybertapahtumia.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-4a

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ACCESS-osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-4b

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ACCESS-osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-4c

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ACCESS-osion toimintaa ohjataan vaatimuksilla, jotka on asetettu yrityksen johtotason politiikassa (tai vastaavassa ohjeistuksessa).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-4d

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ACCESS-osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-4e

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ACCESS-osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ACCESS-4f

Osa-alue: Identiteetin- ja pääsynhallinta (ACCESS)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ACCESS-osion toiminnan vaikuttavuutta arvioidaan ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1a

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Yrityksellä on suunnitelma tai strategia kyberarkkitehtuurin kehittämiselle (joka sisältää esimerkiksi kyberarkkitehtuurin tavoitteet, prioriteetit, vastuut ja seurannan). Tasolla 1 sen kehittämisen ja ylläpidon ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1b

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Kyberarkkitehtuurin kehittämiseksi on määritetty suunnitelma tai strategia, jota ylläpidetään. Kyberarkkitehtuurin kehittämissuunnitelma tukee yrityksen kyberturvallisuusstrategiaa [kts. PROGRAM-1b] ja yritysarkkitehtuuria (myös "kokonaisarkkitehtuuri") sekä noudattaa niiden periaatteita ja vaatimuksia.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1c

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Kyberarkkitehtuuri on määritetty, dokumentoitu ja sitä ylläpidetään. Arkkitehtuuri kattaa yrityksen IT/OT järjestelmät ja verkot ja se on linjassa järjestelmien, laitteiden, ohjelmistojen ja tietovarantojen kategorisoinnin ja priorisoinnin kanssa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1d

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Kyberarkkitehtuurille on määritetty hallintamalli (ref. "governance"), jota ylläpidetään (esim. arkkitehtuurin arviointitoimikunta). Hallintamalli kattaa vaatimukset säännöllisistä arkkitehtuurikatselmoinneista sekä päätöksenteon poikkeusprosessille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1e

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Yrityksen johto tukee aktiivisesti ja näkyvästi yrityksen kyberarkkitehtuuria (ja sen kehitystä).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1f

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Kyberarkkitehtuuri määrittää kyberturvallisuusvaatimukset toiminnon kannalta tärkeille laitteille, ohjelmistoille ja tietovarannoille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1g

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Kyberturvallisuuden suojausmekanismit on valittu ja toteutettu siten, että kyberturvallisuusvaatimukset toteutuvat.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1h

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Kyberarkkitehtuurin kehittämissuunnitelma tai strategia ja kyberarkkitehtuurin hallinta ovat linjassa yrityksen yritysarkkitehtuuristrategian (myös "kokonaisarkkitehtuuri") ja yritysarkkitehtuurin hallinnan kanssa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1i

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Yrityksen järjestelmien ja verkkojen vaatimustenmukaisuutta kyberarkkitehtuuriin nähden arvioidaan aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1j

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Kyberturvallisuusarkkitehtuurin kehitystä ohjaavat yrityksen riskiarviointien tulokset [kts. RISK-3d] sekä yrityksen uhkaprofiili [kts. THREAT-2e].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-1k

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Kyberarkkitehtuurin kehittäminen

**Vaatimus**

Kyberarkkitehtuuri käsittelee ennalta määriteltyjä toimintatiloja [kts. SITUATION-3g].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2a

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Verkon suojauksia on toteutettu, ainakin tapauskohtaisesti. Tasolla 1 tämän ei tarvitse olla systemaattista tai säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2b

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Yrityksen IT-järjestelmät on eriytetty mahdollisista OT-järjestelmistä segmentoimalla ne joko fyysisesti tai loogisesti. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä. [Tulkintaohje: mikäli OT-järjestelmiä tai vastaavia ei ole, aseteta käytäntö "täysin toteutetuksi"]

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2c

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Verkkojen suojaus on määritetty ja käytössä valituille laite-, ohjelmisto- ja tietotyypeille riippuen niiden riski- ja prioriteettitasosta (esimerkkeinä sisäiset laitteet, verkkojen reunoilla olevat laitteet, langattomaan verkkoon kytketyt laitteet, pilviomaisuus, etäyhteydet tai ulkoisesti hallitut laitteet).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2d

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Toiminnon kannalta tärkeät laitteet, ohjelmistot ja tietovarannot on segmentoitu loogisesti tai fyysisesti erillisiin turvallisuusvyöhykkeisiin perustuen niille (laitteille, ohjelmistoille ja tietovarannoille) asetettuihin kyberturvallisuusvaatimuksiin [kts. ASSET-1a, ASSET-2a].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2e

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Verkkojen suojauksessa huomioidaan pienimmän valtuuden ja pienimmän toiminnallisuuden periaatteet.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2f

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Verkkojen suojaus sisältää valvonnan, analyysin ja verkkoliikenteen hallinnan (esimerkiksi palomuurit, IDPS)

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2g

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Verkkoliikennettä ja sähköpostia valvotaan, analysoidaan ja hallitaan (esimerkiksi estämällä haitallisia linkkejä tai epäilyttäviä latauksia, sähköpostin autentikointi tai IP-osoitteiden estäminen).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2h

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Kaikki laitteet, ohjelmistot ja tietovarannot on segmentoitu turvallisuusvyöhykkeisiin perustuen niille asetettuihin kybervaatimuksiin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2i

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Verkkojen erottelu on toteutettu turvallisuuslähtöisesti siten että laitteet, ohjelmistot ja tietovarannot on segmentoitu loogisesti tai fyysisesti omiin turva-alueisiinsa, joilla on jokaisella oma todentamisensa/ autentikointi.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2j

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

OT-verkot ovat toiminnallisesti itsenäisiä IT-verkoista siten, että OT ympäristön toimintoja voidaan pitää yllä ja jatkaa myös IT-järjestelmien vikaantuessa. [Tulkintaohje: mikäli OT-verkkoja tai vastaavia ei ole, aseteta käytäntö "täysin toteutetuksi"]

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2k

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Laitteiden yhteyksiä verkkoon hallitaan siten, että vain luvalliset laitteet voivat muodostaa yhteyden (esimerkiksi laitetason pääsynhallinta (NAC)).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-2l

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietoverkkojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Kyberarkkitehtuuri mahdollistaa saastuneiden laitteiden, ohjelmistojen ja tietovarantojen erottamisen muista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3a

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Käyttöoikeuksien ja pääsynhallinan kontrolleja/suojausmekanismeja on käytössä toiminnon kannalta tärkeille laitteille, ohjelmistoille ja tietovarannoille. Tasolla 1 tämä toteutetaan mikäli tehtävissä, mutta sen ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3b

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Päätelaitteiden suojausmekanismeja (esim. turvalliset konfiguraatiot, tietoturvaohjelmistot, päätelaitteiden valvonta) on käytössä toiminnon kannalta tärkeille laitteille, ohjelmistoille ja tietovarannoille. Tasolla 1 tämä toteutetaan mikäli tehtävissä, mutta sen ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3c

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Pienimmän käyttöoikeuden periaate on pantu täytäntöön (esimerkiksi rajoittamalla hallinta- tai ylläpitotunnusten oikeuksia).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3d

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Pienimmän toiminnallisuuden periaate on pantu täytäntöön (esim. rajoittamalla käytettäviä palveluita, ohjelmia, portteja tai liitettäviä laitteita).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3e

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Turvallisia konfiguraatiota on määritelty ja niitä ylläpidetään sekä käytetään osana laitteiden, ohjelmistojen ja tietovarantojen käyttöönottoprosessia, mikäli tehtävissä / toteutettavissa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3f

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Tietoturvaohjelmistot vaaditaan soveltuvin osin osana laitteiden konfiguraatiota (esimerkiksi päätelaitteen turva- ja havainnointiratkaisut tai päätelaitekohtaiset palomuuriratkaisut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3g

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Siirrettäviä ja irrotettavia muistilaitteita valvotaan (esimerkiksi rajoittamalla USB-laitteiden tai ulkoisten levyjen käyttöä).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3h

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Kyberturvallisuuden kontrolleja / suojausmekanismeja (mukaan lukien fyysiset pääsynhallinnan keinot) käytetään kaikkien toimintoon kuuluvien laitteiden, ohjelmistojen ja tietovarantojen kohdalla, joko esimerkiksi laitetasolla tai kompensoivin keinoin, mikäli laitetason kontrolleja ei voida toteuttaa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3i

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Ylläpidon ja kapasiteetinhallinnan toimenpiteitä tehdään kaikille toiminnon laitteille, ohjelmistoille ja tietovarannoille. (omaisuuserät, assets)

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3j

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Toiminnon laitteiden, ohjelmistojen ja tietovarantojen toimintaa suojataan valvomalla / hallitsemalla myös fyysistä toimintaympäristöä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3k

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Korkean prioriteetin laitteille, ohjelmistoille ja tietovarannoille asetetaan tarkempia kyberturvallisuuskontrolleja / hallintakeinoja.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3l

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Laiteohjelmistojen (firmware) konfiguraatioita ja muutoksia hallitaan koko laitteen eliniän ajan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-3m

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Suojausmekanismeja / kontrolleja (esimerkiksi sallitut / estolistat, suojaavat asetukset) on käytössä estämään valtuuttamattoman / luvattoman koodin suorittaminen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-4a

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Sovellusturvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Sisäisesti kehitettävät ohjelmistot ja sovellukset, jotka on tarkoitettu otettavaksi käyttöön korkean prioriteetin laitteissa tai ohjelmistoissa [kts. ASSET-1c], kehitetään noudattaen turvallisen sovelluskehityksen periaatteita.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-4b

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Sovellusturvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Korkean prioriteetin laitteisiin tai ohjelmistoihin [kts. ASSET-1c] tehtävien ohjelmisto- ja sovellushankintojen valinnassa huomioidaan, miten toimittaja noudattaa turvallisen sovelluskehityksen periaatteita.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-4c

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Sovellusturvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Ohjelmistojen ja sovellusten käyttöönottoprosessissa edellytetään turvallisia ohjelmistokonfiguraatioita (sekä sisäisesti kehitettyjen että hankittujen ohjelmistojen osalta)

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-4d

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Sovellusturvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Kaikki sisäisesti kehitettävät ohjelmistot ja sovellukset kehitetään käyttäen turvallisen sovelluskehityksen periaatteita.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-4e

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Sovellusturvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Kaikkien ohjelmisto- ja sovellushankintojen valinnassa huomioidaan noudattaako toimittaja turvallisen sovelluskehityksen periaatteita.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-4f

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Sovellusturvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Arkkitehtuurikatselmointiprosessissa arvioidaan uusien ja päivitettyjen ohjelmistojen ja sovellusten turvallisuutta ennen niiden vientiä tuotantoon.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-4g

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Sovellusturvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Ohjelmistojen ja laiteohjelmistojen (firmware) aitous varmistetaan ennen käyttöönottoa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-4h

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Sovellusturvallisuus osana kyberarkkitehtuuria

**Vaatimus**

Sisäisesti kehitettyjen tai räätälöityjen ohjelmistojen ja sovellusten turvallisuus testataan (esimerkiksi staattinen tai dynaaminen testaus, fuzz-testaus tai penetraatiotestaus) aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-5a

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Tallennettua arkaluontoista tietoa ("data at rest") suojataan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-5b

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Kaikkea tallennettua tietoa ("data at rest") suojataan valittujen tietotyyppien osalta [kts. ASSET-2c].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-5c

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Kaikkea siirrossa olevaa tietoa ("data in transit") suojataan valittujen tietotyyppien / kategorioiden osalta [kts. ASSET-2c].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-5d

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Salausmenetelmät ovat käytössä tallennetulle ja siirrossa olevalle tiedolle valittujen tietotyyppien / kategorioiden osalta [kts. ASSET-2c].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-5e

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Avaintenhallintainfrastruktuuri (eli avainten luonti, säilytys, tuhoaminen, päivittäminen ja kumoaminen) on käytössä salausmenetelmien tukemiseksi.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-5f

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Käytössä on suojausmekanismeja rajoittamaan tiedon varastamisen mahdollisuutta (esimerkiksi tiedon hävittämistä estävät työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-5g

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Kyberarkkitehtuuriin kuuluu suojausmekanismeja (esimerkiksi laitteiden kovalevyjen salaus) tiedolle, joka on tallennettu laitteille, jotka saatetaan hukata tai varastaa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-5h

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Tietojen suojaus osana kyberarkkitehtuuria

**Vaatimus**

Kyberarkkitehtuuri kattaa suojausmenetelmät sovellusten, laiteohjelmistojen (firmware) ja tiedon luvattomien muutosten varalle.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-6a

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ARCHITECTURE-osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-6b

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ARCHITECTURE-osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-6c

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ARCHITECTURE-osion toimintaa ohjataan vaatimuksilla, jotka on asetettu yrityksen johtotason politiikassa (tai vastaavassa ohjeistuksessa).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-6d

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ARCHITECTURE-osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-6e

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ARCHITECTURE-osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ARCHITECTURE-6f

Osa-alue: Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ARCHITECTURE-osion toiminnan vaikuttavuutta arvioidaan ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-1a

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Laitteiden ja ohjelmistojen hallinta

**Vaatimus**

Toiminnon kannalta tärkeistä IT- ja OT-laitteista ja ohjelmistoista on olemassa rekisteri. (Huomioi myös mahdollisten OT-ympäristöjen laitteet ja ohjelmistot). Tasolla 1 rekisterin ylläpidon ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-1b

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Laitteiden ja ohjelmistojen hallinta

**Vaatimus**

Rekisteriin on kirjattu sellaiset toimintoon kuuluvat laitteet ja ohjelmistot, joita voitaisiin käyttää hyökkääjän tavoitteen saavuttamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-1c

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Laitteiden ja ohjelmistojen hallinta

**Vaatimus**

Rekisteriin kirjatut laitteet ja ohjelmistot on priorisoitu noudattaen määriteltyjä priorisointikriteerejä, joihin kuuluu arviointi laitteen tai ohjelmiston tärkeydestä toiminnolle.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-1d

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Laitteiden ja ohjelmistojen hallinta

**Vaatimus**

Priorisointikriteereissä huomioidaan lisäksi missä laajuudessa hyökkääjä voisi käyttää laitetta tai ohjelmistoa [ks. ASSET-1b] tavoitteensa saavuttamiseen (tietomurto, toiminnan häiriö jne.).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-1e

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Laitteiden ja ohjelmistojen hallinta

**Vaatimus**

Rekisteriin on kirjattu laitteista ja ohjelmistoista sellaisia ominaisuuksia, jotka tukevat yrityksen kybertoimintaa (esimerkiksi laitteen tai ohjelmiston sijainti, prioriteetti, käyttöjärjestelmä tai firmware-versio).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-1f

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Laitteiden ja ohjelmistojen hallinta

**Vaatimus**

Rekisteri (IT ja OT) on täydellinen (eli rekisteri kattaa kaikki toiminnon pyörittämiseen tarvittavat laitteet, ohjelmistot ja tietovarannot).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-1g

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Laitteiden ja ohjelmistojen hallinta

**Vaatimus**

Rekisteri on ajan tasalla (eli rekisteriä päivitetään aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten yhteydessä).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-1h

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Laitteiden ja ohjelmistojen hallinta

**Vaatimus**

Kaikki tiedot on tuhottu tai poistettu laitteista ennen käyttöönottoa uudessa kohteessa ja ennen käytöstä poistamista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-2a

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Tietovarantojen hallinta

**Vaatimus**

Toiminnon kannalta tärkeistä tietovarannoista (kuten asiakastiedosta tai laitteiden ja ohjelmistojen perusasetuksista) on olemassa rekisteri. (Huomioi myös mahdollisten OT-ympäristöjen tietovarannot). Tasolla 1 rekisterin ylläpidon ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-2b

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Tietovarantojen hallinta

**Vaatimus**

Rekisteriin on kirjattu sellaiset toimintoon kuuluvat tietovarannot, joita voitaisiin käyttää hyökkääjän tavoitteen saavuttamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-2c

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Tietovarantojen hallinta

**Vaatimus**

Rekisteriin kirjatut tietovarannot on priorisoitu noudattaen määriteltyjä priorisointikriteerejä, joihin kuuluu arviointi tietovarannon tärkeydestä toiminnolle.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-2d

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Tietovarantojen hallinta

**Vaatimus**

Luokittelukriteereissä huomioidaan missä laajuudessa hyökkääjä voisi käyttää tietovarantoa tavoitteensa (tietovuoto, toiminnan keskeytys jne) saavuttamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-2e

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Tietovarantojen hallinta

**Vaatimus**

Rekisteriin on kirjattu tietovarannoista sellaisia ominaisuuksia, jotka tukevat yrityksen kyberturvallisuustoimenpiteitä (esimerkiksi omaisuuden luokitus, varmuuskopioiden sijainti ja päivitysväli, tiedon tallennussijainti, omistajatiedot, tiedon kyberturvallisuusvaatimukset).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-2f

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Tietovarantojen hallinta

**Vaatimus**

Tietovarantojen rekisteri on täydellinen (eli rekisteri kattaa kaikki toiminnon tietovarannot).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-2g

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Tietovarantojen hallinta

**Vaatimus**

Rekisteri on ajan tasalla (eli rekisteriä päivitetään aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten yhteydessä).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-2h

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Tietovarantojen hallinta

**Vaatimus**

Tietovarannot poistetaan, ylikirjoitetaan tai tuhotaan elinkaaren lopussa käyttäen turvallisuusvaatimusten mukaisia menetelmiä. (huomioidaan mm. tiedon suojaustaso)

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-3a

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Konfiguraation hallinta

**Vaatimus**

Laitteiden, ohjelmistojen ja tietovarantojen konfiguraatioista on luotu vakioidut perusasetukset. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-3b

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Konfiguraation hallinta

**Vaatimus**

Vakioituja perusasetuksia käytetään, kun laitteille, ohjelmistoille tai tietovarannoille luodaan uusi konfiguraatio tai palautetaan vanha konfiguraatio.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-3c

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Konfiguraation hallinta

**Vaatimus**

Vakioidut perusasetukset sisältävät soveltuvilta osin yrityksen kyberarkkitehtuurissa määritellyt vaatimukset [kts. ARCHITECTURE-1f].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-3d

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Konfiguraation hallinta

**Vaatimus**

Perusasetuksia katselmoidaan ja päivitetään säännöllisesti ja ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai kyberarkkitehtuurin muutosten yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-3e

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Konfiguraation hallinta

**Vaatimus**

Konfiguraatioiden yhdenmukaisuutta vakioituihin perusasetuksiin seurataan säännöllisesti koko laitteen, ohjelmiston tai tietovarannon elinkaaren ajan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-4a

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Muutoksenhallinta

**Vaatimus**

Laitteisiin, ohjelmistoihin ja tietovarantoihin tehtävät muutokset arvioidaan ja hyväksytetään ennen niiden toteuttamista. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä. (ad hoc, tapauskohtaisesti)

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-4b

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Muutoksenhallinta

**Vaatimus**

Laitteisiin, ohjelmistoihin ja tietovarantoihin tehtävistä muutoksista pidetään lokia. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä. (ad hoc, tapauskohtaisesti)

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-4c

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Muutoksenhallinta

**Vaatimus**

Laitteiden, ohjelmistojen ja tietovarantojen muutoksille on määritelty dokumentointivaatimukset, joita myös ylläpidetään.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-4d

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Muutoksenhallinta

**Vaatimus**

Tärkeisiin (korkean prioriteetin) laitteisiin, ohjelmistoihin ja tietovarantoihin tehtävät muutokset testataan ennen niiden toteuttamista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-4e

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Muutoksenhallinta

**Vaatimus**

Muutokset ja päivitykset toteutetaan turvallisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-4f

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Muutoksenhallinta

**Vaatimus**

Kyvykkyys palautua muutoksia edeltävään tilaan on olemassa ja sitä ylläpidetään niiden laitteiden, ohjelmistojen ja tietovarantojen osalta, jotka ovat tärkeitä toiminnolle.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-4g

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Muutoksenhallinta

**Vaatimus**

Muutoksenhallinnan käytännöt kattavat laitteiden, ohjelmistojen ja tiedon koko elinkaaren (esimerkiksi hankinnan, käyttöönoton, käytön ja käytöstä poiston).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-4h

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Muutoksenhallinta

**Vaatimus**

Tärkeisiin (korkean prioriteetin) laitteisiin, ohjelmistoihin ja tietovarantoihin tehtävien muutosten kyberturvallisuusvaikutus testataan ennen niiden toteuttamista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-4i

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Muutoksenhallinta

**Vaatimus**

Muutoksenhallinnan lokit sisältävät tietoa sellaisista tehdyistä muutoksista, jotka vaikuttavat kyseisen laitteen, ohjelmiston tai tietovarannon kyberturvallisuusvaatimuksiin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-5a

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ASSET-osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-5b

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ASSET-osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-5c

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ASSET-osion toimintaa ohjataan vaatimuksilla, jotka on asetettu yrityksen johtotason politiikassa (tai vastaavassa ohjeistuksessa).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-5d

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ASSET-osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-5e

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ASSET-osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: ASSET-5f

Osa-alue: Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

ASSET-osion toiminnan vaikuttavuutta arvioidaan ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-1a

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

**Vaatimus**

Yrityksen tuottamat yhteiskunnalle kriittiset palvelut on tunnistettu ja dokumentoitu.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-1b

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

**Vaatimus**

(Yhteiskunnalle kriittisten) palveluiden tuottamiseen tarvittava data on tunnistettu ja dokumentoitu.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-1c

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

**Vaatimus**

Palveluiden tuottamiseen tarvittavat prosessit on tunnistettu ja dokumentoitu.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-1d

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

**Vaatimus**

Palveluiden tuottamiseen tarvittavat järjestelmät (IT- ja OT-omaisuus) on tunnistettu ja dokumentoitu.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-1e

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

**Vaatimus**

Palveluiden tuottamiseen tarvittavat tilat ja laitteet on tunnistettu ja dokumentoitu.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-1f

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

**Vaatimus**

Palveluiden tuottamiseen tarvittavat toimitusketjut on tunnistettu ja dokumentoitu.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-1g

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

**Vaatimus**

Yrityksen on määrittänyt sen kriittisen ajanjakson, jonka jälkeen yhteiskunnan normaaliin toimintaan koituu huomattavaa vaikusta, mikäli kriittisten palveluiden tarvitsemat edellä luetellut resurssit (data, prosessit, järjestelmät, tilat tai toimitusketjut) eivät ole käytettävissä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-1h

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen

**Vaatimus**

Palvelujen heikentymisen tai keskeytymisen aiheuttamat seurannaisvaikutukset yhteiskunnalle on tunnistettu ja dokumentoitu.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2a

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Kaikki resurssit (data, prosessit, järjestelmät, tilat ja toimitusketjut), joita tarvitaan (yhteiskunnalle kriittisten) palveluiden tuottamiseen, ovat yrityksen turvallisuuden hallinnan politiikkojen ja prosessien piirissä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2b

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Kaikki resurssit (data, prosessit, järjestelmät, tilat ja toimitusketjut), joita tarvitaan yhteiskunnallisesti kriittisten palvelujen tuottamiseen, ovat yrityksen riskienhallinnan politiikkojen ja prosessien piirissä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2c

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Johtoryhmä vastaa yrityksen lähestymistavasta ja johtotason politiikasta liittyen palveluiden tuottamiseen tarvittavien tietoverkkojen ja -järjestelmien turvallisuuteen. Yrityksen riskienhallinnan päätöksentekijät pidetään tästä lähestymistavasta ja politiikoista ajan tasalla sopivin menettelyin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2d

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Johtoryhmä käsittelee palveluiden tuottamiseen tarvittavien tietoverkkojen ja -järjestelmien turvallisuuden tasoa säännöllisesti; käyttäen pohjana ajantasaista ja tarkkaa tietoa sekä yrityksen ammattilaisten asiantuntemusta.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2e

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Johtoryhmän nimetyllä jäsenellä on vastuu palveluiden tuottamiseen tarvittavien tietoverkkojen ja -järjestelmien turvallisuuden tasosta. Henkilö ohjaa johtoryhmän säännöllistä keskustelua aiheesta.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2f

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Johtoryhmä asettaa suunnan ja tahtotilan, joista johdetaan tehokkaita toimintatapoja tietoverkkojen ja -järjestelmien turvallisuuden valvontaan ja ohjaukseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2g

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Yrityksen ylimmällä johdolla on näkyvyys tärkeimpiin riskipäätöksiin läpi koko yrityksen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2h

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Yrityksen riskienhallinnan päätöksentekijöillä on vastuu tehdä tehokkaita, oikea-aikaisia ja yrityksen johdon määrittämän riskinottohalukkuuden mukaisia päätöksiä palveluiden tuottamiseen tarvittaviin tietoverkkoihin ja -järjestelmiin liittyen. Henkilöt tunnistavat ja tiedostavat päätöksentekovastuunsa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2i

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Riskienhallinnan päätöksentekoa voidaan tarvittaessa delegoida tai korottaa ("escalate") läpi koko yrityksen sellaisille henkilöille, joilla on sopivat tiedot, taidot ja valtuudet päätösten tekemiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2j

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Tehdyt riskienhallintapäätökset käydään läpi aika ajoin, jotta varmistutaan siitä, että ne ovat pysyneet relevantteina ja pätevinä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-2k

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden hallinta

**Vaatimus**

Riskienhallintaprosessissa ja -päätöksenteossa otetaan huomioon resurssit (data, prosessit, järjestelmät, laitteet ja toimitusketju), kriittinen ajanjakso ja seurannaisvaikutukset [kts. CRITICAL-1b-h].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-3a

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden kyberpoikkeamien vaikutusten minimointi

**Vaatimus**

Yrityksellä on kybertapahtumien ja -poikkeamien hallintasuunnitelma, joka kattaa kaikki (yrityksen tuottamat yhteiskunnalle kriittiset) palvelut.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-3b

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden kyberpoikkeamien vaikutusten minimointi

**Vaatimus**

Hallintasuunnitelma rajoittuu tunnettuihin hyökkäyksiin, mutta kattaa perusteellisesti näiden hyökkäysten todennäköiset vaikutukset.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-3c

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden kyberpoikkeamien vaikutusten minimointi

**Vaatimus**

Kybertapahtumien ja -poikkeamien hallintaan osallistuva henkilöstö on sisäistänyt ja ymmärtää hallintasuunnitelman hyvin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-3d

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden kyberpoikkeamien vaikutusten minimointi

**Vaatimus**

Hallintasuunnitelma on dokumentoitu ja se jaetaan kaikille relevanteille sidosryhmille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-3e

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden kyberpoikkeamien vaikutusten minimointi

**Vaatimus**

Hallintasuunnitelma perustuu (yhteiskunnalle kriittisten palveluiden tuottamiseen tarvittavien) tietoverkkojen ja -järjestelmien riskien perusteelliseen tunnistamiseen ja ymmärtämiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-3f

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden kyberpoikkeamien vaikutusten minimointi

**Vaatimus**

Hallintasuunnitelma kattaa perusteellisesti sekä tunnettujen hyökkäysten, että toistaiseksi tuntemattomien hyökkäysten todennäköiset vaikutukset. Suunnitelma kattaa perusteellisesti poikkeaman koko elinkaaren, roolit ja vastuut sekä raportointivelvoitteet.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-3g

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden kyberpoikkeamien vaikutusten minimointi

**Vaatimus**

Hallintasuunnitelma on dokumentoitu ja integroitu osaksi yrityksen laajempaa liiketoiminnan ja toimitusketjujen jatkuvuudenhallintaa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: CRITICAL-3h

Osa-alue: Kriittisten palveluiden suojaaminen (CRITICAL)

Alakohta: Kriittisten palveluiden kyberpoikkeamien vaikutusten minimointi

**Vaatimus**

Kaikki yhteiskunnalle kriittisten palveluiden tuottamiseen osallistuvat yrityksen liiketoimintayksiköt ovat saaneet ja sisäistäneet hallintasuunnitelman.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-1a

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Kyberturvallisuusstrategia

**Vaatimus**

Yrityksellä on kyberturvallisuusstrategia. Tasolla 1 sen kehittämisen ja ylläpidon ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-1b

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Kyberturvallisuusstrategia

**Vaatimus**

Kyberturvallisuusstrategia määrittelee yrityksen kyberturvallisuustavoitteet.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-1c

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Kyberturvallisuusstrategia

**Vaatimus**

Kyberturvallisuusstrategia ja -prioriteetit on dokumentoitu. Strategia ja prioriteetit ovat linjassa yrityksen yleisten strategisten tavoitteiden ja kriittiseen infrastruktuuriin kohdistuvien riskien kanssa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-1d

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Kyberturvallisuusstrategia

**Vaatimus**

Kyberturvallisuusstrategia määrittää yrityksen kyberturvallisuuden hallintamallin ("governance") ja valvontatoimet.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-1e

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Kyberturvallisuusstrategia

**Vaatimus**

Kyberturvallisuusstrategia määrittelee kyberturvallisuuden hallinta- ja yritysrakenteen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-1f

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Kyberturvallisuusstrategia

**Vaatimus**

Kyberturvallisuusstrategia nimeää ne standardit ja ohjeet, joita tulee noudattaa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-1g

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Kyberturvallisuusstrategia

**Vaatimus**

Kyberturvallisuusstrategia nimeää / tunnistaa kaikki soveltuvat vaatimustenmukaisuusvaatimukset, jotka ohjelman pitää noudattaa. (esimerkiksi NIST CSF, ISO, PCI DSS) (toimeenpano-ohjelma vai strategia)

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-1h

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Kyberturvallisuusstrategia

**Vaatimus**

Kyberturvallisuusstrategia on päivitetty säännöllisesti ja määriteltyjen ehtojen täyttyessä kuten muutokset yrityksen liiketoiminnassa, toimintaympäristössä tai uhkaprofiilissa [kts. THREAT-2e].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-2a

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Johdon tuki kyberturvallisuusohjelmalle

**Vaatimus**

Yrityksen ylin johto tukee kyberturvallisuuden hallintaa. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-2b

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Johdon tuki kyberturvallisuusohjelmalle

**Vaatimus**

Kyberturvallisuuden hallinta perustuu kyberturvallisuusstrategiaan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-2c

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Johdon tuki kyberturvallisuusohjelmalle

**Vaatimus**

Yrityksen ylimmän johdon tuki kyberturvallisuuden hallinnalle on näkyvää ja aktiivista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-2d

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Johdon tuki kyberturvallisuusohjelmalle

**Vaatimus**

Yrityksen ylin johto tukee kyberturvallisuuspolitiikkojen ja -ohjeiden kehittämistä, ylläpitoa ja täytäntöönpanoa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-2e

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Johdon tuki kyberturvallisuusohjelmalle

**Vaatimus**

Vastuu kyberturvallisuuden hallinnasta on osoitettu yrityksessä taholle, jolla on riittävät toimivaltuudet.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-2f

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Johdon tuki kyberturvallisuusohjelmalle

**Vaatimus**

Kyberturvallisuuden hallinnan sidosryhmät on tunnistettu ja osallistettu.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-2g

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Johdon tuki kyberturvallisuusohjelmalle

**Vaatimus**

Kyberturvallisuuden hallinnan toiminta tarkastetaan aika ajoin, jotta varmistetaan että toimet ovat linjassa kyberturvallisuusstrategian kanssa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-2h

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Johdon tuki kyberturvallisuusohjelmalle

**Vaatimus**

Riippumaton taho tarkastaa yrityksen kyberturvallisuuteen liittyvät toiminnat aika ajoin ja määriteltyjen tilanteiden kuten prosessimuutosten yhteydessä, jotta varmistutaan että toiminta on kyberturvallisuuspolitiikkojen ja -ohjeiden mukaista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-2i

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Johdon tuki kyberturvallisuusohjelmalle

**Vaatimus**

Kyberturvallisuuden kehittämisohjelma huomioi yritystä velvoittavien lakien, sääntöjen ja määräysten noudattamisen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-2j

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Johdon tuki kyberturvallisuusohjelmalle

**Vaatimus**

Yritys tekee yhteistyötä ulkoisten toimijoiden kanssa edistääkseen kyberturvallisuusstandardien, suositusten, johtavien käytäntöjen, tapauksista käytävän tiedonvaihdon sekä kehittyvien teknologioiden kehitystä ja käyttöönottoa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-3a

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

PROGRAM-osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-3b

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

PROGRAM-osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-3c

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

PROGRAM-osion toimintaa ohjataan vaatimuksilla, jotka on asetettu yrityksen johtotason politiikassa (tai vastaavassa ohjeistuksessa).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-3d

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

PROGRAM-osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-3e

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

PROGRAM-osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: PROGRAM-3f

Osa-alue: Kyberturvallisuuden hallinta (PROGRAM)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

PROGRAM-osion toiminnan vaikuttavuutta arvioidaan ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-1a

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien havainnointi

**Vaatimus**

Havaitut kybertapahtumat raportoidaan ennalta määritellyille henkilöille tai roolien haltijoille ja ne documentoidaan (ainakin tapauskohtaisesti). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-1b

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien havainnointi

**Vaatimus**

Kybertapahtumista ja niiden havaitsemisesta on laadittu kriteeristö (johon kuuluu esimerkiksi määritelmä tilanteista, jotka täyttävät kybertapahtuman määritelmän tai määritelmä siitä, missä kybertapahtumia voidaan havaita).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-1c

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien havainnointi

**Vaatimus**

Kybertapahtumat dokumentoidaan määritellyn kriteeristön mukaisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-1d

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien havainnointi

**Vaatimus**

Tapahtumien tietoja verrataan keskenään, jotta niistä tunnistettaisiin mahdollisia säännönmukaisuuksia, trendejä tai muita yhteisiä piirteitä, joilla voitaisiin tukea kyberpoikkeamien analysointityötä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-1e

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien havainnointi

**Vaatimus**

Kybertapahtumien havainnointitoimia mukautetaan perustuen tunnistettuihin riskeihin ja yrityksen uhkaprofiiliin [kts. THREAT-2e].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-1f

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien havainnointi

**Vaatimus**

Toiminnon tilannekuvaa seurataan siten, että se tukee mahdollisten kybertapahtumien havaitsemista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-2a

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien analysointi ja poikkeamatilanteiden määrittäminen

**Vaatimus**

Kyberpoikkeamien määrittämisestä on laadittu kriteeristö. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-2b

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien analysointi ja poikkeamatilanteiden määrittäminen

**Vaatimus**

Kybertapahtumat analysoidaan siten, että se tukee mahdollisten kyberpoikkeamien määrittämistä. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-2c

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien analysointi ja poikkeamatilanteiden määrittäminen

**Vaatimus**

Kyberpoikkeamien määrittämisestä on laadittu virallinen kriteeristö, joka perustuu siihen, miten poikkeamat voivat vaikuttaa toimintoon.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-2d

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien analysointi ja poikkeamatilanteiden määrittäminen

**Vaatimus**

Kybertapahtumat määritetään kyberpoikkeamiksi laaditun kriteeristön mukaisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-2e

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien analysointi ja poikkeamatilanteiden määrittäminen

**Vaatimus**

Kyberpoikkeamien määrittämisen kriteeristö päivitetään aika ajoin ja määriteltyjen tilanteiden kuten yritysmuutosten, harjoitustoiminnasta saatujen kokemusten tai uusien havaittujen uhkien perusteella.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-2f

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien analysointi ja poikkeamatilanteiden määrittäminen

**Vaatimus**

Kybertapahtumista ja -poikkeamista pidetään rekisteriä / kantaa, johon tapahtumat ja poikkeamat kirjataan ja jossa niitä seurataan päättymiseen asti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-2g

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien analysointi ja poikkeamatilanteiden määrittäminen

**Vaatimus**

Sisäiset ja ulkoiset sidosryhmät (esimerkiksi johtajat, lakimiehet, viranomaiset, kumppanit, palveluntoimittajat, toimialan muut yrityst, ISAC-ryhmät tai yrityksen muut sisäiset ja ulkoiset sidosryhmät) on tunnistettu ja näitä informoidaan kyberturvallisuustapahtumista ja -poikkeamista tilannekuva-osiossa määritettyjen raportointivaatimusten mukaisesti [kts. SITUATION-3d].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-2h

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien analysointi ja poikkeamatilanteiden määrittäminen

**Vaatimus**

Kyberpoikkeamien määrittämisen kriteeristö on linjassa kyberriskien priorisoinnin kriteereiden kanssa [kts. RISK-3b].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-2i

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumien analysointi ja poikkeamatilanteiden määrittäminen

**Vaatimus**

Kyberpoikkeamien tietoja verrataan keskenään, jotta niistä tunnistettaisiin mahdollisia säännönmukaisuuksia, trendejä tai muita poikkeamille yhteisiä piirteitä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3a

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamiin reagoimista varten on tunnistettu soveltuvat työntekijät ja heille on annettu roolit (ainakin tapauskohtaisesti). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3b

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamiin reagoidaan siten, että toiminnalla (voidaan toteuttaa tapauskohtaisesti) rajoitetaan toimintoon kohdistuvaa vaikutusta ja palautetaan toiminta normaaliksi. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3c

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamista tuotetaan raportointia (esimerkiksi sisäisesti, CERT-FI tai soveltuville ISAC-ryhmille). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3d

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamiin reagoimisen varalle on luotu suunnitelma, jota pidetään yllä ja joka kattaa koko poikkeamanhallinnan elinkaaren.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3e

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamiin reagoidaan määriteltyjen suunnitelmien ja menettelytapojen mukaisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3f

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamien hallintasuunnitelma sisältää viestintäsuunnitelman, joka kattaa sekä sisäiset että ulkoiset sidosryhmät

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3g

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamiin reagoinnin suunnitelmia harjoitellaan määräajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3h

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamista saadut kokemukset käsitellään ja toimista otetaan opiksi (lessons learned). Korjaavia toimenpiteitä toteutetaan, mukaan lukien toimintasuunnitelmien päivittäminen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3i

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamien juurisyyt analysoidaan ja korjaavia toimenpiteitä toteutetaan, mukaan lukien toimintasuunnitelmien päivittäminen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3j

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamiin reagointi koordinoidaan soveltuvin osin toimittajien, viranomaisten ja muiden ulkopuolisten tahojen kanssa. Tähän kuuluu tukitoimet todistusaineiston keräämiselle ja säilyttämiselle.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3k

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamien käsittelyyn ja reagointiin osallistuvat työntekijät ottavat osaa yhteisiin harjoituksiin muiden yritysten kanssa (esim. työpöytäharjoitukset, simulaatiot).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-3l

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Tapahtumiin ja poikkeamiin reagoiminen

**Vaatimus**

Kyberpoikkeamiin reagoinnissa noudatetaan ennalta määriteltyjä toimintatiloja [kts. SITUATION-3g].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4a

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Yritys on kehittänyt toiminnan jatkuvuutta koskevat suunnitelmat, joiden avulla toiminnon toiminta voidaan säilyttää ja palauttaa, mikäli toimintaan kohdistuu kybertapahtuma tai -poikkeama. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4b

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Tiedoista on saatavilla varmuuskopiot, joita testaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4c

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Varaosia tarvitsevat IT-laitteet (ja mahdolliset OT-laitteet) on tunnistettu. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4d

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Jatkuvuussuunnitelmat sisältävät arviot mahdollisten kyberpoikkeamien vaikutuksista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4e

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Jatkuvuussuunnitelmissa on tunnistettu ja dokumentoitu ne laitteet, ohjelmistot ja tietovarannot sekä toiminnat, jotka minimissään tarvitaan toiminnon toiminnan ylläpitämiseksi.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4f

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Jatkuvuussuunnitelmat käsittelevät toiminnon kannalta tärkeät IT- ja OT-laitteet, ohjelmistot ja tietovarannot. Mukaan lukien varmuuskopioiden saatavuuden sekä korvaavat, varmennetut ja varalla olevat (IT ja OT) laitteet ja ohjelmistot. (Huomioi myös mahdolliset OT-laitteet, -ohjelmistot ja tietovarannot).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4g

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Jatkuvuussuunnitelmiin kuuluu toipumisajan ("RTO, Recovery Time Objective") ja toipumispisteen ("Recovery Point Objective, RPO") määrittely toiminnon kannalta tärkeille laitteille, ohjelmistoille ja tietovarannoille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4h

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Jatkuvuussuunnitelman käyttöönottamisen kriteerit kyberpoikkeamatilanteissa on määritetty ja viestitty poikkeamien käsittelystä ja valmiussuunnitelmista vastuussa oleville työntekijöille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4i

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Jatkuvuussuunnitelmat testataan arvioimalla ja/tai harjoittelemalla aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4j

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Varmuuskopiota suojaavat kyberturvallisuus kontrollit / hallintakeinot ovat yhtä hyvät tai perusteellisemmat kuin kontrollit, jotka suojaavat varmuuskopioitavaa tietoa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4k

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Varmuuskopiot on erotettu sekä loogisesti että fyysisesti varmuuskopioidusta tiedosta.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4l

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Varaosia on saatavilla niitä tarvitseviin IT-laitteisiin (ja mahdollisiin OT-laitteisiin).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4m

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Jatkuvuussuunnitelmissa on huomioitu tunnistetut riskit ja yrityksen uhkaprofiili [kts. THREAT-2e], jotta katetaan tunnistetut riskikategoriat ja uhat.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4n

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Jatkuvuusharjoituksiin sisältyy korkean prioriteetin riskeihin varautuminen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4o

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Jatkuvuussuunnitelmien testauksesta tai tositilanteista saatuja havaintoja verrataan asetettuihin toipumistavoitteisiin ja suunnitelmia kehitetään näiden havaintojen perusteella.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-4p

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Kyberturvallisuus osana toiminnan jatkuvuutta

**Vaatimus**

Jatkuvuussuunnitelmien sisältö tarkastetaan ja päivitetään määräajoin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-5a

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RESPONSE-osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-5b

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RESPONSE-osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-5c

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RESPONSE-osion toimintaa ohjataan vaatimuksilla, jotka on asetettu yrityksen johtotason politiikassa (tai vastaavassa ohjeistuksessa).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-5d

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RESPONSE-osion toimintaa suorittaville työntekijöille on määritelty vastuut, velvoitteet ja valtuutukset tehtäviensä suorittamista varten.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-5e

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RESPONSE-osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RESPONSE-5f

Osa-alue: Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RESPONSE-osion toiminnan vaikuttavuutta arvioidaan ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-1a

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskienhallinnan suunnitelma

**Vaatimus**

Yrityksen kyberriskienhallintaa ohjaa suunnitelma (esimerkiksi strategia tai vastaava johtotason politiikka). Tasolla 1 sen kehittämisen ja ylläpidon ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-1b

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskienhallinnan suunnitelma

**Vaatimus**

Yrityksen kyberriskienhallintaa ohjaa järjestelmällinen toimintasuunnitelma, jota ylläpidetään säännöllisesti ja joka tukee yrityksen laajempaa kyberturvallisuuden kehittämisen suunnitelmaa [kts. PROGRAM-1b) ja yrityksen yritysarkkitehtuuria (myös "kokonaisarkkitehtuuri").

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-1c

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskienhallinnan suunnitelma

**Vaatimus**

Kyberriskienhallintaohjelma on määritelty ja sitä ylläpidetään. Se määrittää kyberriskienhallintatoimet, jotka perustuvat yrityksen kyberriskienhallintastrategiaan / toimintasuunnitelmaan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-1d

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskienhallinnan suunnitelma

**Vaatimus**

Kyberriskienhallinnan toimenpiteistä jaetaan tietoa soveltuville sidosryhmille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-1e

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskienhallinnan suunnitelma

**Vaatimus**

Kyberriskienhallintaa varten on määritetty hallintamalli (ref. "governance"), jota ylläpidetään säännöllisesti. Hallintamalliin kuuluvat mm. riskienhallinnan vastuut, velvollisuudet ja päätöksentekorakenteet.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-1f

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskienhallinnan suunnitelma

**Vaatimus**

Yrityksen johto tukee aktiivisesti ja näkyvästi yrityksen kyberriskienhallintaohjelmaa .

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-1g

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskienhallinnan suunnitelma

**Vaatimus**

Yrityksen kyberriskienhallinnan ohjelma on linjassa yrityksen toiminta-ajatuksen (missio) ja tavoitteiden kanssa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-1h

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskienhallinnan suunnitelma

**Vaatimus**

Kyberriskienhallintaohjelma on yhteensovitettu koko yrityksen laajuisen riskienhallintaohjelman kanssa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2a

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Kyberriskejä tunnistetaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2b

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Kyberriskien tunnistamiseen käytetään määriteltyjä menetelmiä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2c

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Kyberriskien tunnistamiseen osallistuu soveltuvilta osin sidosryhmiä operatiivisista ja liiketoimintayksiköistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2d

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Tunnistetut kyberriskit jaetaan erillisiin kategorioihin, jotta riskejä voidaan hallita kategoriakohtaisesti (kategorioita voivat olla esimerkiksi tietovuodot, sisäiset virheet, ransomware tai OT-laitteiden kaappaus).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2e

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Kyberriskit ja kyberriskikategoriat dokumentoidaan riskirekisteriin (tai vastaavaan tietovarastoon).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2f

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Kyberriskeille ja kyberriskikategorioille on nimitetty omistajat.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2g

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Kyberriskien tunnistamista tehdään aika ajoin ja määriteltyjen tilanteiden, kuten järjestelmämuutosten tai ulkoisten kybertapahtumien yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2h

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Kyberriskien tunnistamistoimissa hyödynnetään ASSET-osion laitteiden, ohjelmistojen ja tietovarantojen rekisterejä sekä priorisointitietoja. Esimerkkinä IT- ja OT-laitteiden elinkaaritiedot, kriittiset laitteet sekä tietovarantojen vuotamiseen, muuttamiseen tai tuhoutumiseen liittyvät riskit.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2i

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Uhkien hallinnan -osion [kts. THREAT] toimilla tuotettua haavoittuvuustietoa käytetään uusien kyberriskien tunnistamiseen ja olemassa olevien kyberriskien päivittämiseen (esimerkiksi tunnistamaan haavoittuvuuksista aiheutuvia riskejä, jotka voivat olla jatkuvia tai aiheutua uudesta, vastatunnistetusta haavoittuvuudesta)

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2j

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Uhkatietoa uhkien hallinnan osiosta [kts. THREAT] käytetään uusien kyberriskien tunnistamiseen ja olemassa olevien kyberriskien päivittämiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2k

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Kumppaniverkoston riskienhallinnan osion toimenpiteistä [kts. THIRD-PARTIES] saatua tietoa käytetään uusien kyberriskien tunnistamiseen ja olemassa olevien kyberriskien päivittämiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2l

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Kyberarkkitehtuuri-osion [kts. ARCHITECTURE] toimilla tuotettua tietoa (kuten käsittelemättömät poikkeamat yrityksen tavoitelemassa kyberarkkitehtuurissa) käytetään uusien kyberriskien tunnistamiseen ja olemassa olevien kyberriskien päivittämiseen

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-2m

Osa-alue: Riskienhallinta (RISK)

Alakohta: Kyberriskien tunnistaminen

**Vaatimus**

Kyberriskien tunnistamisessa huomioidaan riskit, jotka aiheutuvat kriittisestä infrastruktuurista tai keskinäisriippuvaisista yritysista tai kohdistuvat niihin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-3a

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskien analysointi

**Vaatimus**

Kyberriskit priorisoidaan niiden arvioidun vaikutuksen perusteella. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-3b

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskien analysointi

**Vaatimus**

Määriteltyjä kriteerejä käytetään kyberriskien priorisoinnissa (esimerkiksi vaikutus yritykseen, yhteiskunnallinen vaikutus, todennäköisyys, alttius, riskinsietokyky).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-3c

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskien analysointi

**Vaatimus**

Korkean prioriteetin kyberriskien vaikutusta (impact) arvioidaan noudattaen määriteltyjä menetelmiä (esimerkiksi vertaamalla toteutuneisiin tapauksiin tai kvantifioimalla riski).G228

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-3d

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskien analysointi

**Vaatimus**

Korkeamman prioriteetin kyberriskit analysoidaan noudattaen määriteltyjä menetelmiä (esimerkiksi analysoimalla toteutuneiden tapausten yleisyyttä riskin todennäköisyyden arvioimiseksi tai hyödyntämällä suojausmekanismien arvioinneista saatuja tuloksia kohteen riskialttiuden määrittelyyn).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-3e

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskien analysointi

**Vaatimus**

Yrityksen sidosryhmät soveltuvista operatiivisen toiminnan ja liiketoiminnan yksiköistä osallistuvat korkeamman prioriteetin kyberriskien analysointiin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-3f

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskien analysointi

**Vaatimus**

Kun kyberriskit eivät enää vaadi seurantaa tai toimenpiteitä, ne poistetaan riskirekisteristä tai muusta tallennuspaikasta, jota on käytetty riskin dokumentointiin ja hallintaan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-3g

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskien analysointi

**Vaatimus**

Kyberriskianalyysit päivitetään määräajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-4a

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskeihin reagointi

**Vaatimus**

Riskeihin reagointikeinot (kuten riskin pienentäminen, hyväksyminen, välttäminen tai siirtäminen) ovat käytössä kyberriskeille. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-4b

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskeihin reagointi

**Vaatimus**

Riskeihin reagoimisen keinot valitaan ja toteutetaan noudattaen määriteltyjä menetelmiä, jotka pohjautuvat analysointiin ja priorisointiin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-4c

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskeihin reagointi

**Vaatimus**

Kyberturvallisuuden suojausmekanismien suunnittelun onnistumista ja niiden tosiasiallista vaikutusta kyberriskien pienenemiseen arvioidaan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-4d

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskeihin reagointi

**Vaatimus**

Yritysjohto tarkastaa sekä kyberriskien vaikutusarviointien että kyberturvallisuuden suojausmekanismien arviointien tulokset varmistuakseen riskienhallinnan riittävyydestä ja siitä, että riskit ovat yrityksen riskinottohalukkuuden mukaisia.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-4e

Osa-alue: Riskienhallinta (RISK)

Alakohta: Riskeihin reagointi

**Vaatimus**

Yritysjohto tarkastaa riskeihin reagoimisen keinot (kuten riskin pienentäminen, hyväksyminen, välttäminen tai siirtäminen) aika ajoin varmistuakseen niiden soveltuvuudesta.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-5a

Osa-alue: Riskienhallinta (RISK)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RISK-osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-5b

Osa-alue: Riskienhallinta (RISK)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RISK-osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-5c

Osa-alue: Riskienhallinta (RISK)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RISK-osion toimintaa ohjataan vaatimuksilla, jotka on asetettu yrityksen johtotason politiikassa (tai vastaavassa ohjeistuksessa).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-5d

Osa-alue: Riskienhallinta (RISK)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RISK-osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-5e

Osa-alue: Riskienhallinta (RISK)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RISK-osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: RISK-5f

Osa-alue: Riskienhallinta (RISK)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

RISK-osion toiminnan vaikuttavuutta arvioidaan ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-1a

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Lokienhallinta

**Vaatimus**

Lokitietoa kerätään toiminnon kannalta tärkeistä laitteista, ohjelmistoista ja tietovarannoista (ainakin tapauskohtaisesti). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-1b

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Lokienhallinta

**Vaatimus**

Lokitietoa kerätään sellaisista laitteista, ohjelmistoista ja tietovarannoista, joita voitaisiin käyttää hyökkääjän tavoitteen saavuttamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-1c

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Lokienhallinta

**Vaatimus**

IT- ja OT-laitteille, ohjelmistoille ja tietovarannoille, jotka ovat tärkeitä toiminnon kannalta tai joita hyökkääjä voisi hyödyntää tavoitteensa saavuttamiseen, on määritetty ja ylläpidetty lokitusvaatimuksia.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-1d

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Lokienhallinta

**Vaatimus**

Verkko- ja päätelaitteiden valvontainfrastruktuurille on määritetty lokitusvaatimukset, joita myös ylläpidetään. (esimerkiksi internetyhdyskäytäville (gateway), EDR ohjelmistot, IDPS tunkeutumisen havaitsemis- ja estojärjestelmät)

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-1e

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Lokienhallinta

**Vaatimus**

Lokitieto koostetaan yhteen keskitetysti toiminnon sisällä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-1f

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Lokienhallinta

**Vaatimus**

Korkean prioriteetin laitteista, ohjelmistoista ja tietovarannoista kerätään tarkempaa lokitietoa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-2a

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Ympäristöjen valvonta

**Vaatimus**

Lokitietojen tarkastelua ja muuta kyberturvallisuusvalvontaa tehdään. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-2b

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Ympäristöjen valvonta

**Vaatimus**

IT- ja OT-ympäristöjen valvontatietoja katselmoidaan säännöllisesti poikkeavan toiminnan ja mahdollisten kybertapahtumien varalta (ainakin tapauskohtaisesti). Tasolla 1 tämän ei tarvitse olla systemaattista.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-2c

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Ympäristöjen valvonta

**Vaatimus**

Valvonnalle ja havaintojen analysoinnille on määritetty tarkempia vaatimuksia, joita päivitetään säännöllisesti ja jotka kattavat tapahtumatietojen oikea-aikaisen tarkastelun.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-2d

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Ympäristöjen valvonta

**Vaatimus**

Poikkeavan toiminnan havaitsemiseksi on määritetty indikaattoreita, jotka pohjautuvat järjestelmälokeihin, tietovuoanalyysiin, verkkojen peruskonfiguraatioihin, kybertapahtumiin ja -arkkitehtuuriin. IT-ympäristöjä (ja mahdollisia OT-ympäristöjä) valvotaan näiden indikaattoreiden avulla.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-2e

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Ympäristöjen valvonta

**Vaatimus**

Kybertapahtumien tunnistamista varten on määritetty erilaisia hälytyksiä ja ilmoituksia, joita päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-2f

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Ympäristöjen valvonta

**Vaatimus**

Valvontatoimenpiteet ovat linjassa toiminnon uhkaprofiilin kanssa [kts. THREAT-2e].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-2g

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Ympäristöjen valvonta

**Vaatimus**

Korkean prioriteetin laitteita, ohjelmistoja ja tietovarantoja valvotaan tarkemmin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-2h

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Ympäristöjen valvonta

**Vaatimus**

Riskianalyyseistä saatua tietoa [kts. RISK-3d] hyödynnetään, kun määritetään poikkeavan toiminnan indikaattoreita.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-2i

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Ympäristöjen valvonta

**Vaatimus**

Poikkeavan toiminnan havaitsemiseksi on luotuja indikaattoreita arvioidaan ja päivitetään säännöllisesti ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-3a

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Tilannekuvan ylläpito

**Vaatimus**

Toiminnon kyberturvallisuuden tilannekuvan viestimiseksi on määritetty menetelmät, joita päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-3b

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Tilannekuvan ylläpito

**Vaatimus**

Valvontatieto kootaan yhteen toiminnon operatiivisen tilannekuvan muodostamiseksi.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-3c

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Tilannekuvan ylläpito

**Vaatimus**

Tilannekuvan rikastamiseksi on saatavilla soveltuvaa tietoa eri puolilta yritystä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-3d

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Tilannekuvan ylläpito

**Vaatimus**

Tilannekuvan raportoinnista on määritetty vaatimuksia, joihin kuuluu oikea-aikaisen kyberturvallisuustiedon jakaminen yrityksen määrittelemille sidosryhmille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-3e

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Tilannekuvan ylläpito

**Vaatimus**

Tilannekuvan rikastamiseksi kerätään soveltuvaa tietoa yrityksen ulkopuolelta. Lisäksi tätä tietoa jaetaan yrityksen määrittelemille sisäisille sidosryhmille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-3f

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Tilannekuvan ylläpito

**Vaatimus**

Kyvykkyys kerätä, ryhmitellä, vertailla ja analysoida valvonnalla tuottua tietoa sekä muodostaa liki reaaliaikaista tilannekuvaa toinnon kyberturvallisuuden tilasta. Kyvykkyyttä myös ylläpidetään.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-3g

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Tilannekuvan ylläpito

**Vaatimus**

Toiminnassa noudatetaan ennalta määriteltyjä, dokumentoituja toimintatiloja, jotka otetaan käyttöön toiminnon kyberurvallisuustilanteen mukaisesti tai muiden osa-alueiden toimintojen käynnistämänä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-4a

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

SITUATION-osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-4b

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

SITUATION-osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-4c

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

SITUATION-osion toimintaa ohjataan vaatimuksilla, jotka on asetettu yrityksen johtotason politiikassa (tai vastaavassa ohjeistuksessa).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-4d

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

SITUATION-osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-4e

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

SITUATION-osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: SITUATION-4f

Osa-alue: Tilannekuva (SITUATION)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

SITUATION-osion toiminnan vaikuttavuutta arvioidaan ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-1a

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkoston tunnistaminen ja priorisointi

**Vaatimus**

Merkittävät kumppaniverkoston IT-riippuvuudet (ja mahdolliset OT-riippuvuudet) on tunnistettu (tällä tarkoitetaan sellaisia sisäisiä tai ulkoisia toimijoita, joista toiminto on riippuvainen - mukaan lukien toimintojen operoinnista vastaavat kumppanit). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-1b

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkoston tunnistaminen ja priorisointi

**Vaatimus**

Kumppaniverkoston toimijat / palveluntarjoajat, joilla on pääsy, hallinnointioikeus, tai ylläpitovastuu tai pääsevät muutoin käyttämään toiminnon kannalta tärkeitä laitteita, ohjelmistoja tai tietovarantoja, on tunnistettu (vähintään tapauskohtaisesti). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-1c

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkoston tunnistaminen ja priorisointi

**Vaatimus**

Toimittajista ja muista kumppaneista aiheutuvien riskien tunnistamiseen käytetään määriteltyjä menetelmiä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-1d

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkoston tunnistaminen ja priorisointi

**Vaatimus**

Kumppaniverkoston toimijat on priorisoitu käyttäen määriteltyjä kriteerejä (esimerkiksi tärkeys toiminnolle, mahdollisen loukkauksen tai häiriötilanteen vaikutus, mahdollisuus neuvotella sopimuksiin asetettavista kyberturvallisuusvaatimuksista).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-1e

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkoston tunnistaminen ja priorisointi

**Vaatimus**

Korotettu prioriteetti on osoitettu sellaisille toimittajille ja muille kumppaniverkoston toimijoille, joiden vaarantuminen tai häiriintyminen voisi johtaa merkittäviin seuraamuksiin (esimerkiksi riippuvuudet yksittäisistä toimittajista tai toimittajista, joilla on erityisoikeuksia).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-1f

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkoston tunnistaminen ja priorisointi

**Vaatimus**

Toimittajien ja muiden kumppaniverkoston toimijoiden priorisointia päivitetään aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2a

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Toimittajien ja muiden kumppaniverkoston toimijoiden valintaan vaikuttaa arvio niiden kyberturvallisuuskelpoisuuksista. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2b

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Tuotteiden ja palveluiden valintaan vaikuttaa arvio niiden kyberkyvykkyyksistä. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2c

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Määriteltyjä menetelmiä noudatetaan, kun tunnistetaan kyberturvallisuusvaatimuksia ja toteutetaan niihin liittyviä suojaustoimia, joilla suojaudutaan toimittajista ja kumppaniverkoston toimijoista aiheutuvilta riskeiltä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2d

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Määriteltyjä menetelmiä noudatetaan, kun arvioidaan ja valitaan toimittajia ja muita kumppaniverkoston toimijoita.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2e

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Tiukempia suojaustoimia toteutetaan korkean prioriteetin toimittajille ja muille kumppaniverkoston toimijoille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2f

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Kyberturvallisuusvaatimukset (esimerkiksi haavoittuvuustiedotus, poikkeamatapausten SLA vaatimukset) ovat osa toimittajien ja muiden kumppaniverkoston toimijoiden kanssa laadittavia sopimuksia.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2g

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Toimittajat ja muut kumppaniverkoston toimijat osoittavat aika ajoin kykynsä täyttää asetetut kyberturvallisuusvaatimukset.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2h

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Toimittajille ja muille kumppaniverkoston toimijoille asetetut kyberturvallisuusvaatimukset sisältävät soveltuvin osin vaatimuksia turvallisesta ohjelmisto- ja tuotekehityksestä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2i

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Tuotteiden valintakriteereissä on huomioitu asianmukaisesti käyttöiän tai käyttötuen päättymisen ajankohdat.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2j

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Valintakriteereiden osana on huomioitu asianmukaisesti toimet väärennettyjä tai vaarantuneita ohjelmistoja, laitteita tai palveluita vastaan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2k

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Korkean prioriteetin omaisuuserien (laitteiden, ohjelmistojen ja tietovarantojen) valintakriteerit sisältävät ns. materiaaliluettelon (bill of materials) ainakin on keskeisten osien, kuten laitteiston ja ohjemlmistojen osalta.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2l

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Korkean prioriteetin omaisuuserien (laitteiden, ohjelmistojen ja tietovarantojen) valintakriteereissä on huomioitu kaikki kolmannen osapuolen hosting ympäristöt ja lähdekoodi

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-2m

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Kumppaniverkostoon liittyvien riskien hallinta

**Vaatimus**

Hankittavien laitteiden, ohjelmistojen ja tietovarantojen hyväksyntätestaukseen kuuluu kyberturvallisuusvaatimusten testaus.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-3a

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THIRD-PARTIES-osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja ylläpidetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-3b

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THIRD-PARTIES-osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-3c

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THIRD-PARTIES-osion toimintaa ohjataan vaatimuksilla, jotka on asetettu yrityksen johtotason politiikassa (tai vastaavassa ohjeistuksessa).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-3d

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THIRD-PARTIES-osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-3e

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THIRD-PARTIES-osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THIRD-PARTIES-3f

Osa-alue: Kumppaniverkoston riskien hallinta (THIRD-PARTIES)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THIRD-PARTIES-osion toiminnan vaikuttavuutta arvioidaan ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1a

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Haavoittuvuuksien tunnistamisen tueksi on tunnistettu soveltuvia tietolähteitä. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1b

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Haavoittuvuustietoa kerätään ja sitä tulkitaan toimintoa varten. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1c

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Haavoittuvuusarviointeja suoritetaan. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1d

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Toiminnon kannalta olennaisiin haavoittuvuuksiin puututaan (esimerkiksi lisäämällä valvontaa tai asentamalla korjauspäivityksiä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1e

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Haavoittuvuustiedon lähteet kattavat korkean prioriteetin laitteet ja ohjelmistot ja näitä tietolähteitä seurataan säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1f

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Haavoittuvuusarviointeja suoritetaan aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1g

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Tunnistetut haavoittuvuudet analysoidaan, priorisoidaan ja niihin puututaan tilanteen edellyttämin keinoin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1h

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Ohjelmistokorjausten vaikutus toiminnon operatiiviseen toimintaan arvioidaan ennen korjausten asentamista tai rajoitustoimia (mitigation).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1i

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Tietoa löydetyistä kyberturvallisuushaavoittuvuuksista jaetaan yrityksen määrittelemille sidosryhmille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1j

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Kaikkille toimintoon kuuluvien IT- ja OT-omaisuuserille (laitteet, ohjelmistot ja tietovarannot) on tunnistettu haavoittuvuustietolähteet, joita myös seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1k

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Haavoittuvuusarvioinnit suorittaa toiminnon operatiivisesta toiminnasta irrallaan oleva riippumaton taho.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1l

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Haavoittuvuuksien seurantaan kuuluu myös toimenpiteiden katselmus, jolla varmistetaan, että haavoittuvuuksia rajaavat tai korjaavat toimenpiteet ovat olleet tehokkaita.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-1m

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Haavoittuvuuksien vähentäminen

**Vaatimus**

Yrityksellä on prosessit vastaanottaa ja käsitellä ulkoisien sidosryhmien lähettämiä raportteja mahdollisista haavoittuvuuksista (esim Bug Bounty), jotka koskevat yrityksen IT- tai OT-laitteita, ohjelmistoja ja tietovarantoja, esimerkiksi internetiin avoimia palveluja tai mobiiliapplikaatioita.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2a

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Uhkien tunnistamisen tueksi on tunnistettu soveltuvia tietolähteitä. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2b

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Kyberuhkatietoa kerätään ja sitä tulkitaan toimintoa varten vähintäänkin tapauskohtaisesti (ad hoc). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2c

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Toimintoon kohdistuvat uhkatoimijoiden tavoitteet on tunnistettu ainakin tapauskohtaisesti. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2d

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Toiminnon kannalta olennaisiin uhkiin puututaan (esimerkiksi lisäämällä valvontaa tai seuraamalla uhkien kehitystä). Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2e

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Toiminnolle on määritetty uhkaprofiili. Uhkaprofiilissa kuvataan uhkatavoitteet sekä lisäksi uhkan ominaispiirteitä, kuten tyypilliset uhkatekijät, motiivit, kyvykkyydet ja kohteet.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2f

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Uhkatiedon lähteet kattavat kaikki uhkaprofiilin eri osat ja näitä tietolähteitä seurataan säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2g

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Tunnistetut uhat analysoidaan, priorisoidaan ja niihin puututaan tilanteen edellyttämin keinoin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2h

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Sidosryhmien kanssa vaihdetaan uhkatietoa (näitä voivat olla esimerkiksi johto, operatiivinen henkilöstö, viranomaiset, palveluntoimittajat, viranomaiset, toimialan muut yritys, ISAC-ryhmät tai yrityksen muut sisäiset ja ulkoiset sidosryhmät).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2i

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Toiminnon uhkaprofiili päivitetään aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten tai ulkoisten tapahtumien yhteydessä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2j

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Uhkien seurannassa ja niihin reagoimisessa noudatetaan ennalta määriteltyjä toimintatiloja [kts. SITUATION-3g].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-2k

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Uhkien torjunta ja uhkatiedon jakaminen

**Vaatimus**

Uhkatietoa käsitellään noudattaen turvallisia ja mahdollisimman reaaliaikaisia menetelmiä, joilla varmistetaan uhkien nopea analysointi ja nopea puuttuminen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-3a

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THREAT-osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-3b

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THREAT-osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-3c

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THREAT-osion toimintaa ohjataan vaatimuksilla, jotka on asetettu yrityksen johtotason politiikassa (tai vastaavassa ohjeistuksessa).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-3d

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THREAT-osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-3e

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THREAT-osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: THREAT-3f

Osa-alue: Uhkien ja haavoittuvuuksien hallinta (THREAT)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

THREAT-osion toiminnan vaikuttavuutta arvioidaan ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-1a

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuden vastuiden jakaminen

**Vaatimus**

Erilaisia tarkastuksia (esimerkiksi taustojen tarkistuksia, huumetestejä) suoritetaan uusia työntekijöitä palkatessa. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-1b

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuden vastuiden jakaminen

**Vaatimus**

Työsuhteen päättymiseen liittyvissä menettelyissä huomioidaan kyberturvallisuus. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-1c

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuden vastuiden jakaminen

**Vaatimus**

Soveltuvia tarkastuksia suoritetaan sellaisille työntekijöille, joilla on käyttö- tai pääsyoikeus toiminnon kannalta tärkeisiin laitteisiin, ohjelmistoihin tai tietovarantoihin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-1d

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuden vastuiden jakaminen

**Vaatimus**

Työntekijöiden sisäisiin siirtoihin liittyvissä menettelyissä huomioidaan kyberturvallisuus. (huomioidaan kriittiset työyhdistelmät, oikeudet, tarve mahdollisille taustatarkistuksille/ turvallisuusselvityksille)

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-1e

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuden vastuiden jakaminen

**Vaatimus**

Henkilöstö on tietoinen vastuistaan ja velvoitteistaan koskien (IT ja OT) laitteiden, ohjelmistojen ja tietovarantojen suojaamista ja hyväksyttävää käyttöä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-1f

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuden vastuiden jakaminen

**Vaatimus**

Jokaista työtehtävää varten teetetään soveltuvat tarkistukset, jotka ovat suhteessa työtehtävän riskeihin (mukaan lukien työntekijät, toimittajat ja alihankkijat).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-1g

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuden vastuiden jakaminen

**Vaatimus**

Yrityksellä on muodollinen vastuullisuusprosessi, johon sisältyy kurinpitomenettelyhenkilöstölle, joka ei noudata määriteltyjä turvallisuuspolitiikkoja ja menettelyjä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-2a

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen

**Vaatimus**

Henkilöstön kyberturvallisuustietoisuutta kohotetaan erilaisin toimin. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-2b

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen

**Vaatimus**

Kyberturvallisuustietoisuudelle on asetettu tavoitteet, joita ylläpidetään ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-2c

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen

**Vaatimus**

Kyberturvallisuustietoisuuden tavoitteet ovat linjassa yrityksen määrittämän uhkaprofiilin kanssa [kts. THREAT-2e].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-2d

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen

**Vaatimus**

Kyberturvallisuustietoisuutta parantava toiminta on säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-2e

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen

**Vaatimus**

Kyberturvallisuustietoisuutta edistävä toiminta on sisällytetty toimenkuvauksiin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-2f

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen

**Vaatimus**

Kyberturvallisuustietoisuuden kohottamisen toimenpiteet ovat linjassa yrityksen ennalta määriteltyjen toimintatilojen kanssa [kts. SITUATION-3g].

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-2g

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen

**Vaatimus**

Kyberturvallisuustietoisuutta parantavien toimenpiteiden tehokkuutta arvioidaan säännöllisesti ja tiettyjen muutosten yhteydessä kuten järjestelmämuutokset, ulkoiset tapahtumat. Toimintaa kehitetään tarvittaessa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-3a

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Henkilöstöhallinnon prosessit

**Vaatimus**

Toiminnon kyberturvallisuuteen liittyvät vastuut on tunnistettu. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-3b

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Henkilöstöhallinnon prosessit

**Vaatimus**

Kyberturvallisuuteen liittyvät vastuut on osoitettu nimetyille henkilöille. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-3c

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Henkilöstöhallinnon prosessit

**Vaatimus**

Kyberturvallisuuteen liittyvät vastuut on osoitettu nimetyille rooleille (mukaan lukien mahdolliset ulkoiset palveluntarjoajat).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-3d

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Henkilöstöhallinnon prosessit

**Vaatimus**

Kyberturvallisuuteen liittyvät vastuut on dokumentoitu.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-3e

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Henkilöstöhallinnon prosessit

**Vaatimus**

Kyberturvallisuuteen liittyvät vastuut ja työtehtävien vaatimukset tarkastetaan ja päivitetään aika ajoin ja määriteltyjen tilanteiden kuten järjestelmämuutosten yhteydessä tai yritysrakenteen muuttuessa.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-3f

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Henkilöstöhallinnon prosessit

**Vaatimus**

Osoitettuja kyberturvallisuuden vastuita hallitaan siten, että varmistutaan niiden riittävyydestä ja riittävästä päällekkäisyydestä (mukaan lukien henkilöstönvaihdosten suunnittelu).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-4a

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Koulutus ja kybertietoisuuden lisääminen

**Vaatimus**

Kyberturvallisuuskoulutusta on saatavana sellaisille työntekijöille, joille on osoitettu kyberturvallisuuteen liittyviä vastuita. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-4b

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Koulutus ja kybertietoisuuden lisääminen

**Vaatimus**

Kyberturvallisuuteen liittyvien tietojen, taitojen ja kykyjen vaatimukset ja niissä mahdollisesti ilmenevät puutteet on tunnistettu sekä nykyiset että tulevat tarpeet huomioiden. Tasolla 1 tämän ei tarvitse olla systemaattista ja säännöllistä.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-4c

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Koulutus ja kybertietoisuuden lisääminen

**Vaatimus**

Tunnistettuihin kyberturvallisuuden osaamispuutteisiin (tiedot, taidot ja kyvyt, pätevyydet) puututaan kouluttamalla, rekrytoimalla ja vaihtuvuuden pienenemiseen tähtäävillä toimilla.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-4d

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Koulutus ja kybertietoisuuden lisääminen

**Vaatimus**

Kyberturvallisuuskoulutus on edellytyksenä käyttö- tai pääsyoikeuksien myöntämiselle toiminnon kannalta tärkeisiin laitteisiin, ohjelmistoihin ja tietovarantoihin.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-4e

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Koulutus ja kybertietoisuuden lisääminen

**Vaatimus**

Koulutustoiminnan tehokkuutta arvioidaan aika ajoin ja koulutusta kehitetään tarpeen mukaan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-4f

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Koulutus ja kybertietoisuuden lisääminen

**Vaatimus**

Koulutusohjelmat sisältävät jatkokoulutusta ja muita ammatillisia kehitysmahdollisuuksia henkilöstölle, jolla on merkittävisä kyberturvallisuusvastuita.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-5a

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

WORKFORCE-osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-5b

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

WORKFORCE-osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-5c

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

WORKFORCE-osion toimintaa ohjataan vaatimuksilla, jotka on asetettu yrityksen johtotason politiikassa (tai vastaavassa ohjeistuksessa).

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-5d

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

WORKFORCE-osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on jalkautettu soveltuville työntekijöille.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-5e

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

WORKFORCE-osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

Tunniste: WORKFORCE-5f

Osa-alue: Henkilöstön johtaminen ja kehittäminen (WORKFORCE)

Alakohta: Yleisiä hallintatoimia

**Vaatimus**

WORKFORCE-osion toiminnan vaikuttavuutta arvioidaan ja seurataan.

**Pisteytys** ✔ 0 1 2 3 4

Havainnot ja perustelut (2000 merkkiä)

Kehitystoimenpiteet (2000 merkkiä)

| | |
|---|---|
| Kokonaispisteet | 0 / 1532 |
| Maksimipisteet | 1532 |
| Täyttymisaste % | 0.0 % |
| Vastattu / yhteensä | 0 / 383 |
| Kypsyystaso | 0 / 5 |
| Liikennevalo / tila | EI ARVIOITU |

**Selite: arviointiasteikko ja kypsyystaso**

Arviointiväittämän pisteet ovat 0-4. Yrityksen kypsyystaso on raportissa 0-5. Kypsyystaso muodostetaan arviointiväittämien tuloksista.

**Liikennevalot**

| | |
|---|---|
| EI ARVIOITU | 0.0 % tai ei vastauksia |
| PUNAINEN - Kriittinen kehitystarve | 0.1-49.9 % |
| KELTAINEN - Osittain hallinnassa | 50.0-84.9 % |
| VIHREA - Hyvä taso | 85.0-100.0 % |

**Kypsyystasot**

0 Ei arvioitu
1 Alkuvaihe
2 Kehittyvä
3 Hallittu
4 Edistynyt
5 Optimoitu

| Osa-alue | Vastattu / yhteensä | Keskipisteet | Kypsyystaso | Tila |
|---|---|---|---|---|
| Identiteetin- ja pääsynhallinta (ACCESS) | 0 / 35 | 0.00 | 0 / 5 | EI ARVIOITU |
| Kyberturvallisuusarkkitehtuuri (ARCHITECTURE) | 0 / 58 | 0.00 | 0 / 5 | EI ARVIOITU |
| Omaisuuden, muutosten ja konfiguraation hallinta (ASSET) | 0 / 36 | 0.00 | 0 / 5 | EI ARVIOITU |
| Kriittisten palveluiden suojaaminen (CRITICAL) | 0 / 27 | 0.00 | 0 / 5 | EI ARVIOITU |
| Kyberturvallisuuden hallinta (PROGRAM) | 0 / 24 | 0.00 | 0 / 5 | EI ARVIOITU |
| Tapahtumien ja poikkeamien hallinta, toiminnan jatkuvuus (RESPONSE) | 0 / 49 | 0.00 | 0 / 5 | EI ARVIOITU |
| Riskienhallinta (RISK) | 0 / 39 | 0.00 | 0 / 5 | EI ARVIOITU |
| Tilannekuva (SITUATION) | 0 / 28 | 0.00 | 0 / 5 | EI ARVIOITU |
| Kumppaniverkoston riskien hallinta (THIRD-PARTIES) | 0 / 25 | 0.00 | 0 / 5 | EI ARVIOITU |
| Uhkien ja haavoittuvuuksien hallinta (THREAT) | 0 / 30 | 0.00 | 0 / 5 | EI ARVIOITU |
| Henkilöstön johtaminen ja kehittäminen (WORKFORCE) | 0 / 32 | 0.00 | 0 / 5 | EI ARVIOITU |