KATAKRI

Kansallinen turvallisuusauditointikriteeristö

versio II, 2011

Elinkeinoelämän keskusliitto EK

Viestintävirasto

FORMIN.FINLAND.FI
ULKOASIAINMINISTERIÖ
UTRIKESMINISTERIET

SISÄASIAINMINISTERIÖ

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

Sisällysluettelo

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

PL 31, 00131 HELSINKI

www.defmin.fi

Taitto: Tiina Takala/puolustusministeriö

ISBN: 978-951-25-2245-3 (nid.)
ISBN: 978-951-25-2246-0 (pdf)

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

SAATE 1 (1)

1325/50.01.00/2009
FI.PLM.2009-4910

20.11.2009

Sisäasiainministeriö

SISÄISEN TURVALLISUUDEN OHJELMA II, TOIMENPIDE 6.4. tp 2, KANSALLINEN TURVALLISUUSAUDITOINTIKRITEERISTÖ

Hallitus vahvisti 8.5.2008 sisäisen turvallisuuden ohjelman toisen vaiheen (STO II). Kyseisen ohjelman toimenpide-ehdotuksen 6.4 toinen toimenpide oli osoitettu puolustusministeriön johtovastuulle. Toimenpiteelle perustettiin johtoryhmä 12.9.2008 ja se organisoitui kokonaisuudessaan 5.12.2008 pidetyssä aloitusseminaarissa. Työn oli määrä olla valmis vuoden 2009 loppuun mennessä. Työ on luovutusvalmis tällä päivämäärällä.

Toimenpiteen tarkoituksena oli luoda viranomaisille ja yrityksille yhteinen turvallisuuskriteeristö yhteisöturvallisuusmenettelyn yhtenäistämiseksi ja omavalvonnan sekä auditoinnin parantamiseksi. Toimenpiteen vastuualueen kattamiseksi johtoryhmä päätti perustaa neljä työryhmää sekä lisäksi erillisen seurantaryhmän palautteen saamiseksi työn eri vaiheissa.

Puolustushallinto, etunenässä puolustusvoimat, on pitkään huolehtinut niistä turvallisuusviranomaisen viranomaisvelvoitteista, joihin on ollut välttämätöntä vastata kansainvälisten sopimusten ja muiden käytänteiden vuoksi yritysten turvallisuustason varmentamiseksi. Sisäasiainhallinto on vuonna 2009 ottanut osaltaan vastuun näistä velvoitteista. Kansallinen turvallisuusauditointikriteeristö valmisteltiin laajalla otannalla maamme viranomais-, järjestö- ja yrityskentästä. Toimenpiteeseen osallistui yli sata henkilöä. Mittava työmäärä on jalostunut kriteeristöksi, jossa on huomioitu työn kuluessa välillä kovaakin ristivetoa aiheuttaneet kansalliset ja kansainväliset sidonnaisuudet. Täydellinen nyt valmistunut kriteeristö ei varmastikaan ole, joten työtä on syytä jatkaa, mihin toimenpiteen johtoryhmä liitteenä olevissa suosituksissaan ottaakin kantaa.

Esitän sisäasiainministeriölle, että tämä kansallinen turvallisuusauditointikriteeristö otetaan käyttöön viranomaisten yrityksiin kohdistaman turvallisuusauditoinnin perustana.

Kansliapäällikkö
Kari Rimpi

LIITTEET Toimenpiteen johtoryhmän suositukset (liite 1)
Luettelo toimenpiteeseen osallistuneista (liite 2)
Kansallinen turvallisuusauditointikriteeristö (liite 3

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8 A
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
(09) 16001
Internat. +358 9 16001

Faksi
Fax
Fax
(09) 160 88278
Internat. +358 9 160 88278

s-posti, internet
e-post, internet
e-mail, internet
puolustusministerio@defmin.fi
www.defmin.fi

FORMIN.FINLAND.FI

ULKOASIAINMINISTERIÖ
Kansallinen turvallisuusviranomainen

LÄHETE 05.11.2010

HELM545-4

Puolustusministeriö, turvallisuusyksikkö
Pääesikunta, tutkintaosasto
Suojelupoliisi, lausuntotoimisto
Viestintävirasto, NCSA-FI

Viite

Asia
Kansallisen turvallisuusauditointikriteeristön vahvistaminen viralliseksi auditointitikriteeristöksi kansallisen turvallisuusviranomaisen organisaatiossa

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) valmistui 20.11.2009 osana hallituksen sisäisen turvallisuuden ohjelmaa. Toimenpide valmisteltiin yhteistyössä viranomaisten, elinkeinoelämän ja turvallisuusalan toimijoiden kesken. Työn lopputulos on sekä kansallisesti että kansainvälisesti merkittävä. KATAKRIn olemassaolo mahdollistaa paitsi sitä käyttävien vastuuviranomaisten toiminnan läpinäkyvyyden ja yhtäläisyyden, myös elinkeinoelämän kustannustehokkaan turvallisuustoiminnan viranomaisvaatimusten ollessa ennakoitavissa.

Kansainvälisten tietoturvallisuusvelvoitteiden täyttämiseksi KATAKRI on ensiarvoinen työkalu määrätyille turvallisuusviranomaisille niiden todentaessa suomalaisten yritysten tai muiden yhteisöjen turvallisuustasoa. Tällaiset velvoitteet ovat yhä tavallisempia esimerkiksi Euroopan unionin hankkeissa. KATAKRI on myös erinomainen työkalu haluttaessa varmistua siitä, että valtionhallinnolle palveluja tarjoava taho kykenee toimimaan riittävän turvallisesti valtionhallinnon turvallisuusluokitelluissa hankkeissa.

Sisäisen turvallisuuden ministeriryhmä suositteli 26.11.2009 annetussa päätöksessään KATAKRIn käyttöönottoa. Samalla ministeriryhmä päätti, että sisäisen turvallisuuden ohjelman ohjausryhmän tulee valmistella päätökset, jotka koskevat johtoryhmän antamia suosituksia toimeenpanosta, ylläpidosta ja jatkovalmistelusta. Näiden päätösten toimeenpano on käynnistynyt.

KATAKRI tukee omalta osaltaan tietoturvallisuusasetuksen, sitä täydentävien ohjeiden sekä erillisten varautumis- ja huoltovarmuusperusteisten ohjeistojen toimeenpanoa. Se on pyritty laatimaan näiden kanssa ristiriidattomaksi. KATAKRI on nähtävä myös osana yhteiskunnan elintärkeiden toimintojen turvaamiseen tähtäävää toimenpidekokonaisuutta.

Kansallinen turvallisuusviranomainen vahvistaa täten, että kansallinen turvallisuusauditointikriteeristö otetaan virallisesti käyttöön kansallisen turvallisuusviranomaisen organisaatiossa.

Charles Murto
Kansallisen turvallisuusviranomaisen päällikkö, suurlähettiläs

Liitteet Kansallinen turvallisuusauditointikriteeristö

Postiosoite
PL 176
00023 VALTIONEUVOSTO

Kanavakatu 3 B

Vaihde
+358-(0)9-160 05

Telefax
+358-(0)9-629 840

Johdanto

Tässä turvallisuusauditointikriteeristön toisessa julkaisuversiossa keskitytään ainoastaan ns. security-turvallisuuteen.

Kansallisen turvallisuusauditointikriteeristön päätavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa yrityksessä tai muussa yhteisössä kohteen turvallisuustason todentavan tarkastuksen, auditoinnin. Viranomainen voi tarpeen mukaan täydentää auditointia arvioinneilla, joissakin tapauksissa jopa konsultoinnilla. Nämä toimet eivät kuitenkaan kuulu itse auditoinnin, eivätkä tämän kriteeristön piiriin. Tämä kriteeristö toimii kansallisesti velvoittavana asiakirjana silloin, kun suomalaisten yritysten turvallisuustaso varmennetaan kansallisen turvallisuusviranomaisen toimesta kansainväliseen viranomaispyyntöön pohjautuen ja yritysturvallisuustodistuksen myöntämiseen tähdäten. Kriteeristö ei ota kantaa suojaustason I (turvallisuusluokitusmerkintä ERITTÄIN SALAINEN) tiedon turvaamismenettelyihin, koska kyseisen tason tietojen luovuttaminen yrityksille on äärimmäisen harvinaista ja vaatii aina viranomaisen erillispäätöksen turvaamistoimista.

Turvallisuusauditointikriteeristön toinen päätavoite on auttaa yrityksiä ja muita yhteisöjä sekä myös viranomaisia sidosryhmineen omassa sisäisessä turvallisuustyössään. Kriteeristö sisältää tästä syystä erilliset, viranomaisvaatimusten ulkopuoliset ”elinkeinoelämän suositukset”, joista toivotaan voitavan poimia kulloinkin käyttökelpoisia turvallisuuskäytänteitä ja edetä tätä kautta tarvittaessa viranomaisvaatimusten tasolle.

Turvallisuusauditointikriteeristössä esitettyjä vaatimuksia ei saa käyttää perusteena sellaiselle (turvallisuus)toiminnalle, joka saattaisi vaarantaa ihmishenkiä. Tällä tarkoitetaan esimerkiksi sitä, että ihmisten pelastustoimia ei saa estää tiedon turvaamisvaatimukseen vedoten.

Turvallisuusauditointikriteeristön toinen versio jakautuu ensimmäisen version tavoin neljään pääosioon: hallinnollinen turvallisuus (turvallisuusjohtaminen), henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Auditointitapahtumassa tulee huomioida näiden kaikkien neljän osion vaatimukset, eli osioita ei ole rakennettu itsenäisiksi kokonaisuuksiksi. Ensimmäisestä versiosta poiketen tuolloin tietoturvallisuusosioon sisältyneet muiden osioiden alaan kuuluneet vaatimukset on siirretty nyt kuhunkin erityisosioon (esim. laitetilavaatimukset viety osaksi fyysisen turvallisuuden vaatimuksia). Viranomaisvaatimukset noudattavat kolmiportaista luokittelua, joka vastaa valtionhallinnon tietoturvallisuusasetuksen mukaisia turvallisuustasokäsitteitä – perustaso, korotettu taso ja korkea taso. Näitä täydentävät edellä mainitut elinkeinoelämän suositukset.

Kansallinen turvallisuusauditointikriteeristö on rakennettu ehdottomien vaatimusten näkökulmasta, eikä se sisällä joissakin kriteeristöissä käytettävää pisteytysmenettelyä. Tällä on pyritty siihen, ettei auditoinnin lopputulokseen jäisi mahdollisesti tunnistamattomia, mutta kriittisiä riskejä. Valittu menettely asettaa erityisiä vaatimuksia turvallisuusauditointeja toteuttavalle henkilöstölle, mihin pyritään vastaamaan tämän kriteeristön toisen version myötä käynnistyvillä turvallisuusauditoinnin koulutusohjelmilla. Koulutuksen erityistavoitteena on luoda auditoijille kyky korvaavien – siis kriteeristössä nimenomaisesti mainitsemattomien - keinojen hyödyntämiseen tapauksissa, joissa yksittäisen vaatimuksen täyttäminen tai toteuttaminen on vaikeaa taikka mahdotonta. On kuitenkin huomattava, että korvaavien keinojen hakeminen ei kuulu itse auditointitoiminnan piiriin, vaan palvelee menossa olevaa auditointitapahtumaa sen jatkumiseen tähtäävänä toimena.

Valtionhallinnolla on käytössään ja jatkuvasti valmisteilla useita yhteiskunnan elintärkeiden toimintojen turvaamisen alaan liittyviä ohjeistoja, jotka omalta osaltaan täydentävät nyt käyttöön otettavaa turvallisuusauditointikriteeristöä. Voimassa olevat linjaukset on pyritty huomioimaan tässä kriteeristötyössä. Mainittavia rinnakkaisaineistoja ovat edellä mainittua tietoturvallisuusasetusta täydentävä valtionhallinnon tietoturvallisuuden johtoryhmän ohje 2/2010, Euroopan Unionin vuonna 2011 päivittynyt turvallisuussäännöstö sekä varautumiseen, jatkuvuuden hallintaan ja huoltovarmuuteen keskittyvät kotimaiset ohjeet.

Kansallisen turvallisuusauditointikriteeristön käytön kuvaus

Kansallinen turvallisuusauditointikriteeristö KATAKRI on tarkoitettu työvälineeksi niille viranomaisille tai viranomaisten lukuun toimiville turvallisuustarkastajille (auditoijille), joille on annettu valtuus todentaa auditoinnin kohteen turvallisuuden taso erityisesti KATAKRI:n vaatimuksiin peilaten. KATAKRI ja sen suositusosio on suunnattu myös perustyökaluksi yritysten omaehtoiselle turvallisuustyölle. On huomattava, että elinkeinoelämän suositukset eivät ole viranomaisvaatimuksia. Suositusten toteuttaminen on kuitenkin varma ja oikean suuntainen tie yrityksille silloin, kun halutaan varautua etukäteen tilanteeseen, jolloin viranomaisvaatimukset joudutaan täyttämään.

Toimivaltaiset viranomaiset toteuttavat yritysten tai muiden kohteiden turvallisuustason tarkastamisen joko valtionhallinnon salassa pidettävää tietoa sisältäviin hankkeisiin liittyen, tai kansainvälisen pyynnön seurauksena. Jälkimmäisessä tapauksessa tilanne on usein se, että suomalainen yritys pääsee osallistumaan kansainväliseen tarjouskilpailuun, mikäli se täyttää hankkeen turvallisuusvaatimukset. Vaatimukset täyttävälle yritykselle toimivaltainen viranomainen voi myöntää tästä erillisen todistuksen (kansainvälisessä yhteydessä Facility Security Clearance, FSC). Olipa kyseessä kotimainen tai ulkomainen tarveasettelu, suomalaiset viranomaiset käyttävät turvallisuustason todentamiseen samoja vaatimuksia, jotka on esitetty KATAKRIssa kolmelle turvallisuustasolle: perustaso, korotettu taso ja korkea taso. Nämä vastaavat kansainvälisiä tasokäsitteitä RESTRICTED, CONFIDENTIAL ja SECRET.

Kohdeorganisaation turvallisuustason todentaminen auditoinnin kautta on vaativa tehtävä. Valtionhallinto hyväksyy tehtävään vain erillisen turvallisuusauditoijan koulutuksen saaneita henkilöitä. Laajamittainen turvallisuusauditoijan koulutus on käynnistymässä ammattikorkeakoulutasoisena KATAKRI:n toisen version myötä syksyllä 2011. Tämän lisäksi täydennyskoulutuksena annettavaa turvallisuusauditointikoulutusta voivat hyödyntää ne henkilöt, joiden tarvitsee tuntea kansallisen turvallisuusauditointikriteeristön vaatimukset erityisesti oman organisaationsa turvallisuustoimintaan liittyen.

Auditointiprosessi

Turvallisuusauditointi on vuorovaikutteinen tapahtuma. Koulutettu auditoija tutustuu prosessin aluksi kohteen turvallisuusdokumentaatioon ja pyrkii jo tätä kautta saamaan vastaukset erityisesti hallinnollisen turvallisuuden kysymyksiin. Mikäli auditoija tässä yhteydessä havaitsee vakavia puutteita, hän tiedottaa havainnoista auditoinnin kohteelle, jotta useimmiten aikaa vievät korjaustoimet saadaan nopeasti käyntiin. Turvallisuusauditointitapahtumassa pääauditoija kiertää yleensä avustavan auditointiryhmän kanssa läpi tarkastettavat kohteet etukäteen tehdyn suunnitelman pohjalta. Auditoinnin tulokset kirjataan joko

- täytettyinä vaatimuksina tai
- poikkeamina vaatimuksista.

Mikäli jokin viranomaisvaatimuksista on mahdoton toteuttaa kyseessä olevassa toimintaympäristössä, turvallisuusvaatimustason täyttämiseksi auditointikohteena olevan yhteisön täytyy osoittaa muita, korvaavia turvallisuusmenettelyjä.

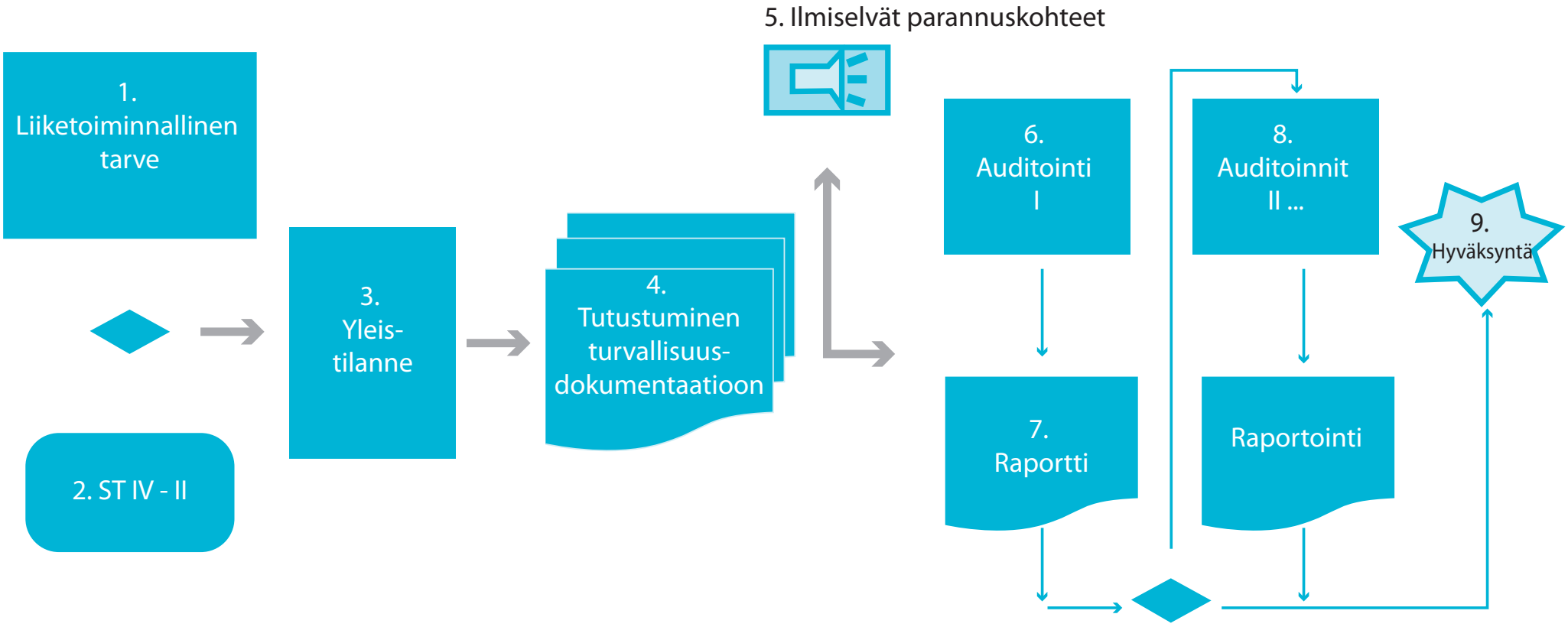
Auditointitapahtumasta annetaan välitön suusanallinen palaute. Kirjallinen raportti toimitetaan kohteelle mahdollisimman pian. Auditointitapahtumia jatketaan, kunnes esitetyt vaatimukset ovat täyttyneet. Auditoinnin yhteydessä on yleensä syytä kouluttaa yrityksen turvallisuusvastaavien toimesta kohdeorganisaation henkilöstö ymmärtämään turvallisuusvastuunsa.

Seuraavalla sivulla on esitetty esimerkki turvallisuusauditoinnin toteutuksesta prosessikaaviomuodossa.

Turvallisuusauditointiprosessi (tekninen suoritus)

SELITE

1. Tarpeen tunnistaminen
2. Tavoitetason määrittäminen
3. Kohteen yleistilanteen hahmottaminen
4. Dokumentaatiopohjainen tilannearviointi
5. Kommunikointi kohteelle pahimmista puutteista (optionaalinen)
6. Ensimmäinen auditointi
7. Auditointiraportti
8. Jatkoauditoinnit ja raportit
9. Hyväksyntä



A

OSA-ALUE

Hallinnollinen turvallisuus

Sisällys

Johdanto

Hallinnollisen turvallisuuden ja turvallisuusjohtamisen kysymyssarja turvallisuusauditointia varten.

Kriteeristön osa-aluetta on lähestytty tarkastelemalla hallinnollista turvallisuustyötä turvallisuuden johtamisena. Kokonaisuuden perusteena käsitellään turvallisuuden johtamisjärjestelmää ja sen osa-alueiden auditoinnissa vaadittavaa vähimmäistasoa suojaustasoissa II (korkea taso), III (korotettu taso) ja IV (perustaso). Lisäksi kriteeristö sisältää elinkeinoelämän omaehtoista turvallisuustyötä silmällä pitäen yrityksille annettavat yleissuositukset turvallisuusjohtamisen alalla.

Ohjeistoa sovelletaan alihankintaketjuun siten, kuin organisaatiolla on mahdollisuus toimeksiantonsa perusteella siirtää työtä alihankintaan. Organisaatio vastaa samojen periaatteiden auditoinnista alihankintayrityksissä.

Turvallisuusauditointikriteeristön ensimmäisen ja toisen version keskinäisiä eroja sisältävät kysymykset/vaatimukset on merkitty kysymyssarakkeeseen tähtimerkillä (*).

Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt, osa-alue A100

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
A 101.0 **Onko organisaation johto määrittänyt ja hyväksynyt turvallisuus-politiikan? Onko politiikka tarkis-tettu määräajoin?** *Kysymyksellä arvioidaan:* *Organisaation turvalli-suusjohtamisen kypsyys-tasoa*	Organisaatiolla on kirjattuna turvalli-suutta koskevat perusasiat erillise-nä dokumenttina tai osana yleisiä tavoitteita	Organisaatiolla on kirjattuna ylimmän johdon hyväksymä turvallisuuspolitiikka tai vastaava turvalli-suustoimintaa ohjaava hyväksytty määrittely.	Organisaatiolla on voimassa oleva, julkaistu ja koulutettu turvallisuuspolitiikan nimellä dokumentoitu turvallisuustoi-minnan ylätason asiakirja, joka on ylimmän johdon hyväksymä. Turvallisuuspolitiikka tarkistetaan vähintään vuosittain ja tarkistuk-set dokumentoidaan sekä hyväksy-tetään ylimmällä johdolla. Organisaation turvallisuuspoli-tiikka ohjaa seuraavia kokonai-suuksia: turvallisuuden vuotuinen toimintaohjelma, turvallisuustyön tavoitteet, riskien tunnistamisen arviointi ja kontrollit, turval-lisuusorganisaatio ja vastuut, onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta-ehkäisevät toimenpiteet, turvalli-suusdokumentaatio ja sen hallinta, koulutuksen ja tietoisuuden lisää-minen sekä osaamisen, raportoin-nin ja johdon katselmukset.	Organisaatiolla on kirjattu-na turvallisuutta koskevat perusasiat erillisenä doku-menttina tai osana yleisiä tavoitteita		

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
A 102.0 **Mitä turvallisuuden osatekijöitä turvallisuus-politiikka ja/tai turvalli-suuden johtaminen organisaatiossa kattaa?** *Kysymyksellä arvioidaan:* *Turvallisuustyön koko-naisvaltaisuutta ja järjes-telmällisyyttä.*	Turvallisuusdoku-mentaatio sisältää ainakin tila-, tieto- ja henkilöstötur-vallisuuden osa-alueet.	Turvallisuusdokumen-taatio sisältää ainakin tila-, tieto- ja henkilös-töturvallisuuden osa-alueet sekä turvallisuus-politiikassa todetun turvallisuusjohtamisen selkeän organisoinnin.	Turvallisuusdokumentaatio sisäl-tää perustan laajalle ja kokonais-valtaiselle lähestymistavalle. Esi-merkiksi turvallisuuskäsite kattaa: turvallisuusjohtamisen, tuotannon ja toiminnan turvallisuuden, työturvallisuuden, ympäristötur-vallisuuden, pelastustoiminnan, poikkeustilanteiden hallinnan, tietoturvallisuuden, henkilöstö-turvallisuuden, tilaturvallisuuden, ulkomaantoimintojen turvallisuu-den ja rikosturvallisuuden.	Turvallisuusdokumentaatio sisältää ainakin tila-, tieto- ja henkilöstöturvallisuuden osa-alueet.		
A 103.0 **Vastaako organisaation turvallisuusdokumentaa-tio toiminnan ja tuotteiden laajuutta ja toiminta-tapaa sekä niihin liittyviä turvallisuusriskejä?** *Kysymyksellä arvioidaan:* *Turvallisuuspolitiikan tasoa.*	Organisaatiolla on kirjattuna turvalli-suutta koskevat perusasiat erillise-nä projektidoku-menttina tai osana yleisten tavoitteita.	Turvallisuusdokumen-taatio käsittelee organi-saatiota yksilöllisesti ja ottaa huomioon muu-tokset organisaation toiminnassa	Organisaation turvallisuusdoku-mentaatio sisältää ja kattaa kaikki organisaation toimintaan kuuluvat menettelyt. Riskien käsittely on suhteessa organisaation toimintaan.	Organisaatiolla on kirjattu-na turvallisuutta koskevat perusasiat erillisenä projek-tidokumenttina tai osana yleisten tavoitteita.		

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
A 104.0 **Toimivatko organisaation kaikki tasot turvallisuuspolitiikan mukaisesti?** *Kysymyksellä arvioidaan:* *Turvallisuuspolitiikan sisältämien asioiden viemistä organisaation kaikille tasoille.*	Ei vaatimusta.	Organisaatiolla on selvä ohjelma valvoa turvallisuuspolitiikan perusteiden mukaista toimintaa. Valvonnan tulokset ovat esitettävissä.	Organisaatio pystyy sisäisten ja ulkoisten auditointien tuloksilla osoittamaan, että se kaikilla tasoilla sitoutuu turvallisuustyön vaatimuksiin ja niiden toteuttamiseen.	Organisaatio pystyy osoittamaan turvallisuustyössään turvallisuuspolitiikan tai projektidokumentin velvoitteiden valvonnan toteutumisen osana muuta valvontaa tai erillisenä turvallisuusauditointina.		
A 105.0 **Huomioiko turvallisuuspolitiikka yleisen lainsäädännön ja paikallisten turvallisuusmääräysten sisältämät velvoitteet?** *Kysymyksellä arvioidaan:* *Organisaatiota koskevan turvallisuuslainsäädännön tuntemusta ja lainsäädännön soveltamisen valvontaa.*	Turvallisuustoimintaa koskeva lainsäädäntö tunnetaan ja lainsäädännön vaatimukset on huomioitu turvallisuusohjeissa.	Turvallisuustoimintaa koskeva lainsäädäntö tunnetaan ja lainsäädännön vaatimukset on huomioitu turvallisuusohjeissa. Turvallisuuslainsäädännön seuraaminen on määritetty organisaation tehtävänkuvauksessa henkilön tai toiminnon tehtäväksi.	Organisaatiota koskevan turvallisuuslainsäädännön seuranta on vastuutettu tietylle henkilölle tai toiminnolle. Lainsäädännön soveltaminen ja sen seuranta turvallisuusohjeissa on myös määritetty tehtäväkuvauksissa.	Turvallisuustoimintaa koskeva lainsäädäntö tunnetaan ja lainsäädännön vaatimukset on huomioitu turvallisuusohjeissa.		

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
A 105.1 **Pääkysymys: Onko toiminnan lakisääteiset vaatimukset huomioitu?** *Lisäkysymykset:* *Miten lakisääteisiä vaatimuksia seurataan ja miten ne huomioidaan toiminnassa?* *Ovatko esimerkiksi henkilötietojen käsittelyn prosessit henkilötietolain edellyttämällä tasolla?* **(ex I 108.0)**	1) Toimintaa koskevat laki- ja sopimusperustaiset vaatimukset on tunnistettu ja täytetty. 2) Kansallisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansallisten käsittelysääntöjen, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti. 3) Kansainvälisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansainvälisten sopimusten, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti.	1) Toimintaa koskevat laki- ja sopimusperustaiset vaatimukset on tunnistettu ja täytetty. 2) Kansallisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansallisten käsittelysääntöjen, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti. 3) Kansainvälisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansainvälisten sopimusten, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti.	1) Toimintaa koskevat laki- ja sopimusperustaiset vaatimukset on tunnistettu ja täytetty. 2) Kansallisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansallisten käsittelysääntöjen, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti. 3) Kansainvälisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansainvälisten sopimusten, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti.	1) Toimintaa koskevat laki- ja sopimusperustaiset vaatimukset on tunnistettu ja täytetty. 2) Kansallisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansallisten käsittelysääntöjen, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti. 3) Kansainvälisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansainvälisten sopimusten, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti.	ISO/IEC 27002 15.1, Kansallisen turvallisuusviranomaisen "Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje", VAHTI 8/2006, http://www.finlex.fi/fi/laki/ajantasa/1999/19990523, http://www.finlex.fi/fi/laki/alkup/2004/20040588, http://www.finlex.fi/fi/laki/alkup/2010/20100885, http://www.finlex.fi/fi/laki/ajantasa/1999/19990621, http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/pdf/ Tietoturvakartoitus_kysymyslista.pdf, http://www.tietosuoja.fi/tulostus/5940.htm, VAHTI 2/2010. Käytännössä kaikkia organisaatioita koskee ainakin henkilötietolain (523/1999) 6 § ja sen asettamat vaatimukset henkilötietojen käsittelyn tarkoituksesta, henkilörekistereistä ja tietojen suojaamisesta koko tiedon elinkaaren ajalta sen kaikissa olomuodoissa. Vrt. turvaluokiteltujen aineistojen käsittelysäännöt tietoaineistoturvallisuuden vaatimuksista.	

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
A 106.0 **Pääkysymys:** **Onko turvallisuuspolitiikan sisältö tiedotettu kaikille työntekijöille, jotta heillä on selvä kuva omista turvallisuuteen liittyvistä velvollisuuksistaan ja vastuistaan?** *Lisäkysymys:* *Onko turvallisuuspolitiikkadokumentaatio jatkuvasti kaikkien saatavilla?* *Kysymyksellä arvioidaan:* *Turvallisuuspolitiikan sisällön viemistä organisaation kaikille tasoille ja politiikan vaatimusten mukaisen toiminnan varmistamista jokapäiväisessä työssä.*	Turvallisuuspolitiikka tai vastaava turvallisuusohjeistus on koulutettu koko henkilöstölle ja se on helposti kerrattavissa esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.	Turvallisuuspolitiikka on koulutettu koko henkilöstölle. Koulutus on dokumentoitu. Koulutus kerrataan esimerkiksi osana muuta koulutusta. Politiikka on helposti kerrattavissa esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla. Organisaation turvallisuuspolitiikka on koulutettu tarvittaville sidosryhmien edustajille.	Organisaation turvallisuuspolitiikka on koulutettu koko henkilöstölle ja se on osa perehdyttämiskoulutusta. Politiikan tunteminen on varmistettu sisällyttämällä sen kertaus osaksi muuta koulutusta. Politiikka on helposti kerrattavissa esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla. Turvallisuuspolitiikan koulutuksen kattavuus on dokumentoitu osallistujien ja sisällön osalta. Turvallisuuspolitiikka on koulutettu myös tarvittaville sidosryhmien edustajille.	Turvallisuuspolitiikka tai vastaava turvallisuusohjeistus on koulutettu koko henkilöstölle ja se on helposti kerrattavissa esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.		

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
A 107.0 **Sisältääkö organisaation turvallisuuspolitiikka vaatimuksen kaikkien työntekijöiden sitoutumisesta jatkuvaan turvallisuustilanteen parantamiseen?** *Kysymyksellä arvioidaan:* *Turvallisuuspolitiikan sisällön kattavuutta.*	Ei vaatimuksia.	Turvallisuuspolitiikka sisältää henkilökohtaisen sitoutumisen merkityksen.	Turvallisuuspolitiikassa kuvataan johdon ja yksittäisten henkilöiden sitoutumisen tarve turvallisuuspolitiikkaan ja korostetaan, että se on jokaista henkilöä koskeva asia, joka toisaalta velvoittaa yksilöä ja toisaalta myös takaa häiriöttömän toiminnan ja työn jatkumisen. Turvallisuus tunnistetaan organisaation laatu- ja kilpailutekijänä.	Turvallisuuspolitiikka ja/ tai -ohjeisto sisältää henkilökohtaisen sitoutumisen merkityksen.		
A 108.0 **Onko turvallisuuspolitiikassa määritetty organisaation keskeiset turvallisuustavoitteet?** *Kysymyksellä arvioidaan:* *Turvallisuuspolitiikan sisällön kattavuutta.*	Keskeiset tavoitteet on kuvattu turvallisuuspolitiikassa tai -ohjeistossa.	Keskeiset turvallisuustavoitteet on kuvattu turvallisuuspolitiikassa.	Organisaation turvallisuuspolitiikassa on kuvattu keskeiset turvallisuuden tavoitteet koskien niitä seikkoja, jotka takaavat organisaation laatu- ja kilpailutekijät.	Keskeiset tavoitteet on kuvattu turvallisuuspolitiikassa tai -ohjeistossa.		

Turvallisuuden vuotuinen toimintaohjelma, osa-alue A200

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
A 201.0 **Onko organisaatiolla kirjoitettu ja dokumentoitu toimintaohjelma turvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?** *Kysymyksellä arvioidaan: Organisaation kykyä tunnistaa turvallisuuden kokonaisuus, oman toiminnan vahvuudet ja sellaiset alueet, joissa tarvitaan parantamista.*	Ei vaatimuksia.	Organisaatiolla on toimintaohjelma, joka kattaa turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisalueet. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.	Organisaatiolla on kaikkia turvallisuuden osa-alueita koskeva toimintaohjelma, joka kattaa toimenpiteet, vastuut, aikataulut ja mitattavat tulokset. Toimintaohjelma käsittelee myös turvallisuuden johtamisen kehitystyön samaan periaatteeseen perustuen.	Organisaatiolla on toimintaohjelma, joka kattaa turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisalueet. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.		
A 202.0 **Onko toimintaohjelmassa eritelty menetelmät, vastuut ja aikataulut tavoitteiden saavuttamiseksi?** *Kysymyksellä arvioidaan:* *Ohjelman yksityiskohtaisuutta.*	Ei vaatimuksia.	Organisaatiolla on turvallisuuden toimintaohjelma, jossa on kuvattu ainakin turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisalueiden osalta vaadittavat tavoitteet, vastuut ja aikataulut. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.	Turvallisuuden vuotuinen toimintaohjelma sisältää organisaation työnkuvauksiin perustuvan suunnitelman turvallisuuden hallinnoitavien osa-alueiden jatkuvaksi parantamiseksi. Vuotuinen suunnitelma sisältää tavoitteet, vastuut ja mitattavat tavoitteet.	Organisaatiolla on turvallisuuden toimintaohjelma, jossa on kuvattu ainakin turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisalueiden osalta vaadittavat tavoitteet, vastuut ja aikataulut. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.		

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
A 203.0 **Tarkistetaanko toiminta-ohjelma säännöllisesti?** *Kysymyksellä arvioidaan:* *Ottaako organisaatio huomioon mahdollisesti muuttuvat tilanteet ja päivitetäänkö vuotuinen toimintaohjelma tarvittaessa*	Ei vaatimuksia.	Ohjelman tarkistaminen on osa jatkuvaa johtamiskäytäntöä.	Organisaatiolla on säännöllinen prosessi (esimerkiksi johtoryhmän tai turvallisuuden johtoryhmän kokouskäytäntö), jossa yhtenä asiakohtana on vastuullisen tahon esittelemä katsaus turvallisuuden toimintaohjelman etenemisestä ja mahdollisista tarpeista kehittää ohjelmaa tavoitteiden, vastuiden tai aikataulun suhteen.	Ohjelman tarkistaminen on osa jatkuvaa johtamiskäytäntöä.		
A 204.0 **Onko organisaatiolla dokumentoitu ohjelma tietoturvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?** **(ex I 102.0)**	Organisaatiolla on tietoturvasuunnitelma, toimintaohje, tai vastaava, ja siihen liittyvät ohjeet tarpeen mukaan. Vaaditaan, että 1) suunnitelma sisältää kuvaukset ainakin hallinnollisesta, fyysisestä ja tietoteknisestä tietoturvallisuudesta; 2) suunnitelma ottaa huomioon mahdollisen toimintaa säätelevän lainsäädännön (ml. tietosuoja); 3) suunnitelmaan liittyvät ohjeet ovat riittäviä suhteessa organisaatioon ja suojattavaan kohteeseen.	Organisaatiolla on tietoturvasuunnitelma, toimintaohje, tai vastaava, ja siihen liittyvät ohjeet tarpeen mukaan. Vaaditaan, että 1) suunnitelma sisältää kuvaukset ainakin hallinnollisesta, fyysisestä ja tietoteknisestä tietoturvallisuudesta; 2) suunnitelma ottaa huomioon mahdollisen toimintaa säätelevän lainsäädännön (ml. tietosuoja); 3) suunnitelmaan liittyvät ohjeet ovat riittäviä suhteessa organisaatioon ja suojattavaan kohteeseen.	Organisaatiolla on tietoturvasuunnitelma, toimintaohje, tai vastaava, ja siihen liittyvät ohjeet tarpeen mukaan. Vaaditaan, että 1) suunnitelma sisältää kuvaukset ainakin hallinnollisesta, fyysisestä ja tietoteknisestä tietoturvallisuudesta; 2) suunnitelma ottaa huomioon mahdollisen toimintaa säätelevän lainsäädännön (ml. tietosuoja); 3) suunnitelmaan liittyvät ohjeet ovat riittäviä suhteessa organisaatioon ja suojattavaan kohteeseen.	Organisaatiolla on tietoturvasuunnitelma, toimintaohje, tai vastaava, ja siihen liittyvät ohjeet tarpeen mukaan. Suositellaan, että 1) suunnitelma sisältää kuvaukset ainakin hallinnollisesta, fyysisestä ja tietoteknisestä tietoturvallisuudesta; 2) suunnitelma ottaa huomioon mahdollisen toimintaa säätelevän lainsäädännön (ml. tietosuoja); 3) suunnitelmaan liittyvät ohjeet ovat riittäviä suhteessa organisaatioon ja suojattavaan kohteeseen.	PCI DSS 12.2, COBIT 4.1 PO, COBIT 4.1 DS5, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	

Turvallisuuden tavoitteiden määrittely, osa-alue A300

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 301.0 **Onko organisaation liiketoiminta ja sitä tukeva turvallisuuspolitiikka ja -ohjelma perusteena turvallisuustyön tavoitteita asetettaessa?** *Kysymyksellä arvioidaan:* *Muodostavatko politiikka, ohjelma ja tavoitteiden asettaminen kokonaisuuden.*	Turvallisuustyön tavoitteet on asetettu politiikan mukaisesti, selkeästi ja mitattavasti.	Turvallisuustyön tavoitteet on asetettu politiikan mukaisesti, selkeästi ja mitattavasti.	Toimintaohjelman tavoitteissa on kattavasti huomioitu turvallisuuspolitiikan kattamat alueet.	Turvallisuustyön tavoitteet on asetettu politiikan mukaisesti, selkeästi ja mitattavasti.		
A 302.0 **Onko organisaatio asettanut turvallisuustavoitteet organisaation eri hierarkiatasoille ja/tai toiminnoille?** *Kysymyksellä arvioidaan:* *Tavoitteiden konkreettista asettamista ja eri osatavoitteiden merkityksellisyyden ymmärtämistä organisaation eri osien ja hierarkiatasojen osalta. Tavoitteiden dokumentoinnilla varmistetaan se, että vaatimustasoa voidaan kehittää jatkuvan parantamisen periaatteella.*	Ei vaatimuksia.	Organisaatiolla on selkeät ja dokumentoidut turvallisuustavoitteet, jotka kattavat ohjelman mukaiset turvallisuuden osa-alueet ja eriteltynä organisaation tarvittavat osat ja tasot.	Organisaatio on määrittänyt selkeästi mitattavat tavoitteet organisaation kokonaisuudelle ja osille sekä tasoille toiminnan vaatimusten mukaisesti. Tavoitteet on dokumentoitu ja ne ovat osa organisaation johtamisjärjestelmää.	Organisaatiolla on selkeät ja dokumentoidut turvallisuustavoitteet, jotka kattavat ohjelman mukaiset turvallisuuden osa-alueet ja eriteltynä organisaation toiminnassa tarvittavat osat ja tasot.		

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 303.0 **Onko tavoitteet asetettu siten, että niiden saavuttaminen on mitattavissa?** *Kysymyksellä arvioidaan:* *Tavoitteiden konkreettista ja realistista asettamista sekä laadullisten mittareiden sisällyttämistä tavoitteisiin.*	Turvallisuustoiminnan tavoitteet on asetettu konkreettisesti ja mitattavasti.	Turvallisuustoiminnan tavoitteet on asetettu konkreettisesti ja mitattavasti.	Turvallisuustyön tavoitteet on asetettu siten, että eri osille ja organisaation hierarkiatasoille on niitä koskevat mitattavat tavoitteet. Mitattavuus on esimerkiksi kuvattu annettavan koulutuksen kattavuutena, turvallisuuspoikkeamien määrän vähenemisenä tai vastaavana selkeänä tavoitteena.	Turvallisuustoiminnan tavoitteet on asetettu konkreettisesti ja mitattavasti.		
A 304.0 **Onko tavoitteiden saavuttamiselle asetettu aikataulu?** *Kysymyksellä arvioidaan:* *Tavoitteiden konkreettista ja realistista asettamista.*	Tavoitteiden saavuttamiselle on asetettu aikataulu.	Tavoitteiden saavuttamiselle on asetettu aikataulu.	Tavoitteiden saavuttamiselle on asetettu aikataulu.	Tavoitteiden saavuttamiselle on asetettu aikataulu.		

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 305.0 **Onko seuraavat tekijät otettu huomioon tavoitteiden asettamisen yhteydessä:** **a. tunnistetut riskit** **b. organisaation oman toiminnan ja/tai liiketoiminnan vaatimukset** **c. tekniset vaatimukset ja mahdollisuudet** **d. taloudelliset vaatimukset** **e. muiden intressiryhmien vaatimukset (esim. asiakkaat, viranomaiset)** **f. lainsäädännön ja/tai muiden ohjeistojen sekä sopimusten vaatimukset** *Kysymyksellä arvioidaan:* *Onko tavoitteita asetettaessa tunnistettu mm. edellä kuvatut vaatimukset, mahdollisuudet ja rajoittavat tekijät*	Ei vaatimuksia	Asetettavat tavoitteet sisältävät tarvittavilta osin kuvauksen liittymisestä tunnistettuihin riskeihin, teknisiin ja taloudellisiin vaatimuksiin sekä mahdollisuuksiin, organisaation oman toiminnan ja/tai liiketoiminnan vaatimuksiin, muiden intressiryhmien vaatimuksiin ja/tai lainsäädännön/muiden ohjeistojen vaatimuksiin huomioiden tekijät a), b), c), e), f).	Tavoitteiden asettamisen yhteydessä on huomioitu tekijät a), b), c), e), f).	Asetettavat tavoitteet sisältävät tarvittavilta osin kuvauksen liittymisestä tunnistettuihin riskeihin, teknisiin ja taloudellisiin vaatimuksiin sekä mahdollisuuksiin, organisaation oman toiminnan ja/tai liiketoiminnan vaatimuksiin, muiden intressiryhmien vaatimuksiin ja/tai lainsäädännön/muiden ohjeistojen vaatimuksiin huomioiden tekijät a), b), c), d), e), f).		

Kysymys	Viranomais-vaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 306.0 **Onko koko suojattavan tiedon käsittely-ympäristö suojattu organisaation tietoturvaperiaatteiden ja tiedon merkityksen/luokituksen mukaisesti?** *Lisäkysymykset:* *Kattavatko suojaukset kaikki loogisesti kytketyt tietoverkot ja -järjestelmät, joissa suojattavaa tietoa käsitellään? Kattavatko suojaukset myös sellaiset tietoverkot ja -järjestelmät, joihin tietoa viedään tai joista tietoa tuodaan ilmaraon yli esimerkiksi USB-muisteilla?*	Kaikki suojaustason IV tiedon käsittely-ympäristöt on suojattu vähintään viranomaisvaatimusten mukaisesti.	Kaikki suojaustason III tiedon käsittely-ympäristöt on suojattu vähintään viranomaisvaatimusten mukaisesti.	Kaikki suojaustason II tiedon käsittely-ympäristöt on suojattu vähintään viranomaisvaatimusten mukaisesti.	Kaikki suojattavaa tietoa käsittelevät tietoverkot ja -järjestelmät ovat organisaation tietoturvaperiaatteiden mukaisesti suojattuja.	Kansallisen turvallisuusviranomaisen ”Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”, VAHTI 2/2010, VAHTI 3/2010 Vaatimuksen päätavoitteena on varmistua siitä, että koko suojattavan tiedon käsittely-ympäristö tulee suojatuksi asianmukaisesti, ja että esimerkiksi pääjärjestelmään kytketyn apujärjestelmän kautta ei ole luvatonta pääsyä suojattavaan tietoon. Oheistavoitteena on varmistua siitä, että suojattavaan tietoon ei ole luvatonta pääsyä esimerkiksi heikosti suojatun tilapäis-, kokeilu-, tai luvattomasti asennetun verkon kautta. Erityisesti turvaluokitellun aineiston tapauksessa tulee koko suojattavan tiedon käsittely-ympäristön olla suojattu ja hyväksytetty käsiteltävän tiedon turvaluokan mukaisesti. Vaatimus kattaa mm. kaikki verkkoon/järjestelmään kytketyt muut verkot/järjestelmät sekä kaikki käsittely-ympäristöt, joihin turvaluokiteltua tietoa viedään tai josta sitä tuodaan. (vrt. I 401.0).	

Riskien tunnistus, arviointi ja kontrollit, osa-alue A400

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 401.0 **Onko organisaatiolla menetelmät tunnistaa ja arvioida turvallisuus-riskit?** *Kysymyksellä arvioidaan:* *Priorisoiko organisaatio turvallisuustyönsä arvioimalla riskit.*	Organisaatio arvioi turvallisuuden kokonaisuuteen liittyvät riskit ja riskienarviointi on turvallisuustyön tärkeysjärjestyksen peruste. Menettelytapa on säännöllinen ja tulokset dokumentoidaan.	Organisaatio arvioi turvallisuuden kokonaisuuteen liittyvät riskit ja riskienarviointi on turvallisuustyön tärkeysjärjestyksen peruste. Menettelytapa on säännöllinen ja tulokset dokumentoidaan.	Riskienarviointi on jatkuva prosessi, joka sisältää riskin tunnistamisen, todennäköisyyden ja vaikuttavuuden arvioinnin, tarvittavat toimenpiteet, vastuut ja aikataulut. Riskienarvioinnit toteuttavat organisaation parhaat asiantuntijat. Riskienarviointi on perustana turvallisuustyön priorisoinnille.	Organisaatio arvioi turvallisuuden kokonaisuuteen liittyvät riskit ja riskienarviointi on turvallisuustyön tärkeysjärjestyksen peruste. Menettelytapa on säännöllinen ja tulokset dokumentoidaan.		
A 401.1 **Pääkysymys:** **Onko toiminnalle tärkeät suojattavat kohteet (toiminnot, tiedot, järjestelmät, prosessit) tunnistettu?** *Lisäkysymykset:* *Mitä uhkia niihin kohdistuu? Onko suojattaville kohteille määritetty vastuuhenkilöt?* **(ex I 103.0)** **Katso lisätietoja liitteestä 1 (A401.1)**	1) Suojattavat kohteet (assets) on tunnistettu. 2) Suojattaviin kohteisiin kohdistuvat uhat on tunnistettu. 3) Suojattaville kohteille on nimetty omistaja/vastuuhenkilö. 4) Suojattavien kohteiden suojausmenetelmät on suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin (vrt. A 401.2).	1) Suojattavat kohteet (assets) on tunnistettu. 2) Suojattaviin kohteisiin kohdistuvat uhat on tunnistettu. 3) Suojattaville kohteille on nimetty omistaja/vastuuhenkilö. 4) Suojattavien kohteiden suojausmenetelmät on suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin (vrt. A 401.2).	1) Suojattavat kohteet (assets) on tunnistettu. 2) Suojattaviin kohteisiin kohdistuvat uhat on tunnistettu. 3) Suojattaville kohteille on nimetty omistaja/vastuuhenkilö. 4) Suojattavien kohteiden suojausmenetelmät on suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin (vrt. A 401.2).	1) Suojattavat kohteet (assets) on tunnistettu. 2) Suojattaviin kohteisiin kohdistuvat uhat on tunnistettu. 3) Suojattaville kohteille on nimetty omistaja/vastuuhenkilö. 4) Suojattavien kohteiden suojausmenetelmät on suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin (vrt. A 401.2).	ISO/IEC 27002 7.1, COBIT 4.1 PO9, VAHTI 8/2006, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 401.2 **Miten suojattaviin kohteisiin kohdistuvia riskejä arvioidaan?** **(ex I104.0)** **Katso lisätietoja liitteestä 1 (A 401.2)**	1) Suojattaviin tietoihin kohdistuvia riskejä hallitaan prosessina jollain järjestelmällisellä menetelmällä. 2) Em. prosessissa on määritelty tunnetut turvallisuusriskit ja turvatoimet niiden vähentämiseksi hyväksyttävälle tasolle. 3) Turvatoimien tehokkuutta arvioidaan vähintään vuosittain ja lisäksi merkittävien muutosten yhteydessä. 4) Turvallisuusriskien hallinta on erottamaton osa suojattavan kohteen viestintä- ja tietojärjestelmien määrittelyä, kehittämistä, käyttöä ja ylläpitoa. 5) Johto ja tiedon omistajat ovat hyväksyneet valitut suojausmenetelmät ja jäännösriskit.	1) Suojattaviin tietoihin kohdistuvia riskejä hallitaan prosessina jollain järjestelmällisellä menetelmällä. 2) Em. prosessissa on määritelty tunnetut turvallisuusriskit ja turvatoimet niiden vähentämiseksi hyväksyttävälle tasolle. 3) Turvatoimien tehokkuutta arvioidaan vähintään vuosittain ja lisäksi merkittävien muutosten yhteydessä. 4) Turvallisuusriskien hallinta on erottamaton osa suojattavan kohteen viestintä- ja tietojärjestelmien määrittelyä, kehittämistä, käyttöä ja ylläpitoa. 5) Johto ja tiedon omistajat ovat hyväksyneet valitut suojausmenetelmät ja jäännösriskit.	1) Suojattaviin tietoihin kohdistuvia riskejä hallitaan prosessina jollain järjestelmällisellä menetelmällä. 2) Em. prosessissa on määritelty tunnetut turvallisuusriskit ja turvatoimet niiden vähentämiseksi hyväksyttävälle tasolle. 3) Turvatoimien tehokkuutta arvioidaan vähintään vuosittain ja lisäksi merkittävien muutosten yhteydessä. 4) Turvallisuusriskien hallinta on erottamaton osa suojattavan kohteen viestintä- ja tietojärjestelmien määrittelyä, kehittämistä, käyttöä ja ylläpitoa. 5) Johto ja tiedon omistajat ovat hyväksyneet valitut suojausmenetelmät ja jäännösriskit.	1) Suojattaviin kohteisiin (vrt. A 401.1) kohdistuvia riskejä arvioidaan jollain järjestelmällisellä menetelmällä. 2) Arviointi tapahtuu vähintään vuosittain ja lisäksi merkittävien muutosten yhteydessä. 3) Valitut suojausmenetelmät on asianmukaisesti suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin. 4) Johto on hyväksynyt valitut suojausmenetelmät ja jäännösriskit	ISO/IEC 27001 luku 4, ISO/IEC 27002 7.1, COBIT 4.1 PO9, Kansallisen turvallisuusviranomaisen "Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje", VAHTI 8/2006, VAHTI 2/2010:n liite 5 (TTT), EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 5. artikla, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 402.0 **Kattavatko nämä menetelmät normaalin toiminnan, erityistilanteet, onnettomuudet ja hätätapaukset? Otetaanko aliurakoitsijat ja palveluntarjoajat huomioon?** *Kysymyksellä arvioidaan: Riskienarvioinnin kattavuutta.*	Riskienarviointi kattaa ainakin turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Asiat on huomioitu tarvittavien sidosryhmien osalta.	Riskienarviointi kattaa ainakin turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Asiat on huomioitu myös normaalitoiminnasta poikkeavien tilanteiden ja tarvittavien sidosryhmien osalta.	Arvioitavat riskit sisältävät laaja-alaisesti koko organisaation toimintakentän ja mahdolliset erityistilanteet. Asiat on huomioitu normaalitoiminnasta poikkeavien tilanteiden ja tarvittavien sidosryhmien osalta.	Riskienarviointi kattaa ainakin turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Asiat on huomioitu tarvittavien sidosryhmien osalta.		
A 403.0 **Dokumentoidaanko riskienarviointien tulokset ja päivitetäänkö ne säännöllisesti?** *Kysymyksellä arvioidaan:* *Onko organisaatiossa todennettava järjestelmä riskien arvioinneista tallenteineen.*	Ei vaatimuksia.	Riskienarviointi tehdään vähintään vuosittain ja organisaation tilanteen muuttuessa siten, että on tarkoituksen mukaista päivittää tehty arvio. Riskien arvioinnit dokumentoidaan siten, että ne ovat todennettavissa.	Turvallisuusriskien arviointi on määritetty osaksi organisaation johtamisprosessia ja se taltioidaan osana organisaation dokumentointijärjestelmää.	Riskienarviointi tehdään vähintään vuosittain ja organisaation tilanteen muuttuessa siten, että on tarkoituksen mukaista päivittää tehty arvio. Riskien arvioinnit dokumentoidaan siten, että ne ovat todennettavissa.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 404.0 **Otetaanko riskienarviointien havainnot huomioon turvallisuustoiminnan tavoitteita asetettaessa?** *Kysymyksellä arvioidaan:* *Onko riskienarviointi osa laadukasta turvallisuustoimintaa, joka tähtää jatkuvaan toiminnan tason parantamiseen.*	Riskienarvioinnin tulokset on huomioitu turvallisuustoiminnan tavoitteita asetettaessa.	Riskienarvioinnin tulokset on huomioitu turvallisuustoiminnan tavoitteita asetettaessa.	Riskienarviointityökalu sisältää toimenpiteet, joita riskien hallitseminen edellyttää sekä vastuut ja aikataulut. Näitä hyödynnetään, kun organisaation turvallisuustoiminnan tavoitteita asetetaan. Riskienarviointiprosessi on kuvattu.	Riskienarvioinnin tulokset on huomioitu turvallisuustoiminnan tavoitteita asetettaessa.		
A 405.0 **Voidaanko riskienarvioinnin tulosten perusteella priorisoida riskit?** *Kysymyksellä arvioidaan:* *Saadaanko tuloksena perusteet riskienhallinnan toimenpiteiden valinnalle, tärkeysjärjestykselle ja kiireellisyydelle.*	Riskienarvioinnin tuloksena riskit luokitellaan tärkeysjärjestykseen.	Riskienarvioinnin tuloksena riskit luokitellaan tärkeysjärjestykseen.	Riskienarviointi perustuu riskin todennäköisyyden ja vaikuttavuuden arviointiin siten, että tuloksena on riskiluokitus, jota voidaan käyttää määritettäessä tarve poistaa riski, parantaa riskin hallitsemista tai pienentää tunnistetun riskin vaikutusta.	Riskienarvioinnin tuloksena riskit luokitellaan tärkeysjärjestykseen.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 406.0 **Antavatko riskienarvioinnit perusteet turvallisuuskoulutuksen vaatimuksille?** *Kysymyksellä arvioidaan:* *Onko riskienarviointi myös työkalu, joka tukee koulutuksen suunnittelua yhtenä keinona pienentää riskin vaikutusta.*	Riskienarviointien tulokset vaikuttavat suunnitellun koulutuksen sisältöön. Koulutus tunnistetaan yhtenä keinona vaikuttaa riskien hallintaan.	Riskienarviointien tulokset vaikuttavat suunnitellun koulutuksen sisältöön. Koulutus tunnistetaan yhtenä keinona vaikuttaa riskien hallintaan.	Riskienarviointien tulokset vaikuttavat suunnitellun koulutuksen sisältöön. Koulutus tunnistetaan yhtenä keinona vaikuttaa riskien hallintaan.	Riskienarviointien tulokset vaikuttavat suunnitellun koulutuksen sisältöön. Koulutus tunnistetaan yhtenä keinona vaikuttaa riskien hallintaan.		
A 407.0 **Onko organisaatiolla menetelmät valvoa turvallisuuden riskienarviointien perusteella tehtyjen toimenpiteiden toteuttamista ja tehokkuutta?** *Kysymyksellä arvioidaan:* *Toteutuuko riskienarvioinnin perusteella valittujen toimenpiteiden haluttu vaikutus.*	Ei vaatimuksia.	Turvallisuusjohtamisen prosessi sisältää riskienarvioinnin perusteella tehtyjen toimenpiteiden toteuttamisen ja tehokkuuden arvioinnin.	Turvallisuusjohtamisen syklissä käsitellään riskienarvioinnin perusteella laadittujen toimenpiteiden oikea laatu ja laajuus sekä vaikuttavuus verrattuna haluttuun tulokseen.	Turvallisuusjohtamisen prosessi sisältää riskienarvioinnin perusteella tehtyjen toimenpiteiden toteuttamisen ja tehokkuuden arvioinnin.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 408.0 **Pääkysymys:** **Miten organisaation tietoturvallisuutta arvioidaan?** *Lisäkysymys:* *Kehitetäänkö toimintaa havaintojen perusteella?* **(ex I 105.0)**	Suojattavan kohteen tietoturvallisuuden tasoa seurataan, arvioidaan ja kehitetään jatkuvasti.	1) Suojattavan kohteen tietoturvallisuuden arviointiin ja mittaamiseen on käytössä järjestelmällinen menetelmä. 2) Suojattavan kohteen turvallisuudelle suoritetaan riippumaton katselmus suunnitelluin väliajoin, ja lisäksi aina, kun turvallisuuden toteuttamisessa tapahtuu merkittäviä muutoksia.	1) Suojattavan kohteen tietoturvallisuuden arviointiin ja mittaamiseen on käytössä järjestelmällinen menetelmä. 2) Suojattavan kohteen turvallisuudelle suoritetaan riippumaton katselmus suunnitelluin väliajoin, ja lisäksi aina, kun turvallisuuden toteuttamisessa tapahtuu merkittäviä muutoksia.	Organisaation tietoturvallisuuden toimintamallia ja tietoturvallisuuden käytännön toteuttamista seurataan, arvioidaan ja kehitetään jatkuvasti.	ISO/IEC 27002 6.1.8, ISO/IEC 27004, VAHTI 8/2006, Vaatimusten täyttyminen voidaan todentaa pyytämällä esimerkkejä siitä, miten tietoturvallisuutta on seurattu, arvioitu ja kehitetty. Erityisesti suojaustasolla III olevien vaatimusten täyttyminen voidaan todentaa pyytämällä kuvaamaan käytetty järjestelmällinen menetelmä ja näyttämään sen antamia tuloksia. Suojaustasolla III voidaan pyytää nähtäväksi myös ulkopuolisen tarkastajan tuottama raportti.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 409.0 **Miten tietoturvallisuudesta on huolehdittu alihankinta-, palveluhankinta- ja muussa vastaavassa yhteistyössä?** **(ex I 106.0)** *Huom!* *Osaa kansainvälisistä aineistoista ei saa luovuttaa alihankkijoille ja vastaaville ilman viranomaisen etukäteissuostumusta edes suojaustasolla IV. Tämä varmistettava tapauskohtaisesti.*	1) Tunnistetuista turvallisuusvaatimuksista huolehditaan ennen kuin asiakkaille annetaan pääsy suojattavaan tietoon tai kohteisiin. 2) Suojaustason IV aineistoa luovutetaan alihankkijalle tai vastaavalle harkiten vain tarpeellisuusperiaatteen (need-to-know) mukaisesti. Aineiston saaja ohjeistetaan siitä, mitä ko. suojaustason aineiston käsittely edellyttää. 3) Organisaation luokiteltua tietoa käsitteleviin palveluihin on varattu oikeus tietoturvatarkastuksiin. 4) Ulkopuolisiin tahoihin (esim. ulkoistuskumppaneihin) liittyvät riskit on tunnistettu ja asianmukaiset turvamekanismit toteutettu. 5) Palveluihin on määritelty palvelun laatutaso (SLA). 6) Ulkoistettujen tietojenkäsittelypalveluiden toimittajien kanssa on sovittu menettelytavat tietoturvapoikkeamien varalle.	Suojaustason III aineistoa ei luovuteta alihankkijalle tai vastaavalle ilman viranomaisen etukäteissuostumusta.	Suojaustason II aineistoa ei luovuteta alihankkijalle tai vastaavalle ilman viranomaisen etukäteissuostumusta.	1) Tarjouspyyntöihin on liitetty tietoturvavaatimukset. 2) Ulkopuolisiin tahoihin (esim. ulkoistuskumppaneihin) liittyvät riskit on tunnistettu ja asianmukaiset turvamekanismit toteutettu. 3) Palveluihin on määritelty palvelun laatutaso (SLA). 4) Ulkoistettujen tietojenkäsittelypalveluiden toimittajien kanssa on sovittu menettelytavat tietoturvapoikkeamien varalle.	ISO/IEC 27002 6.2.1, ISO/IEC 27002 6.2.2, ISO/IEC 27002 10.6.1, ISO/IEC 27002 12.1.1, COBIT 4.1 AI5, COBIT 4.1 DS1, COBIT 4.1 DS2, Kansallisen turvallisuusviranomaisen “Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”, VAHTI 8/2006, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 11. artikla, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 liite V Huolehdittava myös salassapitositoumukset (P 407.0). Alihankkijoilta ja vastaavilta voidaan tapauskohtaisesti vaatia myös säännölliset raportit tietoturvallisuuden nykytilasta (esim. kuukauden havainnot, hyökkäysyritykset, poikkeukset, jne.).	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 410.0 **Miten organisaatiossa toimitaan tietoturvapoikkeamatilanteissa?** *Lisäkysymys:* *Miten tietoturvapoikkeamien hallinta on käytännössä toteutettu?* **(ex I 107.0)**	Tietoturvapoikkeamien hallinta on 1) suunniteltu, 2) ohjeistettu/koulutettu, 3) dokumentoitu käyttöympäristöön nähden riittävällä tasolla, ja erityisesti 4) viestintäkäytännöt ja -vastuut on sovittu.	Perustason vaatimusten lisäksi: 1) Tietoturvapoikkeamien hallinta on harjoiteltu. 2) Tapahtuneesta tai epäillystä tietoturvapoikkeamasta ilmoitetaan välittömästi turvallisuusviranomaiselle tai viranomaisen erikseen hyväksymälle taholle.	Perustason vaatimusten lisäksi: 1) Tietoturvapoikkeamien hallinta on harjoiteltu. 2) Tapahtuneesta tai epäillystä tietoturvapoikkeamasta ilmoitetaan välittömästi turvallisuusviranomaiselle tai viranomaisen erikseen hyväksymälle taholle.	Tietoturvapoikkeamien hallinta on 1) suunniteltu, 2) ohjeistettu/ koulutettu, 3) dokumentoitu käyttöympäristöön nähden riittävällä tasolla, ja erityisesti 4) viestintäkäytännöt ja -vastuut on sovittu.	ISO/IEC 27002 13.2.1, PCI DSS 12.9, COBIT 4.1 DS8, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 13. artikla, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf - Vrt. I 408.0. Taho, jolle poikkeamat raportoidaan, riippuu tiedon omistajasta. Taho voi olla esimerkiksi NCSA-FI, CERT-FI, puolustusvoimien taho tai Euroopan Unionin neuvoston CERT-toimija.	

Turvallisuusorganisaatio ja vastuut, osa-alue A500

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 501.0 **Ovatko turvallisuustyön vastuut määritetty? Kattavatko määrittelyt organisaation eri tasot?** *Kysymyksellä arvioidaan:* *Ovatko turvallisuustyön vastuut asetetut siten, että kaikki toiminnot ja organisaation tasot on katettu.*	Turvallisuusorganisaatio kattaa ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Vastuulliset henkilöt on nimetty.	Turvallisuusorganisaatio kattaa turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Vastuulliset henkilöt on nimetty ja koulutettu ja tehtävä on osa henkilön toimenkuvausta.	Turvallisuustyön vastuut on määritetty turvallisuusjohtamisen ja turvallisuuspolitiikan mukaisten osa-alueiden sekä organisaation toimintojen ja tasojen suhteen. Vastuulliset henkilöt on nimetty ja koulutettu ja tehtävä on osa henkilön toimenkuvausta.	Turvallisuusorganisaatio kattaa ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Vastuulliset henkilöt on nimetty.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 501.1 **Onko organisaation tietoturvallisuudella johdon tuki? Miten tuki käytännössä näkyy organisaation toiminnassa?** **(ex I 101.0)**	Organisaation tietoturvallisuudella on johdon tuki. Vaaditaan vähintään, että 1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.); 2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet; 3) tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon; 4) tietoturvaperiaatteet ja -käytänteet katselmoidaan vuosittain ja aina, kun merkittäviä muutoksia tapahtuu; 5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti; 6) tietoturvallisuudelle on varattu toimintavaatimuksiin nähden riittävät resurssit.	Organisaation tietoturvallisuudella on johdon tuki. Vaaditaan vähintään, että 1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.); 2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet; 3) tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon; 4) tietoturvaperiaatteet ja -käytänteet katselmoidaan vuosittain ja aina, kun merkittäviä muutoksia tapahtuu; 5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti; 6) tietoturvallisuudelle on varattu toimintavaatimuksiin nähden riittävät resurssit.	Organisaation tietoturvallisuudella on johdon tuki. Vaaditaan vähintään, että 1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon/ järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.); 2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet; 3) tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon; 4) tietoturvaperiaatteet ja -käytänteet katselmoidaan vuosittain ja aina, kun merkittäviä muutoksia tapahtuu; 5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti; 6) tietoturvallisuudelle on varattu toimintavaatimuksiin nähden riittävät resurssit.	Organisaation tietoturvallisuudella on johdon tuki. Suositellaan vähintään, että 1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.); 2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet; 3) tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon; 4) tietoturvaperiaatteet ja -käytänteet katselmoidaan vuosittain ja aina, kun merkittäviä muutoksia tapahtuu; 5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti; 6) tietoturvallisuudelle on varattu toimintavaatimuksiin nähden riittävät resurssit.	ISO/IEC 27002 5.1.1, ISO/IEC 27002 5.1.2, ISO/IEC 27002 6.1.1, ISO/IEC 27002 6.1.3, ISO/IEC 27002 7.1, ISO/IEC 27002 8.2.1, PCI DSS 12.1, PCI DSS 12.3.1, PCI DSS 12.4, PCI DSS 12.5, COBIT 4.1 PO4, COBIT 4.1 PO6, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf Suositellaan, että järjestelmille on määritetty ylläpitovastuun lisäksi myös omistajat. Suositellaan, että tekninen ylläpito ei ole sama kuin omistaja.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 502.0 **Ovatko roolit, vastuut ja toimeenpanovalta tiedotettu organisaatiossa ja niille ulkopuolisille tahoille, joiden on tunnettava turvallisuusorganisaation rakenne?** *Kysymyksellä arvioidaan:* *Tietääkö organisaatio ne henkilöt, jotka vastaavat eri turvallisuuden osa-alueista ja jotka samalla pystyvät tukemaan eri ongelmatilanteissa.*	Turvallisuusorganisaatio on koulutettu henkilöstölle ja tieto on saatavissa päivitettynä esimerkiksi tietojärjestelmän tai lmoitustaulun avulla.	Turvallisuusorganisaatio on koulutettu henkilöstölle ja tieto on saatavissa päivitettynä esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.	Turvallisuusorganisaation rakenne ja vastuut on koulutettu ja tiedot on jatkuvasti saatavissa päivitettyinä koko organisaatiossa mukaan lukien tarvittavat sidosryhmät.	Turvallisuusorganisaatio on koulutettu henkilöstölle ja tieto on saatavissa päivitettynä esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.		
A 503.0 **Onko turvallisuustyölle suunnattu riittävästi resursseja työn toteuttamiseksi, kontrolloimiseksi sekä parantamiseksi?** **Resurssien tulisi kattaa:** **– henkilöstö** **– erityisosaaminen** **– teknologiset resurssit** **– taloudelliset resurssit** *Kysymyksellä arvioidaan:* *Onko turvallisuustyöllä realistiset onnistumisen mahdollisuudet.*	Ei vaatimuksia.	Turvallisuustyöstä vastaa koulutettu ja kokenut henkilöstö, jonka osaamistasoa ylläpidetään suunnitellusti ja jatkuvasti. Turvallisuusjohtaminen kattaa mm. henkilöstön, teknologian ja taloudellisten resurssien riittävyyden arvioinnin. Osatekijät on sisällytetty osaksi turvallisuustyön jatkuvaa parantamista.	Turvallisuustyöstä vastaa koulutettu ja kokenut henkilöstö, jonka osaamistasoa ylläpidetään suunnitellusti ja jatkuvasti. Osaamisen jatkuvuus on turvattu hyvällä henkilöstösuunnittelulla. Laadukasta turvallisuusteknologiaa käytetään osana turvallisuuden hallintaa ja se on integroitu tarkoituksenmukaisesti.	Turvallisuusjohtaminen kattaa mm. henkilöstön, teknologian ja taloudellisten resurssien riittävyyden arvioinnin.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 504.0 **Onko organisaation ylin johto määrittänyt henkilön, joka on vastuussa turvallisuustoiminnan kehittämisestä ja johtamisesta sekä siitä, että turvallisuustyö kattaa kaikkien organisaation tasojen tarpeet?** *Kysymyksellä arvioidaan:* *Onko turvallisuudesta vastaavalla henkilöllä johdon tuki ja aseman tuoma valtuus ja onko asetettu tehtävä riittävän laaja-alainen kokonaisuuden hallitsemiseksi. Tehtävä voi olla osa henkilön muuta toimenkuvaa.*	Organisaatiolla on turvallisuudesta vastaava henkilö, jolla on riittävät mahdollisuudet johtaa turvallisuustoimintaa ja hallita ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Tehtäväkenttä voi olla myös jaettu, mikäli se on organisaation toiminnan kannalta tarkoituksenmukaista.	Organisaatiolla on turvallisuudesta keskitetysti vastaava henkilö, jolla on riittävät mahdollisuudet johtaa ja koordinoida turvallisuustoimintaa ja hallita ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet.	Organisaatiossa on nimetty turvallisuusvastaava, jolla on kokonaisvaltainen vastuu turvallisuuden kehittämisestä ja johtamisesta osana organisaation johtamista. Tehtävä kattaa turvallisuuden osa-alueet, organisaation osat ja tasot.	Organisaatiolla on turvallisuudesta vastaava henkilö, jolla on riittävät mahdollisuudet johtaa turvallisuustoimintaa ja hallita ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Tehtäväkenttä voi olla myös jaettu, mikäli se on organisaation toiminnan kannalta tarkoituksenmukaista.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 505.0 **Onko nimetyllä turvallisuustyöstä vastaavalla henkilöllä vastuu ja valtuus sen varmistamiseksi, että turvallisuuden johtamisjärjestelmä on muodostettu niiden vaatimusten mukaisesti, joita tavoitteissa on asetettu?** *Kysymyksellä arvioidaan:* *Onko turvallisuustoimintaa johtavalla henkilöllä mahdollisuus vaikuttaa johtamisjärjestelmään siten, että turvallisuustavoitteiden saavuttaminen on mahdollista.*	Turvallisuudesta vastaava henkilö on organisaatiossa sellaisessa asemassa, että hänellä on mahdollisuus vaikuttaa turvallisuuden toteuttamiseen. Vaikuttamismahdollisuus on yksilöitävä organisaation prosessikuvauksessa ja/tai henkilön tehtävänkuvauksessa.	Turvallisuudesta vastaava henkilö on organisaatiossa sellaisella tasolla, että hänellä on mahdollisuus vaikuttaa turvallisuuden johtamisjärjestelmän kokonaisuuteen. Vaikuttamismahdollisuus on yksilöitävä organisaation prosessikuvauksessa ja/tai henkilön tehtävänkuvauksessa.	Turvallisuudesta vastaava henkilö on organisaatiossa sellaisella tasolla, että hänellä on mahdollisuus vaikuttaa turvallisuuden johtamisjärjestelmään osana organisaation normaalia johtamista. Vaikuttamismahdollisuus on yksilöitävä organisaation prosessikuvauksessa ja/tai henkilön tehtävänkuvauksessa.	Turvallisuudesta vastaava henkilö on organisaatiossa sellaisessa asemassa, että hänellä on mahdollisuus vaikuttaa turvallisuuden toteuttamiseen. Vaikuttamismahdollisuus on yksilöitävä organisaation prosessikuvauksessa ja/tai henkilön tehtävänkuvauksessa.		
A 506.0 **Onko organisaation johto sitoutunut turvallisuustavoitteisiin ja niiden saavuttamiseen sekä turvallisuuden jatkuvaan parantamiseen?** *Kysymyksellä arvioidaan:* *Toteutuuko turvallisuustyöhön sitoutuminen organisaation kaikilla tasoilla. Organisaation johdon esimerkin vaikutus on ratkaiseva tekijä.*	Ei vaatimuksia.	Organisaation johto on mukana turvallisuustyön tavoitteiden asettamisessa, menetelmien valinnassa ja tavoitteiden seurannan arvioinnissa. Malli on yksilöitävä organisaation prosessikuvauksessa.	Organisaation johto osoittaa sitoutumistaan konkreettisesti turvallisuusvaatimuksia noudattamalla ja kehitystyöhön osallistumalla. Johto tuo esille turvallisuuden tavoitteita, menetelmiä ja saavutuksia osana muuta johtamistoimintaa.	Organisaation johto on mukana turvallisuustyön tavoitteiden asettamisessa, menetelmien valinnassa ja tavoitteiden seurannan arvioinnissa.		

Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet, osa-alue A600

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 601.0 **Onko organisaatiolla jatkuvuudenhallintamenettely?** *Kysymyksellä arvioidaan:* *Onko organisaatio tunnistanut toimintaa uhkaavat häiriöt ja varautunut niistä sellaisiin, jotka voivat hidastaa tai estää päätavoitteiden saavuttamista.*	Ei vaatimuksia.	Organisaation toiminnan johtamisessa on otettu huomioon varautuminen liiketoimintaa vaikeuttaviin tai katkaiseviin häiriötilanteisiin ja laadittu niitä koskevat valmius- ja toipumissuunnitelmat organisaation keskeisimpiin toimintoihin. Resurssitarve on määritetty ja niiden saatavuus suunniteltu. Jatkuvuuden hallinnan toteutumista seurataan ja arvioidaan.	Organisaation toiminnan johtamisessa on otettu huomioon varautuminen liiketoimintaa vaikeuttaviin tai katkaiseviin häiriötilanteisiin ja laadittu niitä koskevat valmius- ja toipumissuunnitelmat. Resurssit on määritetty ja varattu, menetelmät on koulutettu ja testattu. Jatkuvuuden hallinnan toteutumista seurataan ja arvioidaan. Jatkuvuudenhallinta on viety läpi koko organisaation kattaen kaikki organisaation prosessit. Menettelytapa on dokumentoitu. Keskeytysriskit on suunnitellusti vakuutettu.	Organisaatio on tunnistanut jatkuvuuttaan uhkaavat tärkeimmät seikat ja varautunut niihin suojaus-, varmennus-, kahdennus- yms. menettelyin. Organisaatiolla on lakisääteinen vakuutusturva.		
A 602.0 **Onko organisaatiossa määritetty onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien käsittelystä ja tutkinnasta vastaavat henkilöt?** *Kysymyksellä arvioidaan:* *Onko organisaatio ottanut huomioon turvallisuuspoikkeamat ja onko niiden hallinta määritetty ja organisoitu. Onko yhteistoiminta viranomaisten suuntaan suunniteltu.*	Ei vaatimuksia.	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Vastuut on kuvattu henkilöiden tehtäväkuvauksissa. Vastaavat henkilöt ovat hyvin selvillä organisaation ja viranomaisen välisestä toimivalta- ja vastuujaosta.	Onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien käsittelystä ja tutkinnasta vastaavat henkilöt on määritetty ottaen huomioon organisaation toiminnan laajuus, organisaation osat ja tasot. Henkilöt ovat hyvin selvillä organisaation ja viranomaisen välisestä toimivalta- ja vastuujaosta.	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 603.0 **Onko vastuut kriisitilanteiden, onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien vaikutusten ennalta pienentämiseksi määritetty?** *Kysymyksellä arvioidaan:* *Onko organisaatio ottanut ennakolta huomioon poikkeavien tilanteiden ilmenemisen ja onko riskien pienentäminen määritetty ja organisoitu.*	Ei vaatimuksia.	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Valtuudet ja vastuut on kuvattu henkilöiden tehtäväkuvauksissa.	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Valtuudet ja vastuut on kuvattu henkilöiden tehtäväkuvauksissa. Kuvaus sisältää riskien pienentämisen vastuun.	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Valtuudet ja vastuut on kuvattu henkilöiden tehtäväkuvauksissa.		
A 604.0 **Onko organisaatiolla menetelmät turvallisuuspoikkeamien havaitsemiseksi ja suojaavien sekä korjaavien toimenpiteiden tekemiseksi?** *Kysymyksellä arvioidaan:* *Onko organisaatiolla menetelmät valvoa turvallisuustilannetta ja menetelmät sekä valmius suojaavien ja korjaavien toimenpiteiden tekemiseksi.*	Organisaatiossa on tunnettava tapa raportoida turvallisuuspoikkeamat.	Organisaatiossa on tunnettava tapa raportoida turvallisuuspoikkeamat. Turvallisuuspoikkeamien esiintymistä on valvottava.	Organisaatiolla on dokumentoitu järjestelmä, jolla se seuraa ja raportoi turvallisuuspoikkeamat kaikkien turvallisuuden osa-alueiden osalta. Poikkeamien seurantajärjestelmä on jatkuva. Organisaatiolle on määritetty vastuut ja valta toteuttaa suojaavat sekä korjaavat toimenpiteet.	Organisaatiossa on tunnettava tapa raportoida turvallisuuspoikkeamat. Turvallisuuspoikkeamien esiintymistä on valvottava.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 605.0 **Onko organisaatiolla menetelmät sen varmistamiseksi, että tehdyt suojaavat ja korjaavat turvallisuustoimenpiteet ovat tehokkaita ja oikein kohdistettuja?** *Kysymyksellä arvioidaan:* *Tehdäänkö turvallisuuden saavuttamiseksi oikeita asioita.*	Ei vaatimuksia.	Turvallisuustoimenpiteiden toivottua ja saavutettua vaikutusta verrataan. Organisaatiolla on käsitys panos-tuotos -suhteesta.	Turvallisuustoimenpiteiden toivottua ja saavutettua vaikutusta verrataan säännöllisesti. Organisaatiolla on käsitys panos-tuotos -suhteesta.	Turvallisuustoimenpiteiden vaikutus arvioidaan ja organisaatiolla on käsitys panos-tuotos -suhteesta.		
A 606.0 **Onko organisaatiolla menetelmät arvioida riskit, joita suunnitellut korjaavat toimenpiteet aiheuttavat?** *Kysymyksellä arvioidaan:* *Varmistaako organisaatio turvallisuusjärjestelmiä muutettaessa, ettei samalla aiheuteta uusia uhkia tai vaaratilanteita.*	Ei vaatimuksia.	Turvallisuustoiminnan prosessi sisältää arvion muutosten negatiivisista vaikutuksista.	Turvallisuustoiminnan prosessi sisältää arvion muutosten negatiivisista vaikutuksista.	Turvallisuustoiminnan prosessi sisältää arvion muutosten negatiivisista vaikutuksista.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 607.0 **Onko organisaatiolla menetelmät turvallisuustoimenpiteiden vaikutusten analysointia varten?** *Kysymyksellä arvioidaan:* *Dokumentoiko ja analysoiko organisaatio turvallisuustoimenpiteet sekä niiden vaikutukset.*	Organisaatio seuraa turvallisuustoimenpiteiden vaikutuksia.	Organisaatio analysoi turvallisuustoimenpiteiden vaikutukset vähintään vuosittain. Esimerkiksi tilastoja seuraamalla tarkastellaan tietyn vaaratilanteen tapahtumataajuuden muutosta.	Organisaatiolla on prosessi, joka dokumentoinnin lisäksi säännöllisesti analysoi tehdyt turvallisuustoimenpiteet ja niiden vaikutukset organisaation turvallisuustasoon ja toimintaan vähintään vuosittain. Analyysit käytetään hyödyksi turvallisuustoimintaa kehitettäessä.	Organisaatio seuraa turvallisuustoimenpiteiden vaikutuksia.		
A 608.0 **Onko organisaatiossa menettely, jonka avulla varmistetaan, että merkittävät tietojenkäsittelyympäristön muutokset tapahtuvat hallitusti?** **(ex I 109.0)** *Huom! Vaadittava toteutustapa riippuu kohteesta.* **Katso lisätietoja liitteestä 1 (A 608.0)**	Tietojenkäsittelyyn liittyviin muutoksiin on käytössä muutoshallintamenettely.	Tietojenkäsittelyyn liittyviin muutoksiin on käytössä muutoshallintamenettely.	Tietojenkäsittelyyn liittyviin muutoksiin on käytössä muutoshallintamenettely.	Tietojenkäsittelyyn liittyviin muutoksiin on käytössä muutoshallintamenettely	ISO/IEC 27002 Luku 12 ja 10.1.2, PCI DSS 6.4, COBIT 4.1 AI6, VAHTI 2/2010, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	

Turvallisuusdokumentaatio ja sen hallinta, osa-alue A700

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 701.0 **Onko organisaatiolla toimintamallit, jotka koskevat:** **a. turvallisuustiedostoja/turvallisuusrekistereitä tai dokumentointimenetelmiä?** **b. turvallisuusdokumentaation tietojen yksilöintiä ja jäljittämistä?** **c. turvallisuusdokumentaation säilyttämisaikoja, säilytyspaikkaa ja säilytyksen vastuita?** *Kysymyksellä arvioidaan:* *Onko organisaatiolla järjestelmä, jonka avulla hallitaan edellä mainitut osatekijät.*	Organisaatiolla on järjestelmä, joka sisältää omat ohjeistot ja tapahtuneet turvallisuuspoikkeamat.	Organisaatiolla on järjestelmä, joka sisältää turvallisuusrekisterit, omat ohjeistot ja tapahtuneet turvallisuuspoikkeamat. Järjestelmä täyttää lainsäädännön asettamat vaatimukset (mm. rekisteriseloste).	Organisaatiolla on helposti käytettävä ja sisällöltään kattava tietojenhallintajärjestelmä, joka on ulotettu organisaation kaikille tasoille. Järjestelmä sisältää turvallisuusrekisterit (esimerkiksi luvat) ja muut dokumentit (kuten ohjeet). Tietojen tallentaminen tapahtuu siten, että järjestelmän avulla tapahtumat voidaan yksilöidä ja jäljittää. Järjestelmä täyttää lainsäädännön asettamat vaatimukset esimerkiksi tiedon luottamuksellisuuden ja säilytysaikavaatimusten osalta.	Organisaatiolla on järjestelmä, joka sisältää omat ohjeistot ja tapahtuneet turvallisuuspoikkeamat.		
A 702.0 **Sisältävätkö rekisterit myös tiedot turvallisuustavoitteiden saavuttamisen tasosta?** *Kysymyksellä arvioidaan:* *Onko mitattavat tavoitteet asetettu selkeästi ja onko tavoitteiden toteutuminen helposti todettavissa järjestelmän avulla.*	Ei vaatimuksia.	Organisaatio pystyy osoittamaan turvallisuustavoitteiden saavuttamisen tason vähintään vuosittain.	Organisaatiolla on tietojenhallintajärjestelmä, josta ajantasaiset tiedot ovat saatavissa. Raportit ovat yksilöitävissä ja vertailtavissa ajan, paikan ja aiheen mukaisesti.	Organisaatio pystyy osoittamaan turvallisuustavoitteiden saavuttamisen tason vähintään vuosittain.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 703.0 **Sisältävätkö turvallisuusrekisterit tiedot annetuista turvallisuuskoulutuksista?** *Kysymyksellä arvioidaan:* *Rekisteröidäänkö turvallisuuskoulutukset siten, että niiden riittävyys ja voimassaolo voidaan todeta. Onko asetetut vaatimukset täytetty.*	Organisaatiolla on koulutusrekisteri, jolla voidaan osoittaa annettu koulutus ja sen sisältö.	Organisaatiolla on koulutusrekisteri, jolla voidaan osoittaa annettu koulutus, sen sisältö ja voimassaolo.	Organisaatiolla on turvallisuuden eri osa-alueisiin liittyvä koulutusrekisteri erillisenä tai osana organisaation muuta koulutusrekisteriä. Tietojen avulla voidaan seurata sitä, että kaikkiin koulutusta vaativiin tehtäviin koulutus on annettu ja koulutusten vanhentuminen on havaittavissa siten, että kertauskoulutus ja täydennyskoulutus voidaan antaa velvoitteiden täyttämiseksi.	Organisaatiolla on koulutusrekisteri, jolla voidaan osoittaa annettu koulutus ja sen sisältö.		
A 704.0 **Voidaanko dokumentaation perusteella osoittaa, että turvallisuuskoulutuksen taso on riittävän korkea?** *Kysymyksellä arvioidaan:* *Onko turvallisuuskoulutukselle asetettu määrälliset ja laadulliset tavoitteet ja rekisteröidäänkö näiden täyttyminen.*	Ei vaatimuksia.	Organisaation koulutusrekisteriin on kirjattu tasovaatimukset ja niiden toteutuminen varmistetaan siten, että työtehtävää ei aloiteta ennen koulutusvaatimuksen täyttymistä.	Organisaation koulutusrekisteriin on kirjattu tasovaatimukset ja niiden toteutuminen varmistetaan siten, että työtehtävää ei aloiteta ennen koulutusvaatimuksen täyttymistä.	Organisaation koulutusrekisteriin on kirjattu tasovaatimukset ja niiden toteutuminen varmistetaan siten, että työtehtävää ei aloiteta ennen koulutusvaatimuksen täyttymistä.		

Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen, osa-alue A800

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 801.0 **Ovatko organisaation kaikki henkilöt tietoisia turvallisuusvaatimusten noudattamisen tärkeydestä ja oikeista toimintatavoista?** *Kysymyksellä arvioidaan:* *Organisaation turvallisuuskulttuurin kypsyystasoa ja johdon sitoutumista turvallisuuden jatkuvaan parantamiseen kouluttamisen avulla.*	Erillisiin projekteihin osallistuva henkilöstö on koulutettu projektikohtaisten vaatimusten mukaisesti.	Organisaation koko henkilöstö on koulutettu henkilöstö-, tila- ja tietoturvallisuuden vaatimuksien osalta. Projektihenkilöstö on koulutettu projektikohtaisten vaatimusten mukaisesti.	Organisaation koko henkilöstö on koulutettu turvallisuuden tavoitteiden osalta. Projektihenkilöstö on koulutettu projektikohtaisten vaatimusten mukaisesti.	Organisaation koko henkilöstö on koulutettu henkilöstö-, tila- ja tietoturvallisuuden vaatimuksien osalta. Erillisiin projekteihin osallistuva henkilöstö on koulutettu projektikohtaisten vaatimusten mukaisesti.		
A 802.0 **Onko varmistuttu siitä, että henkilöstö tuntee omaan työhönsä liittyvät turvallisuusriskit?** *Kysymyksellä arvioidaan:* *Onko turvallisuusasioiden riskienarviointi toteutettu siten, että henkilöstö on itse mukana arvioinnissa ja tuntee työhönsä liittyvät turvallisuusriskit.*	Riskienarvioinnin yhteydessä käsitellään ainakin henkilöstö-, tila- ja tieto-turvallisuuden osa-alueita koskevat seikat. Henkilöstölle selvitetään sen tehtäviin liittyvät turvallisuusriskit.	Riskienarvioinnin yhteydessä käsitellään ainakin henkilöstö-, tila- ja tieto-turvallisuuden osa-alueita koskevat seikat. Henkilöstölle selvitetään sen tehtäviin liittyvät turvallisuusriskit.	Riskienarvioinnin yhteydessä käsitellään turvallisuuden kaikkia osa-alueita koskevat seikat ja henkilöstö osallistuu johdettuun riskienarviointiin.	Riskienarvioinnin yhteydessä käsitellään ainakin henkilöstö-, tila- ja tieto-turvallisuuden osa-alueita koskevat seikat. Henkilöstölle selvitetään sen tehtäviin liittyvät turvallisuusriskit.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 803.0 **Onko varmistuttu siitä, että henkilöstö osaa toimia oikein tilanteissa, joissa turvallisuus on vaarantunut?** *Kysymyksellä arvioidaan:* *Poikkeustilanteiden turvallisuusriskien hallintaa, esimerkiksi tilaturvallisuuden osalta tulipalotilanteet, tietoturvallisuuden osalta tietojen palauttamisen periaatteet.*	Tärkeimpiin poikkeamatilanteisiin on dokumentoidut toimintamallit ja niistä keskeisimpiä harjoitellaan.	Organisaatiolla on tiedossaan sitä uhkaavat keskeiset turvallisuusriskit. Tärkeimpiin poikkeamatilanteisiin on dokumentoidut toimintamallit ja niistä keskeisimpiä harjoitellaan säännöllisesti.	Organisaatiolla on riskienarviointiin perustuva dokumentoitu ja koulutettu toimintasuunnitelma tärkeimpien turvallisuusriskien varalle. Poikkeustilanteiden hallinta koulutetaan ja koulutettu toimintamalli harjoitellaan.	Organisaatiolla on tiedossaan sitä uhkaavat keskeiset turvallisuusriskit. Tärkeimpiin poikkeamatilanteisiin on dokumentoidut toimintamallit ja niistä keskeisimpiä harjoitellaan.		
A 803.1 **Miten organisaatiossa valvotaan tietoturvaohjeiden noudattamista?** *Lisäkysymys: Onko tietoturvarikkomusten käsittely ja seuraukset määritelty?* **(ex I 206.0)**	1) Tietoturvaohjeiden noudattamista valvotaan ja rikkeisiin puututaan. 2) Tietoturvarikkomusten käsittely ja seuraukset on määritelty. 3) Käsittely ja seuraukset ovat samat koko henkilöstölle.	Perustason vaatimusten lisäksi: Tietoturvarikkomukset tutkitaan viranomaistoimenpitein.	Perustason vaatimusten lisäksi: Tietoturvarikkomukset tutkitaan viranomaistoimenpitein.	Tietoturvaohjeiden noudattamista valvotaan ja rikkeisiin puututaan.	ISO/IEC 27002 8.2.3, VAHTI 8/2006 Voidaan todentaa selvittämällä a. miten valvonta käytännössä toteutetaan, b. millaisia rikkeitä on tullut viime vuosina esille, ja c. miten rikkeisiin on puututtu.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 804.0 **Onko organisaatiolla menetelmä varmistua siitä, minkä tasoista turvallisuuskoulutusta henkilöstö tarvitsee tehtävissään?** *Kysymyksellä arvioidaan:* *Onko organisaatiolla prosessi, jossa arvioidaan annettavan koulutuksen tarve huomioiden lakien vaatimukset, riskienarviointien perusteella annettavat keskeiset turvallisuusasiat ja yleiset turvallisuustietoisuuden vaatimukset.*	Ei vaatimuksia.	Organisaatiolla on toiminto, joka määrittää turvallisuuskoulutuksen tasovaatimukset ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueiden osalta.	Organisaatiolla on toiminto, joka arvioi koulutuksen kohderyhmiä, annettavan koulutuksen sisältöä ja laatua.	Organisaatiolla on toiminto, joka määrittää turvallisuuskoulutuksen tasovaatimukset ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueiden osalta.		
A 805.0 **Onko organisaatiolla menetelmä varmistaa, että työntekijöillä on tehtävien edellyttämä sopivuus, turvallisuuskoulutus, tehtävään perehtyminen ja kokemus?** *Kysymyksellä arvioidaan:* *Turvallisuuskoulutustason selvittämisen mahdollisuutta.*	Turvallisuuskoulutusrekisteristä saadaan tieto, onko kyseiselle henkilölle annettu vaadittu koulutus.	Turvallisuuskoulutusrekisteristä saadaan tieto tehtävän edellyttämästä turvallisuuskoulutustasosta.	Turvallisuuskoulutusrekisteristä saadaan tieto tehtävän edellyttämästä turvallisuuskoulutustasosta.	Turvallisuuskoulutusrekisteristä saadaan tieto tehtävän edellyttämästä turvallisuuskoulutustasosta.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 806.0 **Miten organisaatiossa on huolehdittu riittävästä ohjeistuksesta, koulutuksesta ja tiedotuksesta?** **(ex I 204.0)** *	Organisaatiossa on huolehdittu riittävästä ohjeistuksesta ja koulutuksesta. 1) Henkilöstö on saanut perehdytyksen yhteydessä ohjeet kuinka toimia organisaation turvaperiaatteiden mukaisesti. Ohjeistuksen/koulutuksen tulee sisältää tärkeimmät toimintatilanteet (peruskäyttö, etäkäyttö, matkatyö, ylläpito, jne.) ja -tavat. 2) Henkilöille, jotka on otettu palvelukseen sellaiseen asemaan, jossa he voisivat päästä suojattaviin tietoihin, annetaan heti aluksi ja säännöllisin väliajoin tarkat ohjeet turvatoimien tarpeellisuudesta ja niiden täytäntöönpanomenettelyistä. 3) Suojattavia tietoja käsitteleviin järjestelmiin on laadittu turvallisen käytön ohjeistus. 4) Tiedon merkitsemistä (luokittelua), käsittelyä (sis. salaus) ja tallennusta koskeva ohjeistus on laadittu ja otettu käyttöön. 5) Henkilöstö on ohjeistettu ja velvoitettu ilmoittamaan havaitsemistaan tietoturvapoikkeamista ja -uhista. 6) Tulevista työasemien tietoturva-aukkojen päivityksistä tiedotetaan vähintään sillä tarkkuudella, että käyttäjät ovat tietoisia siitä, mitä toimia heiltä vaaditaan. 7) Käyttäjille tiedotetaan kaikkein merkittävimmistä ajankohtaisista uhista, jotka kohdistuvat organisaation käyttäjiin (esim. kohdistetuista hyökkäyksistä). 8) Järjestelmien ylläpitohenkilöstö on suorittanut ko. järjestelmiä koskevan valmistaja-/ympäristökohtaisen turvallisuuskoulutuksen, muun yleisesti hyväksytyn ko. ympäristöön soveltuvan turvallisuuskoulutuksen, tai ylläpitohenkilöstölle on muuten hankittu riittävä osaaminen ko. järjestelmien turvalliseen ylläpitoon.	Perustason vaatimusten lisäksi: Henkilöille annettava turvallisuuskoulutus on dokumentoitu.	Perustason vaatimusten lisäksi: Henkilöille annettava turvallisuuskoulutus on dokumentoitu.	Organisaatiossa on huolehdittu riittävästä ohjeistuksesta ja koulutuksesta. Henkilöstö on saanut perehdytyksen yhteydessä ohjeet, kuinka toimia organisaation turvaperiaatteiden mukaisesti. Ohjeistuksen/koulutuksen tulee sisältää tärkeimmät toimintatilanteet (peruskäyttö, etäkäyttö, matkatyö, ylläpito, jne.) ja -tavat.	ISO/IEC 27002 10.7.3, ISO/IEC 27002 13.1.1, ISO/IEC 27002 7.2.2, ISO/IEC 27002 8.2.2, PCI DSS 12.6, COBIT 4.1 DS7, Kansallisen turvallisuusviranomaisen ”Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”, VAHTI 8/2006, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 liite I, VAHTI 2/2010, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf Voidaan todentaa esim. siten, että kysellään muutamalta tarkastuksen yhteydessä satunnaisesti valitulta käyttäjältä, miten heidät on ohjeistettu toimimaan tietoturvallisesti.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 807.0 **Onko tietoon ja tietojenkäsittelypalveluihin määritetty hyväksyttävän käytön säännöt ja onko niistä tiedotettu henkilöstölle?** **(ex I 205.0)**	1) Tiedon ja tietojenkäsittelypalveluihin liittyvien suojattavien kohteiden hyväksyttävän käytön säännöt on määritetty. 2) Hyväksyttävän käytön säännöissä otetaan kantaa vähintään siihen, saako organisaation tietojärjestelmiä käyttää henkilökohtaisiin tarpeisiin (sähköposti, levytila, pankkipalveluiden käyttö, jne.). 3) On selkeästi tiedotettu hyväksyttävän käytön säännöistä henkilöstölle. 4) Hyväksyttävän käytön säännöt ovat henkilöstölle helposti saatavilla.	1) Tiedon ja tietojenkäsittelypalveluihin liittyvien suojattavien kohteiden hyväksyttävän käytön säännöt on määritetty. 2) Hyväksyttävän käytön säännöissä otetaan kantaa vähintään siihen, saako organisaation tietojärjestelmiä käyttää henkilökohtaisiin tarpeisiin (sähköposti, levytila, pankkipalveluiden käyttö, jne.). 3) On selkeästi tiedotettu hyväksyttävän käytön säännöistä henkilöstölle. 4) Hyväksyttävän käytön säännöt ovat henkilöstölle helposti saatavilla.	1) Tiedon ja tietojenkäsittelypalveluihin liittyvien suojattavien kohteiden hyväksyttävän käytön säännöt on määritetty. 2) Hyväksyttävän käytön säännöissä otetaan kantaa vähintään siihen, saako organisaation tietojärjestelmiä käyttää henkilökohtaisiin tarpeisiin (sähköposti, levytila, pankkipalveluiden käyttö, jne.). 3) On selkeästi tiedotettu hyväksyttävän käytön säännöistä henkilöstölle. 4) Hyväksyttävän käytön säännöt ovat henkilöstölle helposti saatavilla.	1) Tiedon ja tietojenkäsittelypalveluihin liittyvien suojattavien kohteiden hyväksyttävän käytön säännöt on määritetty. 2) Hyväksyttävän käytön säännöissä otetaan kantaa vähintään siihen, saako organisaation tietojärjestelmiä käyttää henkilökohtaisiin tarpeisiin (sähköposti, levytila, pankkipalveluiden käyttö, jne.). 3) On selkeästi tiedotettu hyväksyttävän käytön säännöistä henkilöstölle. 4) Hyväksyttävän käytön säännöt ovat henkilöstölle helposti saatavilla.	ISO/IEC 27002 7.1.3, PCI DSS 12.3, VAHTI 8/2006 Voidaan todentaa tarkistamalla AUP:n (acceptable use policy) olemassaolo ja sisältö, lisäksi se, onko AUP helposti saatavilla henkilöstölle. Selvitetään lisäksi miten AUP:sta tiedotettu henkilöstölle.	

Raportointi ja johdon katselmukset, osa-alue A900

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 901.0 **Raportoiko turvallisuudesta vastaava henkilö suoraan organisaation ylimmälle johdolle turvallisuuteen liittyvissä asioissa?** *Kysymyksellä arvioidaan:* *Johdon sitoutumista turvallisuustyöhön.* *Onko turvallisuusjohdolla suora nopea ja tehokas yhteyskanava organisaation johtoon?*	Turvallisuudesta vastaava henkilö raportoi organisaation johdolle siten, että johtoryhmä on selvillä turvallisuustoiminnan ja turvallisuustilanteen tasosta. Huomattavat poikkeamat tai muutokset on voitava raportoida johdolle välittömästi esimerkiksi kriisienhallintamenettelyn kautta.	Turvallisuudesta vastaava henkilö raportoi organisaation johdolle säännöllisesti siten, että johtoryhmä on selvillä turvallisuustoiminnan ja turvallisuustilanteen tasosta. Huomattavat poikkeamat tai muutokset on voitava raportoida johdolle välittömästi esimerkiksi kriisienhallintamenettelyn kautta.	Turvallisuudesta vastaava henkilö raportoi toimitusjohtajalle, varatoimitusjohtajalle, johtoryhmälle tai johtoryhmän jäsenelle.	Turvallisuudesta vastaava henkilö raportoi organisaation johdolle säännöllisesti siten, että johtoryhmä on selvillä turvallisuustoiminnan ja turvallisuustilanteen tasosta. Huomattavat poikkeamat tai muutokset on voitava raportoida johdolle välittömästi esimerkiksi kriisienhallintamenettelyn kautta.		
A 902.0 **Tarkastaako organisaation ylin johto säännöllisesti (vähintään kerran vuodessa) turvallisuusjärjestelmän toimivuuden?** *Kysymyksellä arvioidaan:* *Organisaation johdon sitoutumista turvallisuustyön jatkuvaan parantamiseen ja laadukkaaseen johtamiseen.*	Turvallisuusasioiden raportointi on järjestetty osaksi muuta johtamisprosessia.	Turvallisuusasiat esitetään osana organisaation johtamisprosessia laaja-alaisesti ainakin kerran vuodessa johtoryhmälle. Johtoryhmästä on nimetty henkilö, joka seuraa turvallisuuteen liittyviä asioita osana toimenkuvaansa.	Turvallisuusasiat esitetään osana organisaation johtamisprosessia laaja-alaisesti ainakin kerran vuodessa johtoryhmälle esimerkiksi johdon katselmuksessa. Johtoryhmästä on nimetty henkilö, joka seuraa turvallisuuteen liittyviä asioita osana toimenkuvaansa.	Vähintään vuosittainen turvallisuusasioiden raportointi on järjestetty osaksi muuta johtamisprosessia.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 903.0 **Arvioidaanko ylimmän johdon tekemissä tarkastuksissa turvallisuusjärjestelmän soveltuvuus, resurssien riittävyys ja toiminnan tehokkuus?** *Kysymyksellä arvioidaan:* *Raportoinnin laatu ja laaja-alaisuus.*	Ei vaatimuksia.	Organisaation turvallisuustavoitteet ja tavoitteiden saavuttaminen esitetään mitattavassa muodossa.	Organisaation turvallisuustyön tavoitteet ja tavoitteiden saavuttaminen esitetään mitattavassa muodossa.	Organisaation turvallisuustavoitteet ja tavoitteiden saavuttaminen esitetään mitattavassa muodossa.		
A904.0 **Dokumentoidaanko tehdyt seurantatarkastukset?** *Kysymyksellä arvioidaan:* *Organisaation johdon systemaattista toimintaa ja mahdollisuutta tarkastella seurannan perusteella tehtyjen ratkaisujen vaikutusta ja tehokkuutta.*	Ei vaatimuksia.	Seurantatarkastukset dokumentoidaan.	Seurantatarkastukset dokumentoidaan turvallisuuden tietojenhallintajärjestelmään.	Seurantatarkastukset dokumentoidaan.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
A 905.0 **Toimivatko nämä seurantatarkastukset jatkuvan parannuksen perustekijöinä, eli vaikuttavatko ne politiikan ja tavoitteiden sisältöön?** *Kysymyksellä arvioidaan:* *Muodostaako turvallisuusjohtaminen laadukkaan toiminnan, jossa politiikka ja tavoitteet sekä turvallisuuden toimintamallit ovat jatkuvan parantamisen kohteina.*	Ei vaatimuksia.	Turvallisuusjohtamiseen kuuluu prosessi, jossa johdon katselmuksen palautetta käytetään turvallisuuspolitiikan ja -tavoitteiden uudelleenarvioimisessa.	Organisaation turvallisuustyön prosessi sisältää toiminnon, jossa johdon katselmuksessa esitetyt tulokset sekä niistä tehdyt johtopäätökset käytetään hyödyksi turvallisuuspolitiikan ja -tavoitteiden uudelleenarvioimisessa.	Turvallisuusjohtamiseen kuuluu prosessi, jossa johdon palautetta käytetään turvallisuuspolitiikan ja -tavoitteiden uudelleenarvioimisessa.		

P

OSA-ALUE

Henkilöstöturvallisuus

Sisällys

Soveltamisala

Osassa työnantajan tehtäviä henkilöstö joutuu käsittelemään viranomaisen salassa pidettäviä tietoja taikka työnantajan sellaista sensitiivistä tietoa (yritys- tai liike- ja ammattisalaisuuksia), joiden turvallisuusmääräysten vastainen käyttö saattaisi aiheuttaa vakavaa vahinkoa työnantajalle. Tämän kriteeristön tarkoituksena on osaltaan parantaa mahdollisuuksia valita näihin tehtäviin turvallisuusvaatimukset täyttävät henkilöt. Kriteeristöä voidaan käyttää henkilöstöturvallisuuden vaatimuksina yritysten keskinäisissä ja viranomaisen kanssa tehtävissä turvallisuussopimuksissa kuitenkin siten, että erityisesti hallinnollisen turvallisuuden (turvallisuusjohtaminen) alaan kuuluvat henkiöstöhallintaa sivuavat vaatimukset otetaan huomioon.

Henkilöstöturvallisuuskriteeristö alkaa teknisellä osiolla, joka on sama kaikissa suojaustasoissa. Sen tarkoituksena on sensitiiviseen tai salassa pidettävään tietoon pääsevän henkilöstön hallinnointi. Kriteeristö jatkuu tietoturvatasoittain (IV-II) jaoteltuna vaatimusluettelona, jossa käsitellään tehtävään rekrytoitaessa taikka valittaessa huomioitavia seikkoja. Vaatimusluetteloa voidaan soveltaa uusrekrytointia tehtäessä, mutta myös soveltuvin osin valittaessa jo olemassa olevasta henkilöstöstä sopivia ammattilaisia turvallisuusluokiteltuun projektiin. Käytettäessä ulkopuolisia alihankkijoita, on sopimusneuvotteluvaiheessa hyvä tuoda esille, että sopimuskumppanin projektiin osallistuva henkilöstö tullaan mahdollisesta alistamaan turvallisuusselvitysmenettelyyn. Viranomaisvaatimuksia täydentää kunkin kysymyksen osalta elinkeinoelämän toimijoille suunnattu, vapaaehtoisuuteen perustuva suositus.

Yksityisyyden suoja

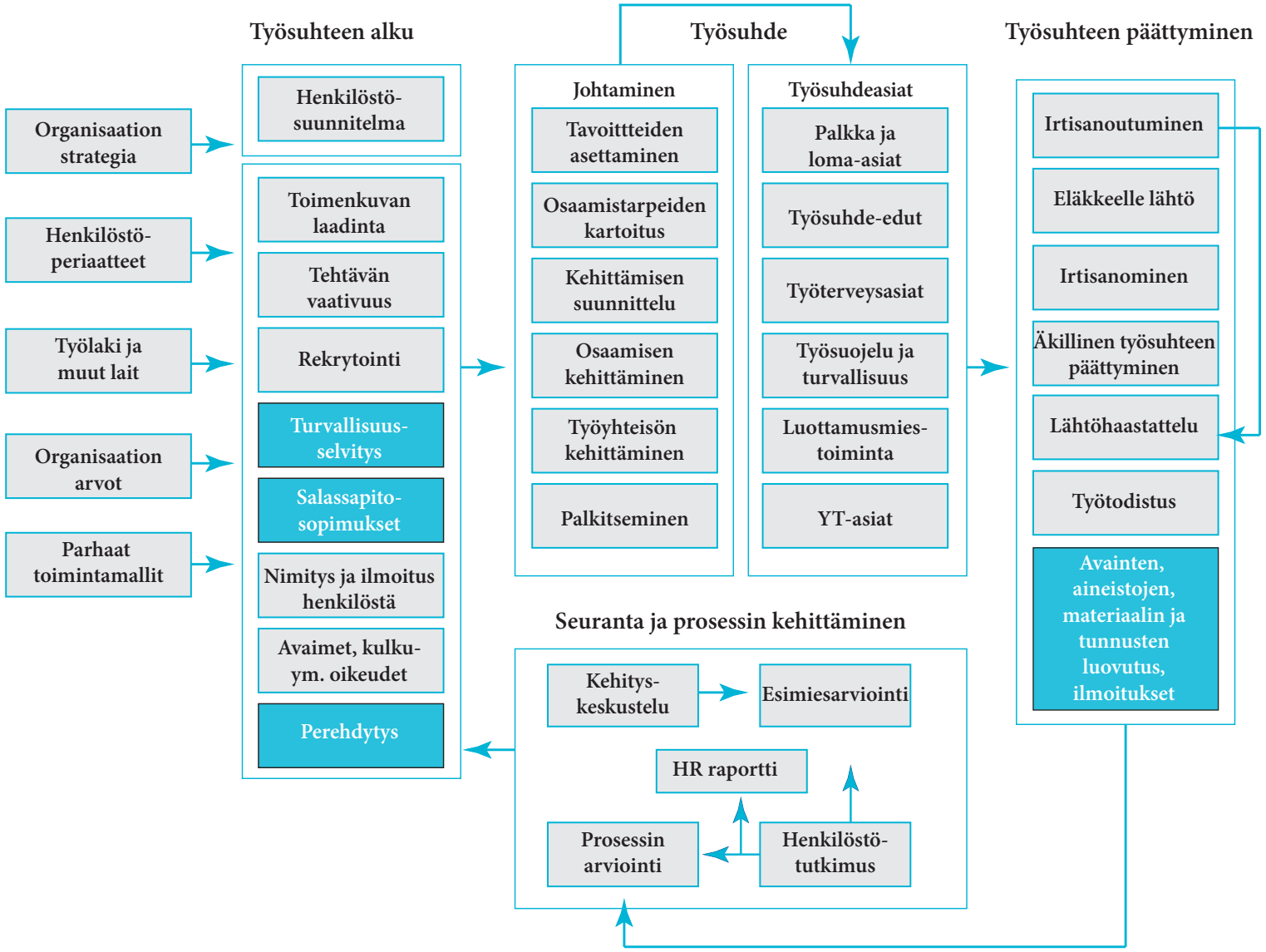
Liiteohjeistoa sovellettaessa on huomioitava laki yksityisyyden suojasta työelämässä. Erityisesti on muistettava, että työantaja saa käsitellä vain välittömästi työsuhteen kannalta merkittäviä tietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työsuhteen erityisluonteesta. Tällaisena työsuhteen erityisluonteena voidaan pitää mm. työsuhteen edellyttämää poikkeuksellisen luotettavuuden vaatimusta. Työantajan on myös pääsääntöisesti kerättävä työntekijää koskevat henkilötiedot työntekijältä itseltään. Muussa tapauksessa työntekijältä on hankittava suostumus tietojen keräämiseen. Henkilöluottotietoja kerättäessä henkilön luotettavuuden selvittämiseksi ei tarvita suostumusta, mutta tällöinkin työntekijää on informoitava etukäteen tietojen hankkimisesta sekä käytettävistä tietolähteistä. Muualta kuin henkilöltä itseltään kerättävien tietojen käytöstä on informoitava työntekijää ennen päätösten tekemistä. Tältä osin työsuhteen pelisäännöt on syytä käsitellä yhteistoimintamenettelyssä.

Ohjeita ja neuvoja

Muilta osin hyvään ja turvalliseen henkilöstöprosessiin liittyen on saatavissa hyviä ohjeita ja neuvoja mm. valtionhallinnon tietoturvallisuuden johtoryhmän julkaisusta VAHTI 2/2008: ”Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta”. Seuraavalla sivulla on esitetty em. julkaisun henkilöstöprosessikaavio.

Turvallisuusauditointikriteeristön ensimmäisen ja toisen version keskinäisiä eroja sisältävät kysymykset/vaatimukset on merkitty kysymyssarakkeeseen tähtimerkillä (*).

Henkilöstöprosessi



Lähde: VAHTI 2/2008

Tekninen kriteeristö, osa-alue P100

Osa-alue on luonteeltaan tekninen kriteeristö. Sen tarkoituksena on sensitiiviseen tai salassa pidettävään tietoon pääsevän henkilöstön hallinnointi.

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
P 101.0 **Onko hankkeeseen osallistuvista henkilöistä tehty luettelo?**	Hankkeeseen osallistuvasta henkilöstöstä on laadittava luettelo, joka sisältää nimen ja henkilötunnuksen, tehtävän sekä yrityksen nimen ja osaston, jonka palveluksessa henkilö on. Henkilöstö on hyväksytettävä hankkeeseen hankkeen turvallisuusvastaavalla.	Hankkeeseen osallistuvasta henkilöstöstä on laadittava luettelo, joka sisältää nimen ja henkilötunnuksen, tehtävän sekä yrityksen nimen ja osaston, jonka palveluksessa henkilö on. Henkilöstö on hyväksytettävä hankkeeseen hankkeen turvallisuusvastaavalla.	Hankkeeseen osallistuvasta henkilöstöstä on laadittava luettelo, joka sisältää nimen ja henkilötunnuksen, tehtävän sekä yrityksen nimen ja osaston, jonka palveluksessa henkilö on. Henkilöstö on hyväksytettävä hankkeeseen hankkeen turvallisuusvastaavalla.	Hankkeeseen osallistuvasta henkilöstöstä on laadittava luettelo, joka sisältää nimen ja henkilötunnuksen, tehtävän sekä yrityksen nimen ja osaston, jonka palveluksessa henkilö on. Henkilöstö on hyväksytettävä hankkeeseen hankkeen turvallisuusvastaavalla.		
P 102.0 **Onko menettelytapaohje luotu ja pitävätkö yhteyshenkilön tiedot paikkansa?** *Lisäkysymys: Säilytetäänkö henkilöstöasiakirjat asianmukaisesti?*	Oltava menettelytapaohje henkilöstössä tapahtuvien muutosten ilmoittamiseksi välittömästi hankkeen turvallisuusvastaavalle.	Oltava menettelytapaohje henkilöstössä tapahtuvien muutosten ilmoittamiseksi välittömästi hankkeen turvallisuusvastaavalle.	Oltava menettelytapaohje henkilöstössä tapahtuvien muutosten ilmoittamiseksi välittömästi hankkeen turvallisuusvastaavalle.	Oltava menettelytapaohje henkilöstössä tapahtuvien muutosten ilmoittamiseksi välittömästi hankkeen turvallisuusvastaavalle.		
P 103.0 **Onko koulutusdokumentaatio olemassa (merkinnät saadusta koulutuksesta)?**	Hankkeeseen osallistuvalle henkilöstölle on koulutettu hankkeen turvallisuuteen liittyvät asiat.	Hankkeeseen osallistuvalle henkilöstölle on koulutettu hankkeen turvallisuuteen liittyvät asiat.	Hankkeeseen osallistuvalle henkilöstölle on koulutettu hankkeen turvallisuuteen liittyvät asiat.	Hankkeeseen osallistuvalle henkilöstölle on koulutettava hankkeen turvallisuuteen liittyvät asiat.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
P 104.0 **Onko vierailijaluettelo olemassa ja pidetäänkö sitä yllä asianmukaisesti?** *Lisäkysymys:* *Ymmärtääkö isäntähenkilöstö vieraiden käsittelysäännöt?*	Tarpeettomia vierailuja hankkeessa käytettäviin tiloihin tulee välttää. Mahdollisien vierailujen aikana tulee tietoaineisto olla säilytettynä siten, että hankkeen ulkopuoliset henkilöt eivät pääse perehtymään siihen. Vieraat eivät saa jäädä valvomatta mainittuihin tiloihin ilman isäntää tai hänen edustajaansa.	Tarpeettomia vierailuja hankkeessa käytettäviin tiloihin tulee välttää. Mahdollisien vierailujen aikana tulee tietoaineisto olla säilytettynä siten, että hankkeen ulkopuoliset henkilöt eivät pääse perehtymään siihen. Vieraat eivät saa jäädä valvomatta mainittuihin tiloihin ilman isäntää tai hänen edustajaansa.	Tarpeettomia vierailuja hankkeessa käytettäviin tiloihin tulee välttää. Mahdollisien vierailujen aikana tulee tietoaineisto olla säilytettynä siten, että hankkeen ulkopuoliset henkilöt eivät pääse perehtymään siihen. Vieraat eivät saa jäädä valvomatta mainittuihin tiloihin ilman isäntää tai hänen edustajaansa.	Tarpeettomia vierailuja hankkeessa käytettäviin tiloihin tulee välttää. Mahdollisien vierailujen aikana tulee tietoaineisto olla säilytettynä siten, että hankkeen ulkopuoliset henkilöt eivät pääse perehtymään siihen. Vieraat eivät saa jäädä valvomatta mainittuihin tiloihin ilman isäntää tai hänen edustajaansa.		
P 105.0 **Noudatetaanko vaatimuksia suojaustasojen tai turvallisuusluokituksen mukaisesti?**	Rekrytointimenettelyohjeistusta sovelletaan.	Rekrytointimenettelyohjeistusta sovelletaan.	Rekrytointimenettelyohjeistusta sovelletaan.	Rekrytointimenettelyohjeistusta sovelletaan.		

Riittävän osaamisen varmistaminen, osa-alue P200

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
P 201.0 **Onko työnhakijalta vaadittu keskeiset dokumentit jo olemassa olevan osaamisen varmistamiseksi?**	Vaaditaan työnhakijalta opinto- ja työhistoria, nimikirjanote, suositukset ja todistukset.	Vaaditaan työnhakijalta opinto- ja työhistoria, nimikirjanote, suositukset ja todistukset.	Vaaditaan työnhakijalta opinto- ja työhistoria, nimikirjanote, suositukset ja todistukset.	Vaaditaan työnhakijalta opinto- ja työhistoria, nimikirjanote, suositukset ja todistukset.	Laki yksityisyyden suojasta työelämässä 4§.	
P 202.0 **Miten työhaastattelussa saatujen tietojen oikeellisuus tarkastetaan?** *Perustelu:* *Harhaanjohtavien referenssien ja todistusten antaminen ei ole harvinaista.*	Tarkistetaan saatujen tietojen oikeellisuus.	Tarkistetaan saatujen tietojen oikeellisuus.	Tarkistetaan saatujen tietojen oikeellisuus.	Tarkistetaan saatujen tietojen oikeellisuus.	Auditoinnin jälkeen ohjataan tarvittaessa, miten toteutetaan käytännössä.	
P 203.0 **Varmennetaanko haastattelutilanteessa työnhakijan osaamista asiantuntevilla kysymyksillä?**	Haastattelulla varmennetaan henkilön taustatietojen paikkansapitävyys ja osaaminen	Haastattelulla varmennetaan henkilön taustatietojen paikkansapitävyys ja osaaminen	Haastattelulla varmennetaan henkilön taustatietojen paikkansapitävyys ja osaaminen	Haastattelulla varmennetaan henkilön taustatietojen paikkansapitävyys ja osaaminen		

Henkilön muu soveltuvuus tehtävään, osa-alue P300

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
P 301.0 **Varmennetaanko haastattelutilanteessa, että henkilö pystyy työssään toimimaan yrityksen arvojen mukaisesti?**	Haastattelulla varmennetaan, ettei henkilö joudu työtehtävissä kohtuuttomiin valintatilanteisiin. Pyydetään tieto myös luottamukseen vaikuttavista aiemmista työtehtävistä.	Haastattelulla varmennetaan, ettei henkilö joudu työtehtävissä kohtuuttomiin valintatilanteisiin. Pyydetään tieto myös luottamukseen vaikuttavista aiemmista työtehtävistä.	Haastattelulla varmennetaan, ettei henkilö joudu työtehtävissä kohtuuttomiin valintatilanteisiin. Pyydetään tieto myös luottamukseen vaikuttavista aiemmista työtehtävistä.	Haastattelulla varmennetaan, ettei henkilö joudu työtehtävissä kohtuuttomiin valintatilanteisiin. Pyydetään tieto myös luottamukseen vaikuttavista aiemmista työtehtävistä.	Laki yksityisyyden suojasta työelämässä 3 §. Myös uuteen projektiin valittaessa. Voidaan kysyä esim. ymmärrystä kilpailunrajoitus- ja salassapitosopimuksista.	
P 302.0 **Onko huumausainetestaus käytettävissä mikäli siihen katsotaan olevan tarvetta?**	Huumausainetestaus edellytetään tarvittaessa.	Huumausainetestaus edellytetään tarvittaessa.	Huumausainetestaus edellytetään tarvittaessa.	Huumausainetestaus edellytetään tarvittaessa.	Laki yksityisyyden suojasta työelämässä 6 §, 7 §, 8 §, 9 §, 14 §. Laki yhteistoiminnasta yrityksissä (334/2007) 19 § 2 kohta	
P 303.0 **Varmennetaanko ammattilaisten tekemillä testeillä henkilön kykenevyys erityistä luotettavuutta vaativaan työhön?**	Henkilö- ja soveltuvuusarviointitesti.	Henkilö- ja soveltuvuusarviointitesti.	Henkilö- ja soveltuvuusarviointitesti.	Henkilö- ja soveltuvuusarviointitesti.	Laki yksityisyyden suojasta työelämässä 13 §	

Rekrytointipäätöksen jälkeiset toimet, osa-alue P400

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
P 401.0 **Käytetäänkö tähän tehtävään otettaessa salassapito- ja vaitiolositoumuksia ja jos, niin mikä niiden tarkka sisältö on?**	Salassapito- tai vaitiolositoumusmenettely on käytössä.	Salassapito- tai vaitiolositoumusmenettely on käytössä.	Salassapito- tai vaitiolositoumusmenettely on käytössä.	Salassapito- tai vaitiolositoumusmenettely on käytössä.	Myös uuteen projektiin valittaessa.	
P 402.0 **Käytetäänkö rekrytoitaessa koeaikaa ja jos, niin kuinka pitkää koeaikaa käytetään?**	Koeaikamenettely on käytössä.	Koeaikamenettely on käytössä.	Koeaikamenettely on käytössä.	Koeaikamenettely on käytössä.	TyösopimusL 1 luku 4 § 2 luku 4 §	
P 403.0 **Minkä tehtävien osalta katsotaan, että vastuuhenkilötiedot ja yrityskytkennät on syytä selvittää?** *Lisäkysymys:* *Miten tiedot selvitetään?*	Selvitysmenettely vastuuhenkilötietojen ja yrityskytkentöjen tarkastamiseksi on käytössä tehtäväperusteisesti.	Selvitysmenettely vastuuhenkilötietojen ja yrityskytkentöjen tarkastamiseksi on käytössä tehtäväperusteisesti.	Selvitysmenettely vastuuhenkilötietojen ja yrityskytkentöjen tarkastamiseksi on käytössä tehtäväperusteisesti.	Selvitysmenettely vastuuhenkilötietojen ja yrityskytkentöjen tarkastamiseksi on käytössä tehtäväperusteisesti.	Henkilötietolaki 8 § 1 mom. 8 kohta. Henkilöltä itseltään ja käytettävissä olevista muista rekistereistä	
P 404.0 **Haetaanko henkilöstä suppea turvallisuusselvitys, mikäli tämä on mahdollista?** *	Haetaan suppea turvallisuusselvitys mahdollisuuksien mukaan tilan, paikan tai toiminnan suojaamiseksi.	Haetaan suppea turvallisuusselvitys mahdollisuuksien mukaan tilan, paikan tai toiminnan suojaamiseksi.	Haetaan suppea turvallisuusselvitys mahdollisuuksien mukaan tilan, paikan tai toiminnan suojaamiseksi.	Haetaan suppea turvallisuusselvitys mahdollisuuksien mukaan tilan, paikan tai toiminnan suojaamiseksi.	Turvallisuusselvityslaki 19§	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
P 405.0 **Onko perusmuotoisen turvallisuusselvityksen hakumahdollisuus selvitetty tämän projektin tai tehtävän osalta?** *	Ei vaatimuksia.	Henkilöltä edellytetään etukäteen hanke- tai tehtäväkohtaisesti suostumus turvallisuusselvitykseen. Turvallisuusselvitys haetaan tarpeen mukaan perusmuotoisena.	Haetaan perusmuotoinen turvallisuusselvitys tietojen suojaamiseksi mahdollisuuksien mukaan.	Ei erityissuosituksia.	Myös uuteen projektiin valittaessa. Hakijana joko rekrytoija taikka turvallisuussopimuksen mukainen suojattavan edun omistaja.	
P 406.0 **Haetaanko projektiin tai tehtävään valittavista henkilöistä luottotiedot?** *	Ei viranomaisvaatimuksia.	Ei viranomaisvaatimuksia.	Ei viranomaisvaatimuksia.	Yritys voi projektin tai tehtävän luonteen niin vaatiessa hankkia henkilöistä luottotiedot luottotietolain määrittämissä puitteissa ja edellytyksin.	Laki yksityisyyden suojasta työelämässä (13.8.2004/759) 5 a §. Luottotietolaki (11.5.2007/527) 9§.	
P 407.0 **Onko salassapito- tai vaitiolositoumukset laadittu ja otettu käyttöön siten, että ne vastaavat organisaation tietojen suojaamistarpeita?** **(ex I 202.0)**	Kaikki työntekijät, toimittajat, kumppanit, alihankkijat ja ulkopuoliset käyttäjät allekirjoittavat salassapito- tai vaitiolositoumuksen ennen pääsyoikeuden saamista suojattavaan tietoon.	Kaikki työntekijät, toimittajat, kumppanit, alihankkijat ja ulkopuoliset käyttäjät allekirjoittavat salassapito- tai vaitiolositoumuksen ennen pääsyoikeuden saamista suojattavaan tietoon.	Kaikki työntekijät, toimittajat, kumppanit, alihankkijat ja ulkopuoliset käyttäjät allekirjoittavat salassapito- tai vaitiolositoumuksen ennen pääsyoikeuden saamista suojattavaan tietoon.	Salassapito- tai vaitiolositoumukset vastaavat organisaation tietojen suojaamistarpeita.	ISO/IEC 27002 6.1.5, ISO/IEC 27002 8.1.3 Koko salassapitoketju tulee olla tuettu salassapitosopimuksin. Ts. kun organisaatio tekee sopimuksen salassapidosta alihankkija-/kumppaniyrityksen kanssa ja alihankkija/kumppani oman työntekijänsä kanssa, tavoitteena on henkilökohtainen vastuu (työntekijä) ja korvausvelvollisuus (alihankkija/kumppani).	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
P408.0 **Pääkysymys:** **Ovatko avainhenkilöt ja organisaation riippuvuus heistä tunnistettu?** *Lisäkysymys:* *Onko heidän varalleen suunniteltu varahenkilöt tai -menettelyt?* **(ex I 203.0)**	1) Organisaation avainhenkilöt on tunnistettu ja estymisiin on varauduttu esimerkiksi osaamisen dokumentoinnilla ja varahenkilömenettelyillä. 2) Varahenkilöt ovat riittävästi koulutettuja varallaolotehtäviinsä.	1) Organisaation avainhenkilöt on tunnistettu ja estymisiin on varauduttu esimerkiksi osaamisen dokumentoinnilla ja varahenkilömenettelyillä. 2) Varahenkilöt ovat riittävästi koulutettuja varallaolotehtäviinsä.	1) Organisaation avainhenkilöt on tunnistettu ja estymisiin on varauduttu esimerkiksi osaamisen dokumentoinnilla ja varahenkilömenettelyillä. 2) Varahenkilöt ovat riittävästi koulutettuja varallaolotehtäviinsä.	Organisaation avainhenkilöt on tunnistettu ja estymisiin on varauduttu riskienarvioinnin mukaisesti.	VAHTI 8/2006, COBIT 4.1 PO4.13, COBIT 4.1 PO7	

Toimenpiteet työsuhteen solmimisen yhteydessä, osa-alue P500

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
P 501.0 **Miten varmistetaan, että työnhakija ja työnantaja ovat samaa mieltä työntekijän tehtävistä, vastuista, oikeuksista sekä velvollisuuksista etenkin tietojen suojaamisen osalta?**	Tehtävät, vastuut, oikeudet ja velvollisuudet on mahdollisimman tarkkaan määritelty esimerkiksi toimenkuvassa.	Tehtävät, vastuut, oikeudet ja velvollisuudet on mahdollisimman tarkkaan määritelty esimerkiksi toimenkuvassa.	Tehtävät, vastuut, oikeudet ja velvollisuudet on mahdollisimman tarkkaan määritelty esimerkiksi toimenkuvassa.	Tehtävät, vastuut, oikeudet ja velvollisuudet on mahdollisimman tarkkaan määritelty esimerkiksi toimenkuvassa.	Myös uuteen projektiin valittaessa.	
P 502.0 **Miten uusi työntekijä perehdytetään yhtiön turvallisuusmääräyksiin?** *Perustelu:* *Henkilökohtainen keskustelu turvallisuusasiantuntijan tms. kanssa yhtiön turvallisuusmääräyksistä ja niiden merkityksestä parantaa huomattavasti määräysten noudattamista.*	Turvallisuusperehdytys.	Turvallisuusperehdytys.	Turvallisuusperehdytys.	Turvallisuusperehdytys.	Myös uuteen projektiin valittaessa.	
P 503.0 **Miten uusi työntekijä perehdytetään tehtäviinsä ja yrityksen toimintaan?**	Perehdytys toimintaan ja tehtäviin.	Perehdytys toimintaan ja tehtäviin.	Perehdytys toimintaan ja tehtäviin.	Perehdytys toimintaan ja tehtäviin.	Myös uuteen projektiin valittaessa.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
P 504.0 Miten tietoturvakoulutus on yrityksessä järjestetty? *Lisäkysymys:* *Kuinka usein ja miten osaamista päivitetään?*	Koulutus tietoturva-asioihin, päivitys määräajoin.	Koulutus tietoturva-asioihin, päivitys määräajoin.	Koulutus tietoturva-asioihin, päivitys määräajoin.	Koulutus tietoturva-asioihin, päivitys määräajoin.	Myös uuteen projektiin valittaessa.	
P 505.0 **Miten prosessikuvaukset on toteutettu valtuuttamisesta ja pääsyoikeuksien antamisesta tietoon ja tiloihin?**	Valtuuttaminen ja pääsyoikeuden antaminen tietoon ja tiloihin.	Valtuuttaminen ja pääsyoikeuden antaminen tietoon ja tiloihin.	Valtuuttaminen ja pääsyoikeuden antaminen tietoon ja tiloihin.	Valtuuttaminen ja pääsyoikeuden antaminen tietoon ja tiloihin.	VAHTI 2/2008 Myös uuteen projektiin valittaessa.	

Toimenpiteet työsuhteen aikana, osa-alue P600

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
P 601.0 **Miten sijaisuusjärjestelyihin ja avainhenkilöihin liittyvät ohjeistukset (VAP-varaukset) on järjestetty?**	Ohjeisto on olemassa.	Ohjeisto on olemassa ja sitä ylläpidetään.	Ohjeisto on olemassa ja sitä ylläpidetään.	Ohjeisto on olemassa.	Pyydetään nähdä ko. ohjeistukset.	
P 602.0 **Miten yrityksessä on huolehdittu työtyytyväisyyden ja työmotivaation ylläpitämisestä?** *Lisäkysymys:* *Kannustetaanko täydennyskoulutukseen osallistumista ja osaamisen kehittämistä?*	Huolehtiminen työtyytyväisyydestä ja työmotivaatiosta.	Huolehtiminen työtyytyväisyydestä ja työmotivaatiosta voidaan näyttää toteen dokumenttipohjaisesti.	Huolehtiminen työtyytyväisyydestä ja työmotivaatiosta voidaan näyttää toteen dokumenttipohjaisesti.	Huolehtiminen työtyytyväisyydestä ja työmotivaatiosta.	Perustelu: Alhainen työtyytyväisyys ja työmotivaatio ovat merkittävä tehokkuutta huonontava tekijä sekä turvallisuusriski	
P 603.0 **Miten työssä jaksamisen ja työkyvyn seuranta on järjestetty?**	Työssä jaksamista ja työkykyä seurataan.	Työssä jaksamista ja työkykyä seurataan.	Työssä jaksamista ja työkykyä seurataan.	Työssä jaksamista ja työkykyä seurataan.	Mm. työterveyshuoltolaki 13 § Perustelu: Työkyvyn seuranta on merkittävä turvallisuuskysymys luotettavuutta vaativissa tehtävissä.	
P 604.0 **Miten toimitaan kun työntekijän toiminta muuttuu ilman havaittavaa syytä huolestuttavasti? Kenellä on toimintavastuu?**	Huomattavat muutokset käytöksessä tai toiminnassa; menettelyohjeet epäiltäessä väärinkäytöksiä tai hoitoonohjauksen tarvetta.	Huomattavat muutokset käytöksessä tai toiminnassa; menettelyohjeet epäiltäessä väärinkäytöksiä tai hoitoonohjauksen tarvetta.	Huomattavat muutokset käytöksessä tai toiminnassa; menettelyohjeet epäiltäessä väärinkäytöksiä tai hoitoonohjauksen tarvetta.	Huomattavat muutokset käytöksessä tai toiminnassa; menettelyohjeet epäiltäessä väärinkäytöksiä tai hoitoonohjauksen tarvetta.	Perustelu: Alentunut työkyky esimerkiksi alkoholismista johtuen taikka väärinkäytöksiin syyllistyminen näkyvät monesti poikkeavana käyttäytymisenä.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
P 605.0 **Löytyykö organisaatiosta menettelyohje työsuhteen päättämisestä?**	Organisaatiossa on käytössä menettelyohje toimenpiteistä työsuhteen päättyessä.	Organisaatiossa on käytössä menettelyohje toimenpiteistä työsuhteen päättyessä.	Organisaatiossa on käytössä menettelyohje toimenpiteistä työsuhteen päättyessä.	Organisaatiossa on käytössä menettelyohje toimenpiteistä työsuhteen päättyessä.	Perustelu: Oikean toimintatavan noudattaminen jouduttaessa päättämään työsuhde on tärkeä turvallisuuskysymys.	
P 606.0 **Miten vierailukäytäntö on järjestetty?**	Organisaatiossa on käytössä toimenpideohjeet vieraiden hallitsemiseksi organisaation eri tiloissa.	Organisaatiossa on käytössä toimenpideohjeet vieraiden hallitsemiseksi organisaation eri tiloissa.	Organisaatiossa on käytössä toimenpideohjeet vieraiden hallitsemiseksi organisaation eri tiloissa.	Organisaatiossa on käytössä toimenpideohjeet vieraiden hallitsemiseksi organisaation eri tiloissa.	Pyydetään nähdä vierailuja koskevat ohjeet.	

SUOSITUKSET JA VAATIMUKSET

F

OSA-ALUE

Fyysinen turvallisuus

Sisällys

Johdanto

Fyysisen turvallisuuden auditointikriteeristö keskittyy toimitilaturvallisuuteen, mutta huomioi tarvittavissa määrin myös muita fyysisen turvallisuuden elementtejä.

Kriteeristöosion perusajatus on suojata sensitiivisen tai suojattavan tiedon salassa pysyminen kuoriajatteluun pohjautuen siten, että pääsy edellä mainittuihin tietoihin estetään mahdollisimman varhaisessa vaiheessa ja tiukennetaan suojaamisvaatimuksia sitä mukaa, mitä lähemmäs fyysisesti tietoon päästään (turvallisuusvyöhykemalli). Tärkeimpiä suojattavia kohteita ovat usein tietojärjestelmien kriittisiä osia sisältävät laitetilat.

Turvallisuusauditointikriteeristön ensimmäisen ja toisen version keskinäisiä eroja sisältävät kysymykset/vaatimukset on merkitty kysymyssarakkeeseen tähtimerkillä (*).

Alueen turvallisuus, osa-alue F100

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
F 101.0 **Onko pysäköinnissä tarpeellista huomioida suojautuminen lähialueelta toteutettavalta elektroniselta tiedustelulta?**	Tiestölle ja pysäköinnille ei vaatimuksia.	Tiestölle ja pysäköinnille ei vaatimuksia.	Pysäköintialueen tulee sijaita riittävän kaukana tai se on suojattu siten, että sieltä ei voi suorittaa hajasäteilyyn perustuvaa tiedustelua. Pysäköintialueen tulee olla valvottu siten, että sinne ei voi viedä elektronisia tiedustelulaitteita. Pysäköintialue voi olla myös katveessa, jolloin suora elektroninen tiedustelu ei ole mahdollista.	Tiestölle ja pysäköinnille ei erityissuosituksia.	Jos tilaa tai laitetta ei ole suojattu, tulee huolehtia siitä että pysäköintialueelta ei voida suorittaa ko. tiedustelua.	
F 102.0 **Onko lastaus- ja purkualueella tarpeellista huomioida suojautuminen lähialueelta toteutettavalta elektroniselta tiedustelulta?**	Lastaus- ja purkualueille ei vaatimuksia.	Lastaus- ja purkualueille ei vaatimuksia.	Lastaus ja purkualue tulee sijaita riittävän kaukana tai se on suojattu siten, että sieltä ei voi suorittaa hajasäteilyyn perustuvaa tiedustelua. Lastaus ja purkualueen tulee olla valvottu siten, että sinne ei voi viedä elektronisia tiedustelulaitteita. Lastaus ja purkualue voi olla myös katveessa, jolloin suora elektroninen tiedustelu ei ole mahdollista.	Lastaus- ja purkualueille ei erityissuosituksia.	Jos tilaa tai laitetta ei ole suojattu, tulee huolehtia siitä että lastaus- ja purkualueelta ei voida suorittaa ko. tiedustelua.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/ lisätietoa	Auditointitulos: OK/ poikkeama
F 103.0 **Onko tarpeellista rajoittaa kiinteistön alueella liikkumista aidoilla, porteilla ja ajoesteillä?**	Aidoille, porteille ja ajoesteille ei rakenteellisia vaatimuksia. Jos aidalla parannetaan heikkoja isoja ajoneuvo-ovia, tulee aidan täyttää seuraavat vähimmäisvaatimukset (uusi aita): - sinkitystä teräslangasta tehty metalliverkkoaita, h= min 2,25m silmäkoko max 40*40 mm, langan paksuus min 3,0 mm, etäisyys maasta max 0,05m - aidan yläosaan min kaksi päällekkäistä piikkilankaa (sinkitty teräs min 2*1,6mm), verkon alareunan ja maan väliin yksi piikkilanka (sinkitty teräs min 2*1,6mm) - koko aitarakenteen korkeus min 2,40m, pylväät halkaisijaltaan 70mm:n alumiiniprofiilia (tai vast.), pylväiden väli max 3,00m -metalliverkon kiinnitysruuvien (vast) tulee olla aidalla suljetun alueen sisäpuolella. Porttien tulee olla kulunvalvottuja.	Aidoille, porteille ja ajoesteille ei rakenteellisia vaatimuksia. Jos aidalla parannetaan heikkoja isoja ajoneuvo-ovia, tulee aidan täyttää seuraavat vähimmäisvaatimukset (uusi aita): - sinkitystä teräslangasta tehty metalliverkkoaita, h= min 2,25m silmäkoko max 40*40 mm, langan paksuus min 3,0 mm, etäisyys maasta max 0,05m - aidan yläosaan min kaksi päällekkäistä piikkilankaa (sinkitty teräs min 2*1,6mm), verkon alareunan ja maan väliin yksi piikkilanka (sinkitty teräs min 2*1,6mm) - koko aitarakenteen korkeus min 2,40m, pylväät halkaisijaltaan 70mm:n alumiiniprofiilia (tai vast.), pylväiden väli max 3,00m -metalliverkon kiinnitysruuvien (vast) tulee olla aidalla suljetun alueen sisäpuolella. Porttien tulee olla kulunvalvottuja.	Aidoille, porteille ja ajoesteille ei rakenteellisia vaatimuksia. Jos aidalla parannetaan heikkoja isoja ajoneuvo-ovia, tulee aidan täyttää seuraavat vähimmäisvaatimukset (uusi aita): - sinkitystä teräslangasta tehty metalliverkkoaita, h= min 2,25m silmäkoko max 40*40 mm, langan paksuus min 3,0 mm, etäisyys maasta max 0,05m - aidan yläosaan min kaksi päällekkäistä piikkilankaa (sinkitty teräs min 2*1,6mm), verkon alareunan ja maan väliin yksi piikkilanka (sinkitty teräs min 2*1,6mm) - koko aitarakenteen korkeus min 2,40m, pylväät halkaisijaltaan 70mm:n alumiiniprofiilia (tai vast.), pylväiden väli max 3,00m -metalliverkon kiinnitysruuvien (vast) tulee olla aidalla suljetun alueen sisäpuolella. Porttien tulee olla kulunvalvottuja.	Aidoille, porteille ja ajoesteille ei rakenteellisia suosituksia. Jos aidalla parannetaan heikkoja isoja ajoneuvo-ovia, kannattaa aidan täyttää vähintään seuraavat suositukset (uusi aita): - sinkitystä teräslangasta tehty metalliverkkoaita, h= min 2,25m silmäkoko max 40*40 mm, langan paksuus min 3,0 mm, etäisyys maasta max 0,05m - aidan yläosaan min kaksi päällekkäistä piikkilankaa (sinkitty teräs min 2*1,6mm), verkon alareunan ja maan väliin yksi piikkilanka (sinkitty teräs min 2*1,6mm) - koko aitarakenteen korkeus min 2,40m, pylväät halkaisijaltaan 70mm:n alumiiniprofiilia (tai vast.), pylväiden väli max 3,00m -metalliverkon kiinnitysruuvien (vast) tulee olla aidalla suljetun alueen sisäpuolella. Porttien tulee olla kulunvalvottuja.		
F 104.0 **Pystytäänkö videovalvonnalla seuraamaan alueella liikkumista?**	Huomioitava mahdollisen alueen kameravalvontajärjestelmän vaatima riittävä valaistus myös pimeällä. Ei muita erityisvaatimuksia.	Huomioitava mahdollisen alueen kameravalvontajärjestelmän vaatima riittävä valaistus myös pimeällä. Ei muita erityisvaatimuksia.	Huomioitava mahdollisen alueen kameravalvontajärjestelmän vaatima riittävä valaistus myös pimeällä. Ei muita erityisvaatimuksia.	Huomioitava mahdollisen alueen kameravalvontajärjestelmän vaatima riittävä valaistus myös pimeällä. Ei muita erityissuosituksia.		

Rakenteellinen turvallisuus, osa-alue F200

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
F 201.0 **Mitä materiaalia tilan seinät, katto ja lattia ovat?** * **Katso lisätietoja liitteen 1 kohdasta F201.0**	Kuoren rakenne normaalia toimistorakennetta.	Tilan seinät, katto ja lattia on oltava betonia, terästä, tiiltä tai vahvaa puuta. Puutteelliset rakenteet on vahvennettava. Seinäelementtejä ei saa voida irrottaa kokonaisina tilan ulkopuolelta.	Tilan seinät, katto ja lattia on oltava betonia, terästä, tiiltä tai vahvaa puuta. Puutteelliset rakenteet on vahvennettava. Seinäelementtejä ei saa voida irrottaa kokonaisina tilan ulkopuolelta.	Tilanteen mukaiset rakenteet.		
F 202.0 **Onko tilassa (tiloissa) alle 4 metrin korkeudessa ikkunoita?** *Korkean tason (II) kysymys:* *Onko tilassa (tiloissa) yli 4 metrin korkeudessa ikkunoita?* *	Ikkunat on varustettava näköestesuojalla, joilla peitetään suora näkyvyys tilaan turva-alueen ulkopuolelta.	Maatason (alle 4 m) ikkunat on suojattava turvalasilla (SFS-EN 356 / P6B), tai sitä turvallisemmalla järjestelyllä. Lisäksi huomioitava karmin kiinnitys ympäröivään seinään, saranoiden ja lukituksen rakenne.	Maatasossa (alle 4m) sijaitsevassa tilassa ei saa olla ikkunoita. Maatason yläpuolella (yli 4 m) ikkunat on suojattava turvalasilla (SFS-EN 356 / P6B), tai sitä turvallisemmalla järjestelyllä, joka on murronkestävä, eikä välitä äänivärähtelyjä uloimpaan lasiin. Lisäksi huomioitava karmin kiinnitys ympäröivään seinään, saranoiden ja lukituksen rakenne. Jos tietoteknisiä laitteita ei ole Tempest-suojattu, voidaan tilan rakenteita muuttamalla saavuttaa vastaa suojaus. (Jos alue ei ole kulunvalvottu väh. 300metrin etäisyydeltä kohteesta, tulee ikkunoiden ja tilan olla Tempest-suojattuja)	Ikkunoiden on syytä olla suojattuja siten, että niitä ei saa rikkomatta ulkopuolelta auki.	Heikoista ikkuna-aukoista on helpompi murtautua kuin ovesta. Ikkunapuiterakenteet: kysy tarvittaessa ohjausta vastuuviranomaisilta.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
F 203.0 **Onko tilassa (tiloissa) kattoikkunoita?** *	Kattoikkunat/luukut oltava lukitut.	Kattoikkunat (tai kattotasanteiden tasolla olevat ikkunat) on suojattava turvalasilla (SFS-EN 356 / P6B), tai sitä turvallisemmalla järjestelyllä. Lisäksi huomioitava karmin kiinnitys ympäröivään seinään, saranoiden ja lukituksen rakenne.	Kattoikkunoita (tai kattotasanteita) ei saa olla II –tason tiloissa.	Kattoikkunoiden/ luukkujen on syytä olla lukitut ja ne on suositeltavaa suojata turvakalvolla P1A (SFSEN 356) tai sitä turvallisemmalla järjestelyllä.	Heikoista ikkuna-aukoista on helpompi murtautua kuin ovesta. Ikkunapuiterakenteet: kysy tarvittaessa ohjausta vastuuviranomaisilta.	
F 204.0 **Onko tilan kuoressa muita aukkoja, joita voitaisiin käyttää tunkeutumiseen?**	Ei vaatimuksia.	Tilan kuoressa ei saa olla muita aukkoja, kuin tunkeutumisen ilmaisujärjestelmillä valvottuja ovia, ikkunoita tai savunpoisto- ja ilmanottoaukkoja. Aukot voidaan sulkea kalteroinnilla tai vahvoilla terässäleiköillä.	Tilan kuoressa ei saa olla muita aukkoja, kuin tunkeutumisen ilmaisujärjestelmillä valvottuja ovia, ikkunoita tai savunpoistoja ilmanottoaukkoja. Aukot on suljettava kalteroinnilla tai vahvoilla terässäleiköillä.	Tilan kuoressa ei pidä olla muita kuin lukittuja aukkoja.	IV- ja kaapeli-kanavia, savunpoisto- ja ilmanottoaukkoja voidaan käyttää tunkeutumiseen.	
F 205.0 **Minkälaiset ovat tilaan johtavat ovet?** * **Katso lisätietoja liitteestä 1, kohdasta F205.0**	Ovien äänieristyksen tulee olla sellainen, että asiattomat eivät pääse kuulemaan työtilassa käytyjä keskusteluja.	Ovien on täytettävä SFS EN 1627-luokka 3:n murronkestoluokan vaatimukset. Ovien rakenteita tarkastettaessa on lisäksi kiinnitettävä huomiota karmin rakenteeseen, oven ja karmin välykseen, sekä karmien kiinnitykseen seinärakenteeseen. Karmirakenteen on estettävä kiinnitysruuvien sahaaminen ulkoapäin. Välys oven ja karmin välillä max 2 mm. Oven läpinäkeminen suojattavaan tilaan tulee estää.	Ovien on täytettävä SFS EN 1627-luokka 3:n murronkestoluokan vaatimukset. Ovien rakenteita tarkastettaessa on lisäksi kiinnitettävä huomiota karmin rakenteeseen, oven ja karmin välykseen, sekä karmien kiinnitykseen seinärakenteeseen. Karmirakenteen on estettävä kiinnitysruuvien sahaaminen ulkoapäin. Välys oven ja karmin välillä max 2 mm. Oven läpinäkeminen suojattavaan tilaan tulee estää.	Ei erityissuosituksia.	Kaksilehtisten ovien osalta omat vaatimukset: kysy yksityiskohdat valtionhallinnon vastuuviranomaisilta.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
F 206.0 **Onko tilassa suuria, esim. halliovia?** *	Ovien äänieristyksen tulee olla sellainen, että asiattomat eivät pääse kuulemaan työtilassa käytyjä keskusteluja.	Mikäli ovia ei voida rakentaa em. periaatteella esimerkiksi niiden suuren koon takia, on kyseisen aukon teknilliseen suojaamiseen kiinnitettävä erityistä huomiota. Teräspuomien on estettävä ajoneuvon läpiajoa. Hyväksytyt rullakalterit toimivat murtosuojana.	Mikäli ovia ei voida rakentaa em. periaatteella esimerkiksi niiden suuren koon takia, on kyseisen aukon teknilliseen suojaamiseen kiinnitettävä erityistä huomiota. Teräspuomien on estettävä ajoneuvon läpiajoa. Hyväksytyt rullakalterit toimivat murtosuojana.	Ei erityissuosituksia.	Nostettavat halliovet ovat usein murtosuojauksellisesti heikkoja.	
F 207.0 **Miten hyvin ääni liikkuu naapuritiloihin?** *	Tilan äänieristyksen tulee olla sellainen, että asiattomat eivät pääse kuulemaan työtilassa normaaliäänellä käytyjä keskusteluja.	Tilan äänieristyksen tulee olla sellainen, että tilasta ei suoranaisesti johdu ääntä ympäröiviin huonetiloihin esimerkiksi kaapelikourujen tai ilmastointikotelointien kautta. Kaapelikouruihin äänieristemateriaalin lisääminen, ilmastointikanaviin ääniloukut.	Tilan äänieristyksen tulee olla sellainen, että tilasta ei suoranaisesti johdu ääntä ympäröiviin huonetiloihin esimerkiksi kaapelikourujen tai ilmastointikotelointien kautta. Kaapelikouruihin äänieristemateriaalin lisääminen, ilmastointikanaviin ääniloukut.	Ei erityissuosituksia.	Suojattavasta tilasta ei saa välittyä puhetta suojaamattomiin naapuritiloihin.	
F 208.0 **Onko tilassa tiedon säilyttämistä varten kassakaappi tai holvi?** *	Tilassa kassakaappi (ei standardivaatimusta), tai jos suojaustason IV tietoaineistoa säilytetään lukitussa kaapissa, tulee tila olla valvottu rikosilmoitinjärjestelmällä (rikosilmoitinkeskuksen taso oltava vähintään 2-luokka FK). Ovet ja tilat valvottava.	Tilassa kassakaappi (vähintään Euro II SFS-EN 1143-1) tai holvi (vähintään Euro IV).	Tilassa kassakaappi (vähintään Euro II SFS-EN 1143-1) tai holvi (vähintään Euro IV).	Tilassa kassakaappi (vähintään Euro I SFS-EN 1143-1) tai jos luokiteltua tietoaineistoa säilytetään lukitussa kaapissa, tulee tila olla valvottu rikosilmoitinjärjestelmällä (rikosilmoitinkeskuksen taso oltava vähintään 2-luokka FK). Ovet ja tilat valvottava.	Tietoa tulee säilyttää lukitussa kaapissa tai holvissa pidemmän vasteajan mahdollistamiseksi.	
F 209.0 **Miten pääsyoikeudet on hallinnoitu?**	Pääsyoikeudet ko. tiloihin myöntää nimetty vastuuhenkilö yrityksessä.	Pääsyoikeudet ko. tiloihin myöntää nimetty vastuuhenkilö yrityksessä.	Pääsyoikeudet ko. tiloihin myöntää nimetty vastuuhenkilö yrityksessä.	Pääsyoikeudet ko. tiloihin myöntää nimetty vastuuhenkilö yrityksessä.	Tiloihin liittyvien pääsyoikeuksien tulee olla prosessissa yksiselitteisesti vastuutettu.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
F 209.1 **Hallitaanko kaikkien käyttäjien pääsy- ja käyttöoikeuksia hyvän tiedonhallintatavan mukaisesti?** *Lisäkysymys:* *Miten on varmistuttu siitä, että käyttäjät voivat käsitellä vain niitä tietoja, joihin heillä on käsittelyoikeus?* **(ex I 201.0)** **Ks. lisätietoja liitteestä 1 (F209.1)**	1) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö. 2) Järjestelmän käyttäjistä on olemassa lista. 3) Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin verkkoihin, tietoihin ja järjestelmiin. 4) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. 5) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu. 6) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen. 7) Käyttö- ja pääsyoikeuksien muutokset välittyvät sekä fyysiseen että loogiseen pääsyyn ja käyttöön. 8) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti. 9) Yhteistyökumppanien/muiden ulkopuolisten oikeutetusta henkilöstöstä on olemassa oma rekisterinsä. 10) Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen).	1) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö. 2) Järjestelmän käyttäjistä on olemassa lista. 3) Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin verkkoihin, tietoihin ja järjestelmiin. 4) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. 5) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu. 6) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen. 7) Käyttö- ja pääsyoikeuksien muutokset välittyvät sekä fyysiseen että loogiseen pääsyyn ja käyttöön. 8) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti. 9) Yhteistyökumppanien/muiden ulkopuolisten oikeutetusta henkilöstöstä on olemassa oma rekisterinsä. 10) Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen).	1) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö. 2) Järjestelmän käyttäjistä on olemassa lista. 3) Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin verkkoihin, tietoihin ja järjestelmiin. 4) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. 5) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu. 6) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen. 7) Käyttö- ja pääsyoikeuksien muutokset välittyvät sekä fyysiseen että loogiseen pääsyyn ja käyttöön. 8) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti. 9) Yhteistyökumppanien/muiden ulkopuolisten oikeutetusta henkilöstöstä on olemassa oma rekisterinsä. 10) Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen).	1) Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. 2) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. 3) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu. 4) On olemassa selkeä ja toimiva tapa muutosten ilmoittamiseen ja tarvittavien muutosten tekemisiin. 5) Käyttö- ja pääsyoikeuksien muutokset välittyvät sekä fyysiseen että loogiseen pääsyyn ja käyttöön. 6) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö.	ISO/IEC 27002 11.1, ISO/IEC 27002 11.1.1, ISO/IEC 27002 11.2.4, ISO/IEC 27002 11.4.1, ISO/IEC 27002 11.6.1, ISO/IEC 27002 8.3.3, COBIT 4.1 PO7, Kansallisen turvallisuusviranomaisen "Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje", VAHTI 4/2002, VAHTI 8/2006, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 liite IV, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf, http://www.sans.org/critical-security-controls/control.php?id=8, http://www.sans.org/critical-security-controls/control.php?id=11	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
F 209.2 **Pääkysymys:** **Millaisia menettelytapoja organisaatiolla on tunnistaa ulkopuoliset työntekijät sekä vierailijat?** *Lisäkysymys:* *Onko henkilöstö ohjeistettu vieraiden isännöintiä varten?* (ex I 207.0)	1) Henkilöstö on ohjeistettu vierailijoiden isännöintiä varten. 2) Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita. 3) Kaikki urakoitsijat, ulkopuoliset käyttäjät, huoltohenkilökunta sekä vierailijat käyttävät jonkinlaista näkyvää tunnistetta (esim. henkilökortti/vierailijakortti). 4) Henkilökunta on ohjeistettu reagoimaan ilman henkilökorttia (tai vastaavaa muuta näkyvää tunnistetta) liikkuviin henkilöihin. 5) Vieraat eivät koskaan jää valvomatta tiloihin ilman isäntää tai hänen edustajaansa.	1) Henkilöstö on ohjeistettu vierailijoiden isännöintiä varten. 2) Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita. 3) Kaikki urakoitsijat, ulkopuoliset käyttäjät, huoltohenkilökunta sekä vierailijat käyttävät jonkinlaista näkyvää tunnistetta (esim. henkilökortti/vierailijakortti). 4) Henkilökunta on ohjeistettu reagoimaan ilman henkilökorttia (tai vastaavaa muuta näkyvää tunnistetta) liikkuviin henkilöihin. 5) Vieraat eivät koskaan jää valvomatta tiloihin ilman isäntää tai hänen edustajaansa.	1) Henkilöstö on ohjeistettu vierailijoiden isännöintiä varten. 2) Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita. 3) Kaikki urakoitsijat, ulkopuoliset käyttäjät, huoltohenkilökunta sekä vierailijat käyttävät jonkinlaista näkyvää tunnistetta (esim. henkilökortti/vierailijakortti). 4) Henkilökunta on ohjeistettu reagoimaan ilman henkilökorttia (tai vastaavaa muuta näkyvää tunnistetta) liikkuviin henkilöihin. 5) Vieraat eivät koskaan jää valvomatta tiloihin ilman isäntää tai hänen edustajaansa.	1) Henkilöstö on ohjeistettu vierailijoiden isännöintiä varten.	ISO/IEC 27002 9.1.2, PCI DSS 9.2, PCI DSS 9.3, VAHTI 8/2006 Näkyvät tunnisteet eivät tarpeen jos organisaatiossa työskentelee vain muutama henkilö, jotka varmasti tuntevat toisensa ja toistensa työsuhteiden keston. Vieraat voivat jäädä valvomatta julkisiin tiloihin.	
F 210.0 **Minkälainen tilan lukitus on?**	Tilan lukituksen on oltava kunnossa. Tila on lukittava aina, kun se ei ole miehitetty. Käyttölukko vyöhykkeen rajalla FK:n varmuusluokka 3.	Tilan lukituksen on oltava kunnossa. Tilaan johtavat kulkuaukot on oltava aina lukittuina. Käyttölukko vyöhykkeen rajalla FK:n varmuusluokka 3. Tämän lisäksi vyöhykkeen rajalla varmuuslukko, varmuusluokka 4. Vyöhykkeen sisällä käyttölukko, FK:n varmuusluokka 3.	Tilan lukituksen on oltava kunnossa. Tila on lukittava aina. Käyttölukko vyöhykkeen rajalla FK:n varmuus-luokka 3. Tämän lisäksi vyöhykkeen rajalla varmuuslukko, varmuusluokka 4. Vyöhykkeen sisällä käyttölukko, FK:n varmuusluokka 3.	Tilan lukituksen on oltava kunnossa. Tila on lukittava aina, kun se ei ole miehitetty. Käyttölukko vyöhykkeen rajalla FK:n varmuusluokka 3.	Lukot on luokiteltu eri tasoihin murtosuojan perusteella.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
F 211.0 **Miten (mekaanisten) avainten hallinta on järjestetty?**	Avainten / kulkuoikeuksien hallinta on oltava kunnossa. Asiaa hoitaa vastuuhenkilö ja hänellä on luettelo jaetuista avaimista, tilan lukostokaavio ja avainkortti.	Avainten / kulkuoikeuksien hallinta on oltava kunnossa. Asiaa hoitaa vastuuhenkilö ja hänellä on luettelo jaetuista avaimista, tilan lukostokaavio ja avainkortti.	Avainten / kulkuoikeuksien hallinta on oltava kunnossa. Asiaa hoitaa vastuuhenkilö ja hänellä on luettelo jaetuista avaimista, tilan lukostokaavio ja avainkortti.	Avainten / kulkuoikeuksien hallinta on oltava kunnossa. Asiaa hoitaa vastuuhenkilö ja hänellä on luettelo jaetuista avaimista, tilan lukostokaavio ja avainkortti.	Tilan hallinnan vuoksi on tarkastettava myös ylimääräisten avainten säilytys, sekä lisäavainten hallittu teettäminen.	
F 212.0 **Kenellä suojattavaan tilaan on avaimia?**	Vain nimetyillä saa olla avaimet / kulkuoikeudet suojattuihin työskentelytiloihin.	Vain nimetyillä saa olla avaimet / kulkuoikeudet suojattuihin työskentelytiloihin.	Vain nimetyillä saa olla avaimet / kulkuoikeudet suojattuihin työskentelytiloihin.	Vain nimetyillä saa olla avaimet / kulkuoikeudet suojattuihin työskentelytiloihin.	Tilan hallinnan vuoksi on aina tiedettävä kenellä avaimia suojattavaan tilaan on.	
F 213.0 **Mihin tiloihin yleisavaimella pääsee?**	Ei vaatimuksia.	Suojaustason III tilaan ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. III –tason yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos sidosryhmän tiloista on kielletty.	Suojaustason II tilaan ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. II –tason yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos sidosryhmän tiloista on kielletty.	Ei erityissuosituksia.	Yleisavaimella ei pääse suojattuun tilaan.	
F 214.0 **Onko vartiointi- ja kiinteistönhoitohenkilöstölle jaettu avaimia suojattuun tilaan?**	Ei vaatimuksia.	Vartiointi- ja kiinteistönhoitohenkilöstölle jaettavat avaimet tulee olla sinetöitynä poikkeuksellisien tilanteiden hoitamista varten.	Vartiointi- ja kiinteistönhoitohenkilöstölle jaettavat avaimet tulee olla sinetöitynä poikkeuksellisien tilanteiden hoitamista varten. Hälytystilanteissa II –tason tilaan edellytetään saapuvan kaksi henkilöä samanaikaisesti.	Ei erityissuosituksia.	Vartiointi- ja kiinteistönhoitohenkilöstöllä ei saa olla hallitsematonta pääsyä suojattavaan tilaan.	
F 215.0 **Miten tilan huoltotoimenpiteet on ohjeistettu tapahtuvaksi?**	Ei vaatimuksia.	Tilaan liittyvät huoltotoimenpiteet on toteutettava hankkeeseen hyväksytyn henkilön valvonnassa. III -tasoon suojattavan tietoaineiston käsittely on huoltotöiden aikana kielletty ko. tilassa.	Tilaan liittyvät huoltotoimenpiteet on toteutettava hankkeeseen hyväksytyn henkilön valvonnassa. II -tasoon suojattavan tietoaineiston käsittely on huoltotöiden aikana kielletty ko. tilassa.	Ei erityissuosituksia.		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
F 216.0 **Tapahtuvatko laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet vain valvottuina?** **(ex I 302.0)**	Tilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat vain suojaustasolle hyväksytyn henkilön toimesta tai oman henkilökunnan valvonnassa.	Perustason vaatimusten lisäksi: Suojaustasoon III suojattavan aineiston käsittely on huoltotöiden aikana kielletty ko. tilassa.	Perustason vaatimusten lisäksi: Suojaustasoon II suojattavan aineiston käsittely on huoltotöiden aikana kielletty ko. tilassa.	Laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat riskienarvioinnin mukaisesti. Riskienarvioinnissa voidaan päätyä hyväksymään toimet esim. vain oman henkilöstön valvomana, sähköisellä tallentavalla kulunvalvonnalla (esim. sähköinen kulkuavain ja koodi) järjestettynä, ja/tai sopimuksin suojattuna.	VAHTI 8/2006, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf	
F 217.0 **Miten on varauduttu salakuunteluun, hajasäteilyyn ja vastaaviin uhkiin?** **(ex I303.0)** **Katso lisätietoja liitteestä 1 (F217.0)**	1) Tilojen äänieristyksen täytyy olla riittävä, jottei normaali puheääni kuulu sellaisen tilan ulkopuolelle, jossa keskustellaan suojattavista asioista. 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakkakopit, lounasravintolat, jne.) ei saa keskustella suojattavista asioista. 3) Huoneen ovet ja ikkunat on pidettävä kiinni keskusteltaessa suojattavista asioista.	Perustason vaatimusten lisäksi: 1) Tilassa ei käytetä mitään sellaisia elektronisia laitteita (kannettavat tietokoneet, matkapuhelimet, jne.) joiden käyttö on erikseen kielletty. 2) Tapauskohtaisesti arvioidaan tarve järjestelmien ja/tai tilan suojaamiseksi lähtevältä hajasäteilyltä (TEMPEST). 3) Tilan äänieristys on sellainen, että tilasta ei suoranaisesti johdu ääntä ympäröiviin huonetiloihin esimerkiksi kaapelikourujen tai ilmastointikotelointien kautta.	Korotetun tason vaatimusten lisäksi: 1) Tilaan ei saa viedä mitään sellaisia elektronisia laitteita (kannettavat tietokoneet, matkapuhelimet, jne.) jotka eivät ole tilaan erikseen hyväksyttyjä. 2) Tapauskohtaisesti arvioidaan tarve viranomaisen tekemälle tarkastukselle salakuuntelulaitteiden (ja vastaavien) varalta. 3) Tapauskohtaisesti arvioidaan tarve EMP-/HPM-suojaukselle.	1) Tilojen äänieristyksen täytyy olla riittävä, jottei normaali puheääni kuulu sellaisen tilan ulkopuolelle, jossa keskustellaan suojattavista asioista. 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakkakopit, lounasravintolat, jne.) ei saa keskustella suojattavista asioista.	Kansallisen turvallisuus viranomaisen “Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”, VAHTI 8/2006, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 10. artikla, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
F 218.0 **Pääkysymys:** **Onko LVIS-järjestelyt varmistettu niin, että ne vastaavat organisaation toimintavaatimuksia?** *Lisäkysymys:* *Ovatko organisaation kriittiset laitteistot häiriöttömän sähkönsyötön (UPS) piirissä?* **(ex I 304.0)** **Katso lisätietoja liitteestä 1 (F218.0)**	1) LVIS-järjestelyt on varmistettu toimintavaatimusten mukaisesti. 2) Kriittiset laitteistot on tunnistettu ja varmennettu toimintavaatimusten mukaisesti.	1) LVIS-järjestelyt on varmistettu toimintavaatimusten mukaisesti. 2) Kriittiset laitteistot on tunnistettu ja varmennettu toimintavaatimusten mukaisesti.	1) LVIS-järjestelyt on varmistettu toimintavaatimusten mukaisesti. 2) Kriittiset laitteistot on tunnistettu ja varmennettu toimintavaatimusten mukaisesti.	1) LVIS-järjestelyt on varmistettu toimintavaatimusten mukaisesti. 2) Kriittiset laitteistot on tunnistettu ja varmennettu toimintavaatimusten mukaisesti.	ISO/IEC 27002 9.1.4, COBIT 4.1 DS12, VAHTI 8/2006, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	
F 219.0 **Ovatko näyttöpäätteet asetetut siten, ettei suojattavaa tietoa paljastu ohikulkijoille tai muille asiattomille?** **(ex I 305.0)**	1) Näyttöpäätteet on asetettu harkiten siten, ettei tieto paljastu asiattomille. 2) Kannettavissa tietokoneissa on sivusta katselun estävä näyttösuoja.	Perustason vaatimusten lisäksi: Tilaan ei saa olla näköyhteyttä ulkopuolelta silloin, kun tilassa käsitellään suojaustason III aineistoa.	Perustason vaatimusten lisäksi: Tilaan ei saa olla näköyhteyttä ulkopuolelta silloin, kun tilassa käsitellään suojaustason II aineistoa.	Näyttöpäätteet on asetettu harkiten siten, ettei tieto paljastu asiattomille.	Kansallisen turvallisuusviranomaisen “Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”, VAHTI 8/2006. Näyttösuojaa ei vaadita, mikäli kannattavaa tietokonetta käytetään vain suojatussa tilassa vastaavasti kuin työaseman näyttöäkin.	

Turvallisuustekniset järjestelmät, osa-alue F300

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
F 301.0 **Onko tilassa rikosilmoitinjärjestelmä?**	Tila on valvottu rikosilmoitinjärjestelmällä (rikosilmoitinkeskuksen taso oltava vähintään 2-luokka FK). Ovet ja tilat valvottava. Järjestelmä vaaditaan, jos suojaustason IV luokiteltua aineistoa säilytetään tavallisessa lukitussa kaapissa/laatikossa.	Tilassa rikosilmoitinjärjestelmä (vähintään 3-luokka). Ovet, aukot, ikkunat ja tilat valvottava.	Tilassa rikosilmoitinjärjestelmä (vähintään 3-luokka). Ovet, aukot, ikkunat, tilat ja kuori valvottava. Vahvistettuun seinärakenteeseen lisätään joko runkoääni- tai inertiailmaisimet.	Tila on valvottu rikosilmoitinjärjestelmällä (rikosilmoitinkeskuksen taso oltava vähintään 2-luokka FK). Ovia ja tiloja valvotaan. Järjestelmää tarvitaan, jos suojaustason IV luokiteltua aineistoa säilytetään tavallisessa lukitussa kaapissa/ laatikossa.	Rikosilmoitinjärjestelmä antaa ilmaisun ja käynnistää vastatoimenpiteet.	
F 302.0 **Onko tilassa kulunvalvontajärjestelmää?**	Ei vaatimuksia.	Tila on valvottava kulunvalvonnalla siten, että vain hankkeeseen tai projektiin oikeutetuilla henkilöillä on pääsy tilaan, ja että tilaan kulku voidaan myöhemmin todentaa.	Tila on valvottava kulunvalvonnalla siten, että vain hankkeeseen tai projektiin oikeutetuilla henkilöillä on pääsy tilaan, ja että tilaan kulku voidaan myöhemmin todentaa jokaisen henkilön osalta. Kulunvalvonnassa on käytettävä sisään mentäessä kaksoistunnistusta. Poistuttaessa tilasta tulee käyttää kulunvalvontatunnistetta.	Ei erityissuosituksia.	Suojattuun tilaan kulku voidaan myöhemmin todentaa. Lisäkommentti tasolla II: Kaksoistunnistuksella estetään toisen henkilön tunnisteen luvaton käyttö.	
F 303.0 **Onko tilassa kameravalvontajärjestelmä?**	Ei vaatimuksia.	Ei vaatimusta kameravalvonnasta. Voidaan käyttää kehävalvonnassa heikkojen halliovien täydentäjänä.	II –tason tila on varustettava kameravalvonnalla. Kamerat on sijoitettava siten, että II –tason tietoa ei siirry kameran välityksellä. Kameravalvontatieto on tallennettava ja liitettävä rikosilmaisinjärjestelmään.	Ei erityissuosituksia.	Palvelintilan kameravalvonnalla nostetaan oman henkilöstön kynnystä luvattomaan toimintaan. Tasolle II: Rikosilmoitinjärjestelmän antamasta hälytyksestä saadaan liipaisu tallentimelle jolloin saadaan tunkeutujasta myös tunnistuskuvaa.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	Auditointitulos: OK/ poikkeama
F 304.0 **Onko palvelintilassa kameravalvontajärjestelmä?**	Ei vaatimuksia.	Ei vaatimuksia.	Laite- ja palvelintilat on varustettava jatkuvalla kameravalvonnalla.	Ei erityissuosituksia.	Palvelintilan kameravalvonnalla nostetaan oman henkilöstön kynnystä luvattomaan toimintaan.	
F 305.0 **Onko rikosilmoitinjärjestelmä toimintakunnossa?** *	Järjestelmä on toimintakuntoinen.	Rikosilmoitinjärjestelmä ja ilmoituksensiirto testataan kerran kuukaudessa. Vartioinnin vasteajan on oltava sellainen, että kiinnijäämisriski on merkittävä ja vasteajan testaus tulee tehdä kerran vuodessa. Testaukset tulee dokumentoida.	Rikosilmoitinjärjestelmä ja ilmoituksensiirto testataan kerran kuukaudessa. Vartioinnin vasteajan on oltava sellainen, että kiinnijäämisriski on merkittävä ja vasteajan testaus tulee tehdä kerran vuodessa. Testaukset tulee dokumentoida.	Ei erityissuosituksia.	Toimimattomasta rikosilmoitinjärjestelmästä ei ole hyötyä. Vastaako vartioinnin vasteaika ja vartijan toiminta sopimusta? Liian pitkä vasteaika tai vartijan virheellinen toiminta poistaa rakenteellisella suojauksella saavutettua turvaa.	
F 306.0 **Miten kulunvalvontajärjestelmän hallinnointi on järjestetty?**	Ei vaatimuksia.	Ei vaatimuksia.	Kulunvalvontajärjestelmän hallinta voi olla ulkoistettu, jos se on hyvin hallinnoitu. Normaalin käyttäjän työasemalta tapahtuva oven avaus turvatilaan pitää olla estetty.	Ei erityissuosituksia.	Kulunvalvontajärjestelmän hallinnoija voi luoda tai poistaa turvatilan kulkutunnisteita sekä ohjata ovia etäkäyttöisesti.	
F 307.0 **Miten rikosilmoitinjärjestelmän hallinnointi on järjestetty?**	Ei vaatimuksia.	Ei vaatimuksia.	Rikosilmoitinjärjestelmän hallinta tulee olla yrityksen omassa hallinnassa.	Ei erityissuosituksia.	Rikosilmoitinjärjestelmän hallinnoija voi luoda tai poistaa turvatilan ohjaustunnisteita sekä etäkäyttöisesti ilmaisimia.	
F 308.0 **Miten LVI-automaation hallinta on järjestetty?**	Ei vaatimuksia.	Ei vaatimuksia.	Jos turvatilassa on palvelimia tai muita olosuhteelle herkkiä laitteita ei tilan LVI-järjestelmää saa ohjata etäkäyttöisesti.	Ei erityissuosituksia.	LVI-automaation etähallinnan avulla voidaan tilan olosuhdemuutoksilla vahingoittaa laitteita ja tietoa.	

OSA-ALUE

I Tietoturvallisuus

Sisällys

Johdanto

Kansallisen turvallisuusauditointikriteeristön tietoturvaosio kuvaa tietoturvallisuuden vähimmäisvaatimukset sellaisille tiedoille, joiden luottamuksellisuutta, eheyttä ja käytettävyyttä tulee suojata. Tällaisia tietoja ovat esimerkiksi yrityksen sensitiiviset tiedot (esim. tuotekehitykseen liittyvät yrityssalaisuudet) sekä viranomaisten suojattavat tai turvallisuusluokitellut tiedot. Tämän turvallisuusauditointikriteeristön muut osiot ovat looginen osa tietoturvakriteeristöä, jossa viitataankin erityisesti fyysisen turvallisuuden osioon monissa tiedon fyysiseen suojaamiseen liittyvissä vaatimuksissa. Tietoturvakriteeristötyössä on otettu mahdollisimman tarkasti huomioon valtionhallinnon tietoturvallisuusasetuksen ja tätä täydentävien ohjeiden yksityiskohtaiset linjaukset. Samoin on pyritty yhteismitallisuuteen valtiovarainministeriön johdolla toteutetun tietoturvallisuutta ja varautumista ohjeistavan aineiston suhteen.

Auditointikriteeristön tietoturvaosio on jaettu neljään sisällysluettelon mukaiseen osa-alueeseen. Osa-alueiden vaatimukset on jaettu kolmeen tasoon: perustason vaatimukset (IV), korotetun tason vaatimukset (III) ja korkean tason vaatimukset (II). Tasojen IV-II vaatimukset koskevat vain suojattavaa kohdetta.

Erikseen listatut elinkeinoelämän suositukset koskevat temaattisesti koko organisaation kohteiden turvaamista sekä tietoturvallisuuden kokonaishallintaa. Suositusten pohjalta on hyvä edetä vaatimusten täyttämiseen.

Suojattavalla kohteella tarkoitetaan suojattavaa tietoa sekä sen käsittely-ympäristöä. Suojattava kohde voi olla esimerkiksi yksittäinen tietojärjestelmä, verkon osa tai vaikka yksittäinen työhuone. Vaatimukset periytyvät ylemmille tasoille siten, että esimerkiksi II-tasolla edellytetään omien erillisvaatimusten lisäksi tasojen IV ja III vaatimusten täyttymistä.

Viranomaisten suojattavien tai turvaluokiteltujen tietojen käsittely edellyttää myös elinkeinonharjoittajalta valtionhallinnon sisäisten vaatimusten täyttämistä. Täyttämällä viranomaisten vaatimustason organisaatiolla tai sen osalla on tietoturvallisuuden osalta valmiudet suojaustasoa vastaavien tietojen tietotekniseen käsittelyyn edellyttäen, että tämän auditointikriteeristön muiden osioiden asettamat vaatimukset täyttyvät. Tietoturvakriteeristön vaatimustasoja määritettäessä on pyritty huomioimaan keskeisimmät kansainväliset vaatimukset siten, että kotimainen säädöspohja on viime kädessä määräävä tekijä.

Turvallisuusauditointikriteeristön ensimmäisen ja toisen version keskinäisiä eroja sisältävät kysymykset/vaatimukset on merkitty kysymyssarakkeeseen tähtimerkillä (*). Tietoturvallisuusosioon sisältyvien kysymysten maltillinen päivittyminen ei ole aiheuttanut kysymyksen merkitsemistä edellä mainitusti.

Osa KATAKRI:n ensimmäisen version tietoturvaosion kysymyksistä (osa-alueet I 100 – I 300) on siirretty kriteeristön muiden osien yhteyteen seuraavasti:

Aiempi kysymysnumero	Uuden sijoittelun mukainen kysymysnumero
I 101.0	A 501.1
I 102.0	A 204.0
I 103.0	A 401.1
I 104.0	A 401.2
I 105.0	A 408.0
I 106.0	A 409.0
I 107.0	A 410.0
I 108.0	A 105.1
I 109.0	A 608.0
I 201.0	F 209.1
I 202.0	P 407.0
I 203.0	P 408.0
I 204.0	A 806.0
I 205.0	A 807.0
I 206.0	A 803.1
I 207.0	F 209.2
I 301.0	POISTETTU
I 302.0	F 216.0
I 303.0	F 217.0
I 304.0	F 218.0
I 305.0	F 219.0

Tietoliikenneturvallisuus, osa-alue I400

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Aud.tulos: OK/poikkeama
I 401.0 **Onko tietoliikenneverkon rakenne turvallinen?** **Katso lisätietoosio liitteessä 1 (I 401.0)**	1) Ei-luotettuihin verkkoihin ei kytkeydytä ilman palomuuriratkaisua. Erityisesti Internet-verkon on oltava erotettu palomuurilla organisaation tietoverkoista ja -järjestelmistä. 2) Palomuuri- ja VPN-konfiguraatiot ovat organisaation tietoturvaperiaatteiden mukaisia ja dokumentoituja. (Vrt. I 403.0) 3) Tietoliikenneverkko on jaettu vyöhykkeisiin ja segmentteihin asianmukaisesti. Eri suojaustarpeen järjestelmät on sijoitettu erillisille verkkoalueille (esim. DMZ-erottelu). 4) Vyöhykkeisiinjakoperusteet on kuvattu. 5) Vyöhykkeiden välistä liikennettä valvotaan ja rajoitetaan siten, että vain luvallinen liikenne sallitaan. 6) Valvonnan ja rajoitusten periaatteet on kuvattu. 7) Työasemilla, kannettavilla tietokoneilla ja vastaavilla on käytössä (host-based) palomuuriratkaisu, myös organisaatioverkon sisällä.	1) Tietojenkäsittely-ympäristö on fyysisesti tai loogisesti erotettu ja valvottu verkko, josta ei ole suoria liittymiä alemman suojaustason verkkoihin. Viranomainen voi tapauskohtaisesti hyväksyä valvotun ja rajatun yhteyden määriteltyihin vastaavan suojaustason järjestelmiin. 2) Tiettyihin viranomaisen suojaustason III tietojärjestelmiin voidaan tuoda tietoa viranomaisen hyväksymän yhdyskäytäväratkaisun (esim. vain yksisuuntaisen liikenteen sallivan datadiodin) kautta. 3) Mikäli loppukäyttäjän työtehtävät edellyttävät pääsyä Internetiin tai muihin eri suojaustason järjestelmiin/verkkoihin, se on järjestettävä erillisellä tietokoneella, jota ei kytketä suojaustason III verkkoon. Viranomainen voi tapauskohtaisesti hyväksyä myös tietyt yhdyskäytäväratkaisut eri suojaustason järjestelmien välillä.	1) Tietojenkäsittely-ympäristö on fyysisesti erotettu ja valvottu verkko, josta ei ole liittymää muihin järjestelmiin. Viranomaisten tiedonvälitysjärjestelmissä voidaan tapauskohtaisesti hyväksyä valvottu ja rajattu yhteys määriteltyihin vastaavan turvallisuustason järjestelmiin. 2) Tiettyihin viranomaisen suojaustason II tietojärjestelmiin voidaan tuoda tietoa viranomaisen hyväksymän yhdyskäytäväratkaisun (esim. vain yksisuuntaisen liikenteen sallivan datadiodin) kautta. 3) Mikäli loppukäyttäjän työtehtävät edellyttävät pääsyä Internetiin tai muihin eri suojaustason järjestelmiin/verkkoihin, se on järjestettävä erillisellä tietokoneella, jota ei kytketä suojaustason II verkkoon. Viranomainen voi tapauskohtaisesti hyväksyä tietyt yhdyskäytäväratkaisut hyväksyttyihin suojaustason III järjestelmiin.	1) Ei-luotettuihin verkkoihin ei kytkeydytä ilman palomuuriratkaisua. Erityisesti Internetverkon on oltava erotettu palomuurilla organisaation tietoverkoista ja -järjestelmistä. 2) Palomuuri- ja VPN-konfiguraatiot ovat organisaation tietoturvaperiaatteiden mukaisia ja dokumentoituja. (Vrt. I 403.0)	ISO/IEC 27002 11.4.5, ISO/IEC 27002 11.4.6, ISO/IEC 27002 11.6.1, PCI DSS 1.1.5, PCI DSS 1.4, VAHTI 1/2001, VAHTI 2/2003, VAHTI 8/2006, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 liite IV, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Aud.tulos: OK/poikkeama
	8) Fyysinen verkko on jaettu turvavyöhykkeisiin. Käytännössä vaaditaan, että hallitun fyysisen tilan ulkopuolelle menevä liikenne salataan siirrettäessä ST IV –tason (turvallisuusluokitusmerkintä KÄYTTÖ RAJOITETTU) mukaisia tietoaineistoja (vrt. I 605.0).	4) Tietyt viranomaisen tietojärjestelmät koostuvat suuresta määrästä tietyn suojaustason tietoa ja näissä järjestelmissä asiakokonaisuus nousee luokitukseltaan usein yksittäistä tietoa korkeampaan suojaustasoluokkaan (kasautumisvaikutus, esim. suuri määrä suojaustason IV tietoa voi muodostaa yhdistettynä suojaustason III tietovarannon). Viranomainen voi tapauskohtaisesti hyväksyä rajatun ja valvotun pääsyn osaan tällaisen järjestelmän tietosisällöstä myös luokkaa alemman suojaustason hyväksytyistä järjestelmistä. Hyväksyttävä toteutus edellyttää yleisten suojausmenetelmien lisäksi muun muassa pääsyn rajaamista vain tehtävässä tarvittavaan yksittäiseen tai suppeaan osaan tietosisällöstä, havainnointi- ja torjuntakykyä poikkeavien/luvattomien käyttötapausten (esim. suuret määrät tietohakuja) varalle ja sitä, että järjestelmään tehdyistä tietohauista jää lainmukaisesti säilöttävä tallenne, josta voidaan jälkikäteen yksilöidä mm. tapahtuman (esim. tietohaku) suorittanut henkilö.	4) Tietyt viranomaisen tietojärjestelmät koostuvat suuresta määrästä tietyn suojaustason tietoa ja näissä järjestelmissä asiakokonaisuus nousee luokitukseltaan usein yksittäistä tietoa korkeampaan suojaustasoluokkaan (kasautumisvaikutus, esim. suuri määrä suojaustason III tietoa voi muodostaa yhdistettynä suojaustason II tietovarannon). Viranomainen voi tapauskohtaisesti hyväksyä rajatun ja valvotun pääsyn osaan tällaisen järjestelmän tietosisällöstä myös luokkaa alemman suojaustason hyväksytyistä järjestelmistä. Hyväksyttävä toteutus edellyttää yleisten suojausmenetelmien lisäksi muun muassa pääsyn rajaamista vain tehtävässä tarvittavaan yksittäiseen tai suppeaan osaan tietosisällöstä, havainnointi- ja torjuntakykyä poikkeavien/luvattomien käyttötapausten (esim. suuret määrät tietohakuja) varalle ja sitä, että järjestelmään tehdyistä tietohauista jää lainmukaisesti säilöttävä tallenne, josta voidaan jälkikäteen yksilöidä mm. tapahtuman (esim. tietohaku) suorittanut henkilö.				

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Aud.tulos: OK/poikkeama
I 402.0 **Pääkysymys: Ovatko palomuurien ja vastaavien liikennettä suodattavien laitteiden säännöstöt hyvien tietoturvaperiaatteiden mukaisia?** *Lisäkysymys:* *Onko varauduttu yleisimpiin verkkohyökkäyksiin?* **Katso lisätietoosio liitteessä 1 (I 402.0)**	1) Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny). Säännöstöt sallivat vain erikseen määritellyn, toiminnalle välttämättömän liikennöinnin. 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin. 3) Organisaatiopalomuurin takana sisäverkossa olevien työasemien, kannettavien tietokoneiden ja vastaavien ohjelmistopalomuurit sallivat vain erikseen määriteltyjen, toiminnalle välttämättömien ohjelmistojen/protokollien liikennöinnin. 4) Estetyt paketit kirjataan lokiin (vrt. I 504.0). Mikäli teknisesti mahdollista, kirjauksesta on voitava yksilöidä lähettäjätaho esim. MAC-osoitteen tarkkuudella. 5) Web-selailua suodatetaan toimintavaatimusten mukaisesti. 6) Yleisiin verkkohyökkäyksiin on varauduttu: a) Osoitteiden väärentäminen (spoofing) estetty. b) Liikenne, joka käyttää IP-lisämääreitä (IP options) ja erityisesti lähdereititystä (source routing), on oletuksena estetty kaikissa verkkolaitteissa.	Perustason vaatimukset soveltuen, lähinnä vyöhykkeiden sisällä ja/tai rajoilla, vrt. I 401:n määritykset. 1) Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny). Säännöstöt sallivat vain erikseen määritellyn, toiminnalle välttämättömän liikennöinnin. 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin. 3) Organisaatiopalomuurin takana sisäverkossa olevien työasemien, kannettavien tietokoneiden ja vastaavien ohjelmistopalomuurit sallivat vain erikseen määriteltyjen, toiminnalle välttämättömien ohjelmistojen/protokollien liikennöinnin. 4) Estetyt paketit kirjataan lokiin (vrt. I 504.0). Mikäli teknisesti mahdollista, kirjauksesta on voitava yksilöidä lähettäjätaho esim. MAC-osoitteen tarkkuudella. 5) Web-selailua suodatetaan toimintavaatimusten mukaisesti. 6) Yleisiin verkkohyökkäyksiin on varauduttu: a) Osoitteiden väärentäminen (spoofing) estetty. b) Liikenne, joka käyttää IP-lisämääreitä (IP options) ja erityisesti lähdereititystä (source routing), on oletuksena estetty kaikissa verkkolaitteissa.	Perustason vaatimukset soveltuen, lähinnä vyöhykkeiden sisällä ja/tai rajoilla, vrt. I 401:n määritykset. 1) Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny). Säännöstöt sallivat vain erikseen määritellyn, toiminnalle välttämättömän liikennöinnin. 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin. 3) Organisaatiopalomuurin takana sisäverkossa olevien työasemien, kannettavien tietokoneiden ja vastaavien ohjelmistopalomuurit sallivat vain erikseen määriteltyjen, toiminnalle välttämättömien ohjelmistojen/protokollien liikennöinnin. 4) Estetyt paketit kirjataan lokiin (vrt. I 504.0). Mikäli teknisesti mahdollista, kirjauksesta on voitava yksilöidä lähettäjätaho esim. MAC-osoitteen tarkkuudella. 5) Web-selailua suodatetaan toimintavaatimusten mukaisesti. 6) Yleisiin verkkohyökkäyksiin on varauduttu: a) Osoitteiden väärentäminen (spoofing) estetty. b) Liikenne, joka käyttää IP-lisämääreitä (IP options) ja erityisesti lähdereititystä (source routing), on oletuksena estetty kaikissa verkkolaitteissa.	1) Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny). 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin.	Soveltaen VAHTI 2/2003, VAHTI 8/2006, PCI DSS 1.1.5, http://www.cymru.com/Documents/bogon-list.html, RFC 2827, RFC 3704, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf, http://www.sans.org/critical-security-controls/control.php?id=5		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Aud.tulos: OK/poikkeama
	c) Proxy ARP -toiminnallisuus on estetty kaikissa verkkolaitteissa. d) Liikenne, jonka lähde- tai kohdeosoite on lähiverkon broadcast-osoite, on estetty. e) Liikenne, jonka lähde- tai kohdeosoitteena on 127.0.0.1 tai 0.0.0.0, on estetty. f) SNMP-liikenne sallitaan vain erikseen määritellyistä lähteistä. g) On määritetty mitä ICMP-liikennettä sallitaan. Erityisesti on huomioitava, että ICMP-tyypin 3 (unreachable) liikenne tulee estetyksi. h) Varattuja osoitteita (RFC 1918) käyttävä liikenne, joka joko saapuu organisaation verkon ulkopuolelta tai suuntaa sinne, on estetty. i) Palomuurit on konfiguroitu kokoamaan sirpaloituneet (fragment) paketit ennen suodatuspäätöksen tekemistä. j) Palvelunestohyökkäysten (DoS, DDoS, roskapostitulva) uhka on arvioitu ja tarpeelliset torjunta- ja ehkäisykeinot toteutettu.	c) Proxy ARP -toiminnallisuus on estetty kaikissa verkkolaitteissa. d) Liikenne, jonka lähde- tai kohdeosoite on lähiverkon broadcast-osoite, on estetty. e) Liikenne, jonka lähde- tai kohdeosoitteena on 127.0.0.1 tai 0.0.0.0, on estetty. f) SNMP-liikenne sallitaan vain erikseen määritellyistä lähteistä. g) On määritetty mitä ICMP-liikennettä sallitaan. Erityisesti on huomioitava, että ICMP-tyypin 3 (unreachable) liikenne tulee estetyksi. h) Varattuja osoitteita (RFC 1918) käyttävä liikenne, joka joko saapuu organisaation verkon ulkopuolelta tai suuntaa sinne, on estetty. i) Palomuurit on konfiguroitu kokoamaan sirpaloituneet (fragment) paketit ennen suodatuspäätöksen tekemistä. j) Palvelunestohyökkäysten (DoS, DDoS, roskapostitulva) uhka on arvioitu ja tarpeelliset torjunta- ja ehkäisykeinot toteutettu.	c) Proxy ARP -toiminnallisuus on estetty kaikissa verkkolaitteissa. d) Liikenne, jonka lähde- tai kohdeosoite on lähiverkon broadcast-osoite, on estetty. e) Liikenne, jonka lähde- tai kohdeosoitteena on 127.0.0.1 tai 0.0.0.0, on estetty. f) SNMP-liikenne sallitaan vain erikseen määritellyistä lähteistä. g) On määritetty mitä ICMP-liikennettä sallitaan. Erityisesti on huomioitava, että ICMP-tyypin 3 (unreachable) liikenne tulee estetyksi. h) Varattuja osoitteita (RFC 1918) käyttävä liikenne, joka joko saapuu organisaation verkon ulkopuolelta tai suuntaa sinne, on estetty. i) Palomuurit on konfiguroitu kokoamaan sirpaloituneet (fragment) paketit ennen suodatuspäätöksen tekemistä. j) Palvelunestohyökkäysten (DoS, DDoS, roskapostitulva) uhka on arvioitu ja tarpeelliset torjunta- ja ehkäisykeinot toteutettu.				

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Aud.tulos: OK/poikkeama
I 403.0 **Miten varmistutaan siitä, että liikennettä suodattavat tai valvovat järjestelmät toimivat halutulla tavalla?**	1) Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden suodatuslaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen. 2) Suodatussäännöt on dokumentoitu (vrt. I 401.0). 3) Palomuurien, reitittimien, IDS-järjestelmien ja muiden liikennettä suodattavien tai valvovien järjestelmien säännöstöt ja haluttu toiminta varmistetaan tarkastuksilla.	Perustason vaatimusten 1 ja 2 lisäksi: Palomuurien, reitittimien, IDS-järjestelmien ja muiden liikennettä suodattavien tai valvovien järjestelmien säännöstöt ja haluttu toiminta varmistetaan säännöllisillä tarkastuksilla.	Perustason vaatimusten 1 ja 2 lisäksi: Palomuurien, reitittimien, IDS-järjestelmien ja muiden liikennettä suodattavien tai valvovien järjestelmien säännöstöt ja haluttu toiminta varmistetaan säännöllisillä tarkastuksilla.	1) Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden suodatuslaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen. 2) Suodatussäännöt on dokumentoitu (vrt. I 401.0).	PCI DSS 1.1.6, VAHTI 2/2010:n liite 5 (TTT)		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Aud.tulos: OK/poikkeama
I 404.0 **Onko hallintayhteydet suojattu asianmukaisesti?**	1)Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua. 2)Verkon aktiivilaitteisiin sallitaan hallintayhteydenotot vain erikseen määritellyistä lähteistä tai vain fyysisesti laitteeseen kytkeytymällä.	1)Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua. 2)Verkon aktiivilaitteisiin sallitaan hallintayhteydenotot vain erikseen määritellyistä lähteistä tai vain fyysisesti laitteeseen kytkeytymällä.	1)Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua. 2)Verkon aktiivilaitteisiin sallitaan hallintayhteydenotot vain erikseen määritellyistä lähteistä tai vain fyysisesti laitteeseen kytkeytymällä.	Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua.	ISO/IEC 27002 11.1, PCI DSS 2.3, VAHTI 8/2006	Verkon aktiivilaitteilla tarkoitetaan tässä yhteydessä palomuureja, reitittimiä, kytkimiä, langattomia tukiasemia ja vastaavia laitteita/järjestelmiä. Mikäli verkkolaitteita hallitaan muuten kuin laitteeseen fyysisesti kytkeytymällä, ja mikäli hallintayhteys ei ole fyysisesti eriytetty, hallintaliikenteen tulee olla salattua. Vaatimus voidaan toteuttaa usein helpoiten siten, että estetään verkkolaitteiden hallinta telnetiä käyttäen ja käytetään hallinnassa SSH-yhteyttä. Vastaavasti vältettävä muitakin salaamattomia hallintatoteutuksia (käytettävä esim. HTTPS:ää HTTP:n sijaan webselaimella hallittavissa järjestelmissä).	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Aud.tulos: OK/poikkeama
I 405.0 **Miten verkon aktiivilaitteet on kovennettu?** *Katso lisätietoja liitteessä 1* **(I 405.0)**	Verkon aktiivilaitteet on kovennettu organisaation yhtenäisen menettelytavan mukaisesti. Käytännössä vaaditaan, että 1) oletussalasanat on vaihdettu, 2) vain tarpeellisia verkkopalveluita on päällä, 3) verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset, 4) hallinta ei ole mahdollista ilman käyttäjän tunnistamista ja todentamista, 5) Laitteistot on konfiguroitu valmistajien ja luotettujen tahojen ohjeiden mukaisesti. 6) Kytkimen työasemaportit on erotettu toisistaan ja työasemat eivät voi suoraan kommunikoida keskenään. Kytkimet eivät saa olla verkkoliikennettä kaiuttavassa toimintatilassa (HUB-toiminnallisuus). 7) Mikäli kytkimissä käytetään VTP-toimialuetta (VLAN Trunking Protocol domain), on VTP-salasana asetettu ja otettu käyttöön. 8) Kytkimissä ei käytetä oletus-VLAN:ia (tyypillisesti VLAN 1) operatiiviselle liikenteelle.	Perustason vaatimusten lisäksi: 1) Verkkolaitteiden lokeista on pystyttävä jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta. 2) Kytkimien käyttämättömät portit on poistettu käytöstä.	Perustason vaatimusten lisäksi: 1) Verkkolaitteiden lokeista on pystyttävä jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta. 2) Kytkimien käyttämättömät portit on poistettu käytöstä.	Verkon aktiivilaitteet on kovennettu organisaation yhtenäisen menettelytavan mukaisesti. Käytännössä suositellaan vähintään, että 1) oletussalasanat on vaihdettu, 2) vain tarpeellisia verkkopalveluita on päällä, 3) verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset.	ISO/IEC 27002 11.1, ISO/IEC 11.2.3, PCI DSS 2.1, PCI DSS 2.2, PCI DSS 6.1, PCI DSS 6.2, VAHTI 2/2003, VAHTI 8/2006, ISO/IEC 11.2.3, VAHTI 3/2010, http://www.sans.org/critical-security-controls/control.php?id=4		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Aud.tulos: OK/poikkeama
I 406.0 **Miten langattomia verkkoja suojataan?**	1) "Vierasverkoille", joista ei ole pääsyä organisaation sisäverkkoon, suositellaan, mutta ei vaadita salausta ja käyttäjien tunnistamista. 2) Organisaation hallinnoimien langattomien verkkojen käyttö sallitaan vain tunnistetuille ja valtuutetuille käyttäjille. 3) Liikenne salataan luotettavasti.	Langattomat verkot ovat lähtökohtaisesti kiellettyjä. Tapauskohtaisesti voidaan hyväksyä ratkaisu, jossa liikenne on turvatasolle hyväksytyllä menetelmällä salattu päästä-päähän (ei vain radiotie), ts. langatonta verkkoyhteyttä käsitellään kuin julkista verkkoa.	Langattomia verkkoja ei käytetä. Tapauskohtaisesti voidaan hyväksyä ratkaisu, jossa liikenne on turvatasolle hyväksytyllä menetelmällä salattu päästä-päähän (ei vain radiotie), ts. langatonta verkkoyhteyttä käsitellään kuin julkista verkkoa.	"Vierasverkoille", joista ei ole pääsyä organisaation sisäverkkoon, suositellaan, mutta ei vaadita salausta ja käyttäjien tunnistamista.	ISF-SOGP NW2.4, VAHTI 3/2010, http://www.sans.org/critical-security-controls/control.php?id=14	III- ja II-tasot: Riittävän turvatason käytännön toteutus on usein helpompaa langallisia yhteyksiä käyttäen.	
I 407.0 **Onko sisäverkon rakenteen näkyminen Internetiin ja muihin ei-luotettuihin verkkoihin estetty?** *Lisäkysymys:* *Onko sisäverkon rakenteen ja liikenteen tarpeeton näkyminen sisäverkossa estetty?*	1) Sisäverkoissa käytetään julkiseen verkkoon kuulumattomia, ns. privaattiosoitteita. 2) Sisäverkon rakenteen ja liikenteen tarpeeton näkyminen on estetty sisäverkossa (ks. I 402.0 ja I 405.0).	1) Sisäverkoissa käytetään julkiseen verkkoon kuulumattomia, ns. privaattiosoitteita. 2) Sisäverkon rakenteen ja liikenteen tarpeeton näkyminen on estetty sisäverkossa (ks. I 402.0 ja I 405.0).	1) Sisäverkoissa käytetään julkiseen verkkoon kuulumattomia, ns. privaattiosoitteita. 2) Sisäverkon rakenteen ja liikenteen tarpeeton näkyminen on estetty sisäverkossa (ks. I 402.0 ja I 405.0).	Sisäverkoissa käytetään julkiseen verkkoon kuulumattomia, ns. privaattiosoitteita.	PCI DSS 1.3.8, ISO/IEC 27002 12.5.4		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Aud.tulos: OK/poikkeama
I 408.0 **Pääkysymys: Miten verkkoa, järjestelmiä ja niiden käyttöä valvotaan?** *Lisäkysymys:* *Onko resurssit mitoitettu toimintavaatimusten mukaisiksi?*	1) Verkkoliikenteen normaali tila (baseline) on tiedossa. On vähintään oltava tiedossa normaalit liikennemäärät ja käytetyt protokollat verkon eri osissa. 2) Resurssit on mitoitettu siten, että kriittiset tietoliikennejärjestelmät toimivat turvallisesti myös normaaliliikenteestä poikkeavilla liikennemäärillä riskienarvioinnin mukaisesti.	Perustason vaatimusten lisäksi: Käytössä oltava menettely hyökkäyksen / väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan (vrt. A 410.0 ja I 504.0). Verkkoliikennettä tarkkaillaan vähintään sillä tarkkuudella, että havaitaan a) merkittävät poikkeamat työasemien ja palvelinten liikennemäärissä, b) normaalitilaan nähden poikkeavat protokollat, c) luvattomien yhteyksien yritykset (esim. vyöhykkeiden välisessä yhdyskäytävässä).	Perustason vaatimusten lisäksi: Käytössä oltava menettely hyökkäyksen / väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan (vrt. A 410.0 ja I 504.0). Verkkoliikennettä tarkkaillaan vähintään sillä tarkkuudella, että havaitaan a) merkittävät poikkeamat työasemien ja palvelinten liikennemäärissä, b) normaalitilaan nähden poikkeavat protokollat, c) luvattomien yhteyksien yritykset (esim. vyöhykkeiden välisessä yhdyskäytävässä).	Verkkoa, järjestelmiä ja niiden käyttöä valvotaan toimintavaatimusten ja riskienarvioinnin mukaisesti. Resurssit on mitoitettu toimintavaatimusten ja riskienarvioinnin mukaisesti.	ISO/IEC 27002 10.6.1, ISO/IEC 27002 10.10.2, ISO/IEC 27002 10.3.1, PCI DSS 11.4, COBIT 4.1 DS3, COBIT 4.1 ME1, VAHTI 8/2006, VAHTI 3/2009, VAHTI 3/2010, VAHTI 2/2010:n liite 5 (TTT)	Vaatimukset toimivuudelle normaaliliikenteestä poikkeavilla liikennemäärillä arvioidaan tapauskohtaisesti toiminnan käytettävyysvaatimusten mukaisesti.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Aud.tulos: OK/poikkeama
I 409.0 **Miten IPv6:n turvallisuuteen vaikuttavat erityispiirteet on huomioitu verkoissa ja järjestelmissä?** *Lisäkysymys:* *Onko organisaatiolle ongelmalliset piirteet huomioitu ja tarpeelliset vastatoimet otettu käyttöön?* *	1) IPv6-toiminnallisuus on huomioitu verkon/järjestelmän kokonaissuunnittelussa järkevästi tai se on poistettu käytöstä kaikista sellaisista järjestelmistä (työasemat, palvelimet, verkkolaitteet, jne.), joissa sille ei ole todellista käyttöperustetta. 2) IPv6 Privacy Extensions (RFC 4941) estetty organisaation verkossa, ellei tälle ole todellista toimintaperustetta.	1) IPv6-toiminnallisuus on huomioitu verkon/järjestelmän kokonaissuunnittelussa järkevästi tai se on poistettu käytöstä kaikista sellaisista järjestelmistä (työasemat, palvelimet, verkkolaitteet, jne.), joissa sille ei ole todellista käyttöperustetta. 2) IPv6 Privacy Extensions (RFC 4941) estetty organisaation verkossa, ellei tälle ole todellista toimintaperustetta.	1) IPv6-toiminnallisuus on huomioitu verkon/järjestelmän kokonaissuunnittelussa järkevästi tai se on poistettu käytöstä kaikista sellaisista järjestelmistä (työasemat, palvelimet, verkkolaitteet, jne.), joissa sille ei ole todellista käyttöperustetta. 2) IPv6 Privacy Extensions (RFC 4941) estetty organisaation verkossa, ellei tälle ole todellista toimintaperustetta.	IPv6:n erityispiirteet on huomioitu riskienarvioinnin mukaisesti.	http://www.nsa.gov/ia/guidance/security_configuration_guides/IPv6.shtml	Mikäli työasemissa, palvelimissa, verkkolaitteissa tai muissa vastaavissa järjestelmissä käytetään IPv6-toiminnallisuutta, tulee huomioida sen vaikutukset erityisesti liikenteen suodatukseen (palomuurauksen tulee kattaa myös IPv6-liikenne) sekä reititykseen (vrt. I 410.0). Huomattava myös, että sisäverkon käyttäjät olisi pystyttävä tunnistamaan jälkikäteen esim. tietoturvaloukkausten selvittelyssä. IPv6 Privacy Extensions voi vaikeuttaa tunnistamista merkittävästi.	
I 410.0 **Miten reitityksen turvallisuudesta on huolehdittu?** *	1) Reitityksen sanomat todennetaan. 2) Todennus päällä vyöhykekohtaisesti jokaisen naapurin kanssa. 3) Reitityksessä määritellään tarpeelliset ja riittävät suotimet informaation välittämiseen.	1) Reitityksen sanomat todennetaan. 2) Todennus päällä vyöhykekohtaisesti jokaisen naapurin kanssa. 3) Reitityksessä määritellään tarpeelliset ja riittävät suotimet informaation välittämiseen.	1) Reitityksen sanomat todennetaan. 2) Todennus päällä vyöhykekohtaisesti jokaisen naapurin kanssa. 3) Reitityksessä määritellään tarpeelliset ja riittävät suotimet informaation välittämiseen.	Reitityksen turvallisuudesta on huolehdittu riskienarvioinnin mukaisesti.	VAHTI 3/2010		

Tietojärjestelmäturvallisuus, osa-alue I500

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomais-vaatimus: Korkea taso (II)	Elinkeino-elämän suositukset	Lähde/lisätietoa	HUOM!	Audi-tointi-tulos: OK/ poik-keama
I 501.0 **Tunnistetaanko ja todennetaanko käyttäjät ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin?** *Lisäkysymys:* *Miten tämä on käytännössä järjestetty?*	Käyttäjät tunnistetaan ja todennetaan ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin: 1) Käytössä yksilölliset henkilökohtaiset käyttäjätunnisteet. 2) Kaikki käyttäjät tunnistetaan ja todennetaan. 3) Pääsyä käyttöjärjestelmään valvotaan turvallisen sisäänkirjausmenettelyn avulla. 4) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti. 5) Todennus tehdään vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, a) käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, b) käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. 6) Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen. 7) Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä/sovelluksissa ole teknisesti mahdollista, vaaditaan sovitut ja dokumentoidut salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille.	Perustason vaatimusten 1-4, 6, 7 lisäksi: Käyttäjän tunnistamiseen käytetään vahvaa käyttäjäntunnistusta, mikäli samalla tietojärjestelmällä hallinnoidaan useampia kuin yhtä ko. suojaustason hanketta tai projektia.	Perustason vaatimusten 1-4, 6, 7 lisäksi: Käyttäjän tunnistamiseen käytetään aina vahvaa käyttäjäntunnistamista. Ks. kohdennetut vaatimukset: liitteen 1 huomautukset (I 502.0 / IV ja III).	Käyttäjät tunnistetaan ja todennetaan ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin.	ISO/IEC 27002 11.3.1, ISO/IEC 27002 11.4, ISO/IEC 27002 11.5.1, ISO/IEC 27002 11.5.2, PCI DSS 8.1, PCI DSS 8.5, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf, VAHTI 8/2006, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010	Tunnistamisen ja todentamisen luotettavaan järjestämiseen kuuluu huolehtiminen ainakin siitä, että i) todennusmenetelmä on suojattu välimieshyökkäyksiltä (man-in-the-middle), ii) sisäänkirjautuessa, ennen todennusta, ei paljasteta mitään tarpeetonta tietoa, iii) todennuskredentiaalit ovat aina salatussa muodossa jos ne lähetetään verkon yli, iv) todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä vastaan, v) todennusmenetelmä on suojattu brute force –hyökkäyksiä vastaan. Suojaustasojen III ja II vaatimukset vahvasta käyttäjätunnistuksesta voidaan joissain tapauksissa täyttää siten, että tietojärjestelmään on mahdollista päästä vain tiukasti rajatusta fyysisestä tilasta, jonka pääsynvalvonnassa käytetään vahvaa, kahteen tekijään perustuvaa tunnistamista. Tällöin käyttäjän tunnistaminen tietojärjestelmässä voidaan järjestää käyttäjätunnus-salasana -parilla.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomais-vaatimus: Korkea taso (II)	Elinkeino-elämän suositukset	Lähde/lisätietoa	HUOM!	Audi-tointi-tulos: OK/ poik-keama
I 502.0 **Onko organisaatiossa menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, verkkotulostimet ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus?** **Katso lisätietoja liitteestä 1 (I 502.0)**	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. Katso kohdennetut vaatimukset: liite 1 huomautukset (I 502 / IV).	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. Ks. kohdennetut vaatimukset: liite 1 huomautukset (I 502.0 / IV ja III).	Korotetun tason vaatimusten lisäksi: On käytössä mekanismi, menetelmä tai menettelytapa, jolla tietojärjestelmään tehtävät muutokset tallentuvat ja tehdyt muutokset voidaan jälkikäteen havaita (vrt. I 504.0). Ks. kohdennetut vaatimukset: liite 1 huomautukset (I 502.0 / II).	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.	PCI DSS 2.1, PCI DSS 2.2, ISO/IEC 11.2.3, VAHTI 8/2006, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010 Lähteitä järjestelmien/laitteiden kovennukseen ja turvalliseen konfiguraatioon: http://www.nsa.gov/ia/guidance/security_configuration_guides/, http://nvd.nist.gov/fdcc/index.cfm, http://web.nvd.nist.gov/view/ncp/repository, http://usgcb.nist.gov/, http://www.ia.nato.int/ > IA Guidance > Best Practices > Security Checklist, http://iase.disa.mil/stigs/stig/index.html, http://iase.disa.mil/stigs/checklist/index.html, http://technet.microsoft.com/en-us/library/cc163140.aspx, http://technet.microsoft.com/en-us/library/cc757698.aspx, http://httpd.apache.org/docs/1.3/misc/security_tips.html, http://csrc.nist.gov/publications/PubsSPs.html, http://www.cisco.com/en/US/tech/tk648/tk361/ technologies_tech_note-09186a0080120f48.shtml, http://www.hp.com/rnd/pdfs/Hardening_ProCurve_Switches_White_Paper.pdf, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf http://kb2.adobe.com/cps/837/cpsid_83709/attachments/ Acrobat_Enterprise_Administration.pdf, http://www.sans.org/critical-security-controls/control.php?id=3, http://www.sans.org/critical-security-controls/control.php?id=4	Järjestelmäkovennuksissa edellytetään suojaustasolla III FDCC:tä tai vastaavaa tasoa. Osalle kansainvälisistä aineistoista edellytetään FDCC:tä vastaavaa tasoa jo suojaustasolla IV. Katso kohdennetut vaatimukset liitteen 1 huomautuksista (I 502.0) Suojaustason II vaatimus voidaan toteuttaa esimerkiksi tiedostojärjestelmän eheyttä tarkkailevalla ohjelmistolla. Lisätietoa löytyy esimerkiksi osoitteesta http://nsrc.org/security/#integrity. Vrt. sähköpostisuojaukset vaatimuksesta I 605.0.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomais-vaatimus: Korkea taso (II)	Elinkeino-elämän suositukset	Lähde/lisätietoa	HUOM!	Audi-tointi-tulos: OK/ poik-keama
I 503.0 **Miten on pienennetty haittaohjelmien aiheuttamia riskejä?** *Tarkentavia ohjeita liitteessä 1 (I 503).*	1) Haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat yleisesti alttiita haittaohjelmatartunnoille (erityisesti työasemat, kannettavat tietokoneet ja palvelimet). 2) Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä. 3) Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja. 4) Haittaohjelmatunnisteet päivittyvät säännöllisesti. 5) Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta (vrt. A 806.0). 6) Haittaohjelmahavaintoja seurataan (vrt. A 408.0).	Perustason vaatimusten lisäksi: Tapauskohtaisesti arvioidaan tarve järjestelmien USB-porttien ja vastaavien liityntöjen käytölle. Mikäli liityntöjen käytölle ei ole todellista perustetta, ne poistetaan käytöstä. Mikäli liityntöjen käytölle on todelliset perusteet, arvioidaan tapauskohtaisesti edellytykset ja ehdot, minkä mukaisia laitteistoja ja välineitä (esim. USB-muisteja) järjestelmään voidaan kytkeä.	Perustason vaatimusten lisäksi: Tapauskohtaisesti arvioidaan tarve järjestelmien USB-porttien ja vastaavien liityntöjen käytölle. Mikäli liityntöjen käytölle ei ole todellista perustetta, ne poistetaan käytöstä. Mikäli liityntöjen käytölle on todelliset perusteet, arvioidaan tapauskohtaisesti edellytykset ja ehdot, minkä mukaisia laitteistoja ja välineitä (esim. USB-muisteja) järjestelmään voidaan kytkeä.	Haittaohjelmien havaitsemis- ja estotoimet sekä niistä toipumismekanismit ja asiaankuuluvat käyttäjien valppautta lisäävät ohjeet on otettu käyttöön.	ISO/IEC 27002 10.4.1, PCI DSS 5.1, PCI DSS 5.2, http://www.sans.org/critical-security-controls/control.php?id=12, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomais-vaatimus: Korkea taso (II)	Elinkeino-elämän suositukset	Lähde/lisätietoa	HUOM!	Audi-tointi-tulos: OK/ poik-keama
I 504.0 **Pääkysymys: Ovatko organi-saation teknis-ten laitteiden ja palveluiden lokimenettelyt kunnossa?** *Lisäkysymys:* *Kerätäänkö ver-koista, laitteista ja järjestelmistä kes-keiset lokitiedot ja käsitelläänkö niitä asianmukaisesti?* **Katso lisämää-reet liitteestä 1 (I 504).**	1) Tallenteiden kattavuus on riittävä tietomurtojen tai niiden yritysten jälkikäteiseen todenta-miseen. 2) Keskeisiä tallenteita säilytetään 6 kk tai erillisessä sopimuksessa määrätty aika. 3) Suojattavaa tie-toa sisältävät lokitiedot on suojattu asianmukaisesti (pääsynvalvonta, käsittely, poisto).	Perustason vaatimusten 1 ja 3 lisäksi: 1) Keskeisiä tallenteita säilytetään 24 kk tai erillisessä sopimuksessa määrätty aika. 2) On käytössä menettely hyök-käyksen/väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaan. Menettelyn on sisäl-lettävä vähintään kerran viikossa tapahtuva lokitietojen tarkkailu normaalitilaan nähden poikkeavi-en tapahtumien havaitsemiseksi. Erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitse-maan (vrt. I 408.0 ja A 410.0). 3) Samassa organisaatiossa tai turvallisuusalueella olevien olen-naisten tietojenkäsittelyjärjestelmi-en kellot on synkronoitu sovitun tarkan ajanlähteen kanssa. 4) Lokitiedot ja niiden kirjauspal-velut ovat suojattuja väärentämi-seltä ja luvattomalta pääsyltä. On käytössä jokin menetelmä lokien eheyden (muuttumattomuuden) varmistamiseen. 5) Keskeiset lokitiedot varmuusko-pioidaan säännöllisesti. 6) Syntyneiden lokitietojen käytöstä ja käsittelystä muodostuu merkintä. 7) Kriittisistä ylläpitotoimista tal-lennetaan kirjausketju (audit trail).	Korotetun tason vaatimusten lisäksi: 1) Tietojärjes-telmän eheydes-tä varmistutaan vähintään kerran viikossa (vrt. I 502.0). 2) Suojaustason II tietojen käsit-telystä tallenne-taan käsittely-tiedon sisältävät lokimerkinnät (vrt. I 607.0).	1) Tallentei-den kattavuus on riittävä tietomurtojen tai niiden yritysten jälkikäteiseen todentami-seen. 2) Keskeisiä tallenteita säilytetään riskienar-vioinnissa määritetty aika.	ISO/IEC 27002 10.6.1, ISO/IEC 27002 10.10.1, ISO/IEC 27002 10.10.2, ISO/IEC 27002 10.10.3, ISO/IEC 27002 10.10.6, PCI DSS 10.1, PCI DSS 10.2, PCI DSS 10.3, PCI DSS 10.4, PCI DSS 10.5, VAHTI 8/2006, VAHTI 3/2009, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010 http://www.sans.org/critical-security-controls/control.php?id=6, http://technet.microsoft.com/en-us/library/bb742610.aspx, http://technet.microsoft.com/en-us/library/dd408940%28WS.10%29.aspx, http://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomais-vaatimus: Korkea taso (II)	Elinkeino-elämän suositukset	Lähde/lisätietoa	HUOM!	Audi-tointi-tulos: OK/ poik-keama
I 505.0 **Miten suojattavat tiedot säilytetään tietojärjestelmissä?** **Katso lisätietoja liitteestä 1 (I505)**	1) Tietojärjestelmissä suojattavat tiedot on eritelty käyttöoikeus-määrittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä. 2) Tietojärjestelmien käytön yhteydessä syntyvät suojattavaa tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti (ks. I 603.0). 3) Suojaustason IV tietoa sisältävät kannettavien tietokoneiden kiintolevyt ovat riittävällä tasolla suojattuja (vrt. I 506).	Perustason vaatimusten 1 ja 2 lisäksi: 1) Palvelimissa, työasemissa, kannettavissa tietokoneissa, ja muissa tallennusvälineissä suojaustason III tiedot säilytetään aina luotettavasti salakirjoitettuna (ks. I 509.0). 2) Mikäli samalla palvelimella/ palvelimilla säilytetään useamman kuin yhden ko. turvatason hankkeen/projektin/ toiminnon tietoja, palvelimella olevat tiedot säilytetään luotettavasti salakirjoitettuna käyttöoikeusrajoitteisissa hakemistoissa tai alueilla. 3) Suojaustason III tieto pidetään erillään julkisesta ja muiden suojaustasojen tiedoista.	1) Palvelimissa, työasemissa, kannettavissa tietokoneissa, ja muissa tallennusvälineissä suojaustason II tiedot säilytetään aina luotettavasti salakirjoitettuna (ks. I 509.0). 2) Suojaustason II tieto pidetään erillään julkisesta ja muiden suojaustasojen tiedoista.	Tietojärjestelmissä suojattavat tiedot on eritelty käyttöoikeus-määrittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä.	VAHTI 8/2006, VAHTI 2/2010, VAHTI 3/2010 http://www.nsa.gov/ia/guidance/security_configuration_guides/database_servers.shtml, http://www.oracle.com/technetwork/articles/idm/tde-089026.html, http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf, http://www.ibm.com/developerworks/data/library/techarticle/dm-0907encryptionexpert/, http://publib.boulder.ibm.com/epubs/pdf/eetuga13.pdf, http://technet.microsoft.com/en-us/library/cc278098%28SQL.100%29.aspx, http://technet.microsoft.com/en-us/library/cc875821.aspx, http://support.microsoft.com/kb/223316, http://publib.boulder.ibm.com/infocenter/lnxinfo/v3r0m0/topic/liaai/secure/ liaaisecuresles.htm, http://www.linuxtopia.org/online_books/suse_linux_guides/SLES10/ suse_enterprise_linux_server_installation_admin/cha_cryptofs.html, http://www.postgresql.org/docs/manuals/, http://www.sans.org/critical-security-controls/control.php?id=15		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 506.0 **Kuinka varmistutaan siitä, että suojattavaa tietoa sisältävät liikuteltavat kiintolevyt, muistit, mediat, älypuhelimet, mobiilipäätteet ja vastaavat ovat aina suojattuja luvatonta pääsyä vastaan?**	1) Suojattavaa tietoa sisältävät kannettavien tietokoneiden kiintolevyt, USB-muistit, tallennusmediat ja vastaavat ovat luotettavasti suojattuja. 2) Turvaluokiteltua tietoa sisältävät älypuhelimet: a) Pääsy puhelimen ja muistikortin tietoihin suojataan salasanalla. b) Käytössä puhelimen/SIM-kortin/muistikortin automaattinen lukittuminen. c) Etätyhjennysmahdollisuus käytössä. d) Puhelimen ja muistikortin muisti suojataan. e) Verkko- ja haittaohjelmauhat huomioidaan riskienarvioinnin mukaisesti. f) Bluetooth- ja WLAN-yhteydet ovat oletusarvoisesti kytketyt pois päältä ja ne aktivoidaan vain käytön ajaksi. Bluetooth-asetuksissa puhelimen näkyvyys on oletuksena asetettu piilotetuksi.	Perustason vaatimuksen 1 lisäksi: Suojaustason III aineistoa ei lähtökohtaisesti käsitellä älypuhelimilla. Toimivaltainen viranomainen voi kuitenkin tapauskohtaisesti erillishyväksyä tietyt toteutukset, joissa älypuhelin ja kaikki sen kautta kulkeva liikenne suojataan luotettavasti.	Perustason vaatimuksen 1 lisäksi: Suojaustason II aineistoa ei lähtökohtaisesti käsitellä älypuhelimilla. Toimivaltainen viranomainen voi kuitenkin tapauskohtaisesti erillishyväksyä tietyt toteutukset, joissa älypuhelin ja kaikki sen kautta kulkeva liikenne suojataan luotettavasti.	Suojattavaa tietoa sisältävät kannettavien tietokoneiden kiintolevyt, USB-muistit, tallennusmediat ja vastaavat ovat luotettavasti suojattuja. Suojattavaa tietoa sisältävät älypuhelimet suojataan riskienarvioinnin mukaisesti (lukitus, salakirjoitus, etähallinta, jne.).	ISO/IEC 27002 10.8.3, ISO/IEC 27002 9.2.5, VAHTI 8/2006, VAHTI 2/2010, VAHTI 3/2010, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 9. artikla, http://www.sans.org/score/handheld-checklist.php	Useimmat nykyiset käyttöjärjestelmät tarjoavat jo asennuksen yhteydessä mahdollisuuden kiintolevyn salaamiseen. Vaihtoehtoisesti voidaan käyttää erillistä ohjelmistoratkaisua. USB-muistien ja muiden tallennusmedioitten salaamiseen on olemassa sekä ohjelmisto- että laitetason ratkaisuja. Vrt. I 509.0.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 507.0 **Kuinka varmistutaan siitä, etteivät suojattavat tiedot joudu kolmansille osapuolille huoltotoimenpiteiden tai käytöstä poiston yhteydessä?**	1) Kaikki suojattavaa tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, suojattavaa tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (esim. monitoimilaite), jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä.	1) Kaikki suojattavaa tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, suojattavaa tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (esim. monitoimilaite), jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä.	1) Kaikki suojattavaa tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, suojattavaa tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (esim. monitoimilaite), jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä.	1) Kaikki suojattavaa tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, suojattavaa tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (esim. monitoimilaite), jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä.	ISO/IEC 27002 9.2, ISO/IEC 27002 9.2.6, VAHTI 8/2006, VAHTI 2/2010	Luotettavalla tyhjennyksellä tarkoitetaan tässä yhteydessä tiedon ylikirjoittamista. Vaatimus kattaa kaikki laitteistot, joihin on joskus tallennettu suojattavaa tietoa, esim. kannettavat, työasemat, palvelimet, puhelimet, tulostimet, verkkolaitteet, jne. Vrt. I 603.0. Mikäli luotettava tyhjennys ei ole mahdollista, laitteisto tai sen osa on tuhottava mekaanisesti.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 508.0 **Pääkysymys: Miten varmistutaan, ettei organisaation verkossa ole luvattomia laitteita tai järjestelmiä?** *Lisäkysymykset:* *Miten tiedetään mitä (tietojärjestelmiin liittyviä) laitteita organisaatiossa on käytössä? Miten hallitaan tietoa käytetyistä ohjelmistoista ja niiden versio- ja lisenssitilanteesta? Havaitaanko, jos laite viedään luvatta pois organisaation tiloista? Havaitaanko, jos järjestelmiin on asennettu luvattomia ohjelmistoja? Tarkistetaanko kaikki tilat, joista on mahdollista päästä organisaation verkkoon, säännöllisesti luvattomien laitteistojen ja ohjelmistojen havaitsemiseksi?*	1) Laitteista pidetään laiterekisteriä, johon kirjataan myös hävitetyt/käytöstä poistetut laitteet. 2) Ohjelmistoista pidetään rekisteriä, johon kirjataan käytössä olevat ohjelmistot ja lisenssit. 3) Konesalit, kytkentäkaapit ja vastaavat tilat tarkistetaan todennettavaan suunnitelmaan pohjautuen säännöllisesti luvattomien laitteistojen (pakettikaappaimet, key-loggerit, luvattomat langattomat tukiasemat, jne.) löytämiseksi.	Perustason vaatimusten lisäksi: 1) Kaikki tilat, joista on mahdollista päästä suojattuun verkkoon, tarkistetaan todennettavaan suunnitelmaan pohjautuen säännöllisesti luvattomien laitteistojen löytämiseksi. 2) Verkkopistokkeet ja muut vastaavat tietoliikenneyhteydet, jotka eivät ole käytössä, on kytketty fyysisesti kytkentäpisteistä irti. 3) Tuntemattomien laitteiden kytkeminen verkkoon estetään verkkoteknisin keinoin.	Korotetun tason vaatimusten lisäksi: 1) Sähkökaapelointi sekä tietoja siirtävä tai tietotekniikkapalveluja tukeva tietoliikennekaapelointi on suojattu salakuuntelulta ja vaurioilta. 2) Laitteistot on suojattu luvattomien laitteiden (key-loggerit ja vastaavat) liittämistä vastaan. Mikäli käytetään sinetöintiä, sinettien eheys tarkistetaan aina ennen laitteiston käyttöä.	1) Laitteista pidetään laiterekisteriä, johon kirjataan myös hävitetyt/käytöstä poistetut laitteet. 2) Ohjelmistoista pidetään rekisteriä, johon kirjataan käytössä olevat ohjelmistot ja lisenssit.	ISO/IEC 27002 9.2.1, ISO/IEC 27002 9.2.3, ISO/IEC 27002 11.4.1, ISO/IEC 27002 15.1.2, VAHTI 8/2006, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010, http://www.sans.org/critical-security-controls/control.php?id=1, http://www.sans.org/critical-security-controls/control.php?id=2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf	Suojaustason III vaatimus 3 voidaan toteuttaa hyödyntämällä esimerkiksi 802.1X-menettelyä. Suojaustason II vaatimusten toteutus voi edellyttää esim. a) laitteiden sijoittamista sinetöityyn ja/tai hälytyslaitteella varustettuun turvakehikkoon tai vastaavaan, b) peukalointia vastaan suojattujen laitteiden käyttämistä, tai c) jotain vastaavaa menettelyä (esim. käytettävien laitteiden sinetöintiä). Sähkö- ja tietoliikennekaapeloinnin suojausta edellytetään osalle kansainvälisistä aineistoista jo suojaustasolta III lähtien. Vrt. verkkolaitteiden kovennus: I 405.0	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 509.0 **Miten on varmistuttu siitä, että käytetyt salausratkaisut ovat riittävän turvallisia?**	Salausratkaisujen (ja -tuotteiden) tietoturvallisuus on tarkastettu ja hyväksytty ko. suojaustasolle a) kansainvälisen tietoturvaviranomaisen toimesta, b) kansallisen tietoturvaviranomaisen toimesta, tai c) erillisessä ratkaisulle suoritetussa tarkastuksessa.	Salausratkaisujen (ja -tuotteiden) tietoturvallisuus on tarkastettu ja hyväksytty ko. suojaustasolle a) kansainvälisen tietoturvaviranomaisen toimesta, b) kansallisen tietoturvaviranomaisen toimesta, tai c) erillisessä ratkaisulle suoritetussa tarkastuksessa.	Salausratkaisujen (ja -tuotteiden) tietoturvallisuus on tarkastettu ja hyväksytty ko. suojaustasolle a) kansainvälisen tietoturvaviranomaisen toimesta, b) kansallisen tietoturvaviranomaisen toimesta, tai c) erillisessä ratkaisulle suoritetussa tarkastuksessa.	Käytetään tunnettuja ja yleisesti luotettavina pidettyjä salausratkaisuja, tai ratkaisun luotettavuudesta on varmistuttu jollain muulla luotettavalla menetelmällä.	EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 10. artikla, http://www.consilium.europa.eu/information-assurance, http://www.ia.nato.int/niapc, Kansallisen salaustuotteiden hyväksyntäviranomaisen hyväksyttyjen salausratkaisujen lista, Kansallisen turvallisuusviranomaisen "Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje"	Erityisesti kansainvälisen turvaluokitellun tiedon salaamisessa edellytetään käytettävän käytännössä vain tiedon omistajan (esim. EU) hyväksymiä salausratkaisuja. Kansallisella salaustuotteiden hyväksyntäviranomaisella (CAA, Crypto Approval Authority, Suomessa NCSA-FI) on tietyin rajauksin mahdollisuus hyväksyä myös muita tuotteita/ratkaisuja kansainvälisen turvaluokitellun tiedon suojaamiseen. Usean kansainvälisen turvallisuusviranomaisen salaustuotehyväksynnät edellyttävät tuotteelta erinäisiä sertifikaatteja (erityisesti Common Criteria, toisinaan myös esim. FIPS 140), ja lisäksi tiettyjen erityisvaatimusten (esim. lähdekoodin luovutus ja tarkastus, hajasäteilysuojaukset) täyttämistä.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 510.0 **Salausavainten hallinta.** **Pääkysymys: Ovatko salaiset avaimet vain valtuutettujen käyttäjien ja prosessien käytössä?** **Lisäkysymys:** **Ovatko salausavainten hallinnan prosessit ja käytännöt dokumentoituja? Miten käytännön toteutus on järjestetty?** **Katso lisätiedot liitteestä 1 (I 510.0).**	1) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. 2) Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen.	1) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. 2) Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen.	1) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. 2) Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen.	Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä.	ISO/IEC 27002 12.3.2, PCI DSS 3.6, VAHTI 8/2006, VAHTI 2/2010		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 511.0 **Käytetäänkö istunnonhallinnassa tunnettua ja luotettavana pidettyä tekniikkaa?**	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	ISO/IEC 27002 11.5, VAHTI 3/2001		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 512.0 **Onko huolehdittu, että autentikaatiodataa ei säilytetä tietojärjestelmissä selväkielisinä?**	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.	PCI DSS 3.2, PCI DSS 8.4, ISO/IEC 27002 11.5.3		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 513.0 **Miten on varmistuttu ajettavan koodin turvallisuudesta?** * **Katso lisätiedot liitteestä 1 (I 513.0).**	Ohjelmistoja hankitaan ja asennetaan vain luotettavista ja luvallisista lähteistä.	Perustason vaatimuksen lisäksi: 1) Asennettavien ohjelmistojen ja päivitysten eheys tarkistetaan (tarkistussummat, haittaohjelmatarkistus). 2) Hankittavilta/toteutettavilta sovelluksilta vaaditaan turvallisen ohjelmoinnin periaatteiden, esim. Open Web Application Security Project Guide, toteuttamista. Toimittajilta vaaditaan selvitys, miten tietoturvallisuus on otettu huomioon tuotekehityksessa.	Perustason vaatimuksen lisäksi: Vaihtoehdot: 1) Käytetään vain viranomaisen ko. toimintaympäristöön hyväksymiä järjestelmiä/ohjelmistoja. 2) Hankittavilta/toteutettavilta sovelluksilta vaaditaan turvallisen ohjelmoinnin periaatteiden, esim. Open Web Application Security Project Guide, toteuttamista. Toimittajilta vaaditaan selvitys, miten tietoturvallisuus on otettu huomioon tuotekehityksessä. Lisäksi kaikki ko. järjestelmän turvallisuuteen oleellisesti vaikuttava koodi on avoimesti tarkastettavissa (esim. takaportit, turvattomat toteutukset, jne.) tai sopimuksessa on varattu oikeus lähdekoodin tarkastukseen. Vaihtoehdossa 2 on näytettävä todiste koodin luotettavaksi toteamisesta (esim. kuvaukset toimittajan prosesseista ja ulkopuolisen tekemä katselmointiraportti).	Ohjelmistoja hankitaan ja asennetaan vain luotettavista ja luvallisista lähteistä.	ISO/IEC 27002 12.2.1, ISO/IEC 27002 12.4.1, ISO/IEC 27002 15.1.2, PCI DSS 6.5, VAHTI 8/2006, http://www.bsi-mm.com/, http://www.opensamm.org/, http://www.owasp.org/index.php/Category:OWASP_Guide_Project, http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, http://www.cpni.gov.uk/Docs/Vendor_security_questions.pdf, http://www.sans.org/critical-security-controls/control.php?id=7	Ohjelmistotoimittajalta voidaan vaatia esim. seuraavia: 1) Ohjelmistokehittäjien riittävä tietoturvatietous on varmistettu. 2) Ohjelmistokehityksen aikana on suoritettu tietoturvauhka-analyysi ja havaitut riskit on joko kontrolloitu tai nimenomaisesti hyväksytty. 3) Rajapinnat (ainakin ulkoiset) on testattu viallisilla syötteillä sekä suurilla syötemäärillä. 4) Riippuen ohjelmointiympäristöstä, helposti ongelmia aiheuttavien funktioiden ja rajapintojen käyttöön on määritelty politiikka ja sitä valvotaan (esim. Microsoftilla on listat kielletyistä funktioista). 5) Arkkitehtuuri ja lähdekoodi on katselmoitu. 6) Ohjelmakoodi on tarkastettu automatisoidulla staattisella analyysillä. 7) Ohjelmakoodin versionhallinnan ja kehitystyökalujen eheys on varmistettu. Hankittavista ohjelmistoista on saatava myös dokumentaatio, josta selviää lisäksi ainakin sovelluksen käyttämät verkkoportit. Suotavaa on myös edellyttää, että a) sovellukset käyttävät pientä määrää määriteltyjä portteja, b) dynaamisia portteja käyttävät sovellukset käyttävät vain pientä porttiavaruutta, ja c) ohjelmistot eivät vaadi laajoja käyttöoikeuksia toimiakseen (ts. ohjelmistojen on toimittava “peruskäyttäjän” oikeuksilla).	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 514.0 **Kuinka varmistutaan siitä, että organisaatioon hankittavat laitteistot ovat tietoturvaperiaatteiden mukaisia ja käyttötarkoitukseensa nähden riittävän tietoturvallisia?** *	Tietoturva-asiat otetaan huomioon laitehankinnoissa. Tulee huomioida ainakin 1) mahdollistaako laite riittävän turvallisen pääsynvalvonnan (esim. puhelin, tulostin, verkkolaite, kannettava tietokone), 2) jääkö käsitellyt dokumentit laitteen muistiin (esim. tulostimet, monitoimilaitteet), 3) mahdollistaako laite muistinsa salakirjoituksen (esim. tulostin, kannettava tietokone, puhelin), 4) tarjoaako laitevalmistaja kuinka hyvää tukea (turvapäivitykset, lisenssi- ja takuuehdot, jne.), 5) mitä muita turvaominaisuuksia laitteessa on, 6) onko laitetta mahdollista muokata itse turvallisemmaksi.	Tietoturva-asiat otetaan huomioon laitehankinnoissa. Tulee huomioida ainakin 1) mahdollistaako laite riittävän turvallisen pääsynvalvonnan (esim. puhelin, tulostin, verkkolaite, kannettava tietokone), 2) jääkö käsitellyt dokumentit laitteen muistiin (esim. tulostimet, monitoimilaitteet), 3) mahdollistaako laite muistinsa salakirjoituksen (esim. tulostin, kannettava tietokone, puhelin), 4) tarjoaako laitevalmistaja kuinka hyvää tukea (turvapäivitykset, lisenssi- ja takuuehdot, jne.), 5) mitä muita turvaominaisuuksia laitteessa on, 6) onko laitetta mahdollista muokata itse turvallisemmaksi.	Tietoturva-asiat otetaan huomioon laitehankinnoissa. Tulee huomioida ainakin 1) mahdollistaako laite riittävän turvallisen pääsynvalvonnan (esim. puhelin, tulostin, verkkolaite, kannettava tietokone), 2) jääkö käsitellyt dokumentit laitteen muistiin (esim. tulostimet, monitoimilaitteet), 3) mahdollistaako laite muistinsa salakirjoituksen (esim. tulostin, kannettava tietokone, puhelin), 4) tarjoaako laitevalmistaja kuinka hyvää tukea (turvapäivitykset, lisenssi- ja takuuehdot, jne.), 5) mitä muita turvaominaisuuksia laitteessa on, 6) onko laitetta mahdollista muokata itse turvallisemmaksi.	Tietoturva-asiat otetaan huomioon laitehankinnoissa. Tulee huomioida ainakin 1) mahdollistaako laite riittävän turvallisen pääsynvalvonnan (esim. puhelin, tulostin, verkkolaite, kannettava tietokone), 2) jääkö käsitellyt dokumentit laitteen muistiin (esim. tulostimet, monitoimilaitteet), 3) mahdollistaako laite muistinsa salakirjoituksen (esim. tulostin, kannettava tietokone, puhelin), 4) tarjoaako laitevalmistaja kuinka hyvää tukea (turvapäivitykset, lisenssi- ja takuuehdot, jne.), 5) mitä muita turvaominaisuuksia laitteessa on, 6) onko laitetta mahdollista muokata itse turvallisemmaksi.	ISO 27002 12.1.1, VAHTI 8/2006, VAHTI 2/2010:n liite 5 (TTT)	Hankittavalle laitteistolle asetettavat tietoturvavaatimukset riippuvat suuresti laitteen käyttötarkoituksesta. Esimerkiksi tulostimelle voidaan asettaa hyvin erilaisia vaatimuksia riippuen siitä, minkä suojaustason aineistojen tulostamiseen sitä käytetään. Vaatimuksia voivat olla esimerkiksi pääsynvalvonta (pelkkä lukitus vs. käyttäjän tunnistaminen ja todentaminen), lokienkeruun mahdollisuudet, muistin/kiintolevyn salauksen ja tyhjennyksen mahdollisuudet, kytkentä (paikallinen vs. verkkotulostin), verkkoliikenteen salaus, etähallinnan turvaratkaisut, hajasäteilysuojaukset, jne.	

Tietoaineistoturvallisuus, osa-alue I600

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 601.0 **Millainen tiedon luokittelumenettely organisaatiolla on?**	1) Tiedot on luokiteltu niiden merkittävyyden ja/tai lakisääteisten vaatimusten perusteella. Tietosisällöltään suojattavat (esim. turvaluokitellut) dokumentit (ml. luonnokset) varustetaan suojaustasoa kuvaavalla merkinnällä. 2) Dokumentit merkitään dokumentin osien (esim. liitteet) ylintä suojaustasoa vastaavalla merkinnällä. 3) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi dokumentista.	1) Tiedot on luokiteltu niiden merkittävyyden ja/tai lakisääteisten vaatimusten perusteella. Tietosisällöltään suojattavat (esim. turvaluokitellut) dokumentit (ml. luonnokset) varustetaan suojaustasoa kuvaavalla merkinnällä. 2) Dokumentit merkitään dokumentin osien (esim. liitteet) ylintä suojaustasoa vastaavalla merkinnällä. 3) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi dokumentista.	1) Tiedot on luokiteltu niiden merkittävyyden ja/tai lakisääteisten vaatimusten perusteella. Tietosisällöltään suojattavat (esim. turvaluokitellut) dokumentit (ml. luonnokset) varustetaan suojaustasoa kuvaavalla merkinnällä. 2) Dokumentit merkitään dokumentin osien (esim. liitteet) ylintä suojaustasoa vastaavalla merkinnällä. 3) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi dokumentista.	1) Tiedot on luokiteltu niiden merkittävyyden ja/tai lakisääteisten vaatimusten perusteella. Tietosisällöltään suojattavat (esim. turvaluokitellut) dokumentit (ml. luonnokset) varustetaan suojaustasoa kuvaavalla merkinnällä. 2) Dokumentit merkitään dokumentin osien (esim. liitteet) ylintä suojaustasoa vastaavalla merkinnällä. 3) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi dokumentista.	ISO/IEC 27002 7.2.1, VAHTI 2/2010, COBIT 4.1 PO2.3, Kansallisen turvallisuusviran-omaisen "Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje", EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 2. artikla, http://www.finlex.fi/fi/laki/ajantasa/1999/19990621	Vrt. käsittelysääntövaatimukset I 505.0, I 602.0, I 506.0, I 603.0, I 604.0, I 605.0, I 606.0, I 607.0.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 602.0 **Onko huolehdittu siitä, että suojattavaa tietoa sisältäviä aineistoja ja tietovälineitä säilytetään turvallisesti?**	1) Suojattavalle aineistolle on työtiloissa lukitut kaapit, kassakaapit tai vastaavat. 2) Huonetilasta poistuttaessa selväkielisessä muodossa oleva, mutta suojassa pidettävä aineisto (paperimuotoiset aineistot, ulkoiset muistivälineet ja vastaavat) siirretään kassakaappiin, lukittuun kaappiin tai vastaavaan säilytystilaan. 3) Huonetilasta poistuttaessa työskentelytila tarkistetaan tai tila lukitaan ulkopuolisilta.	Huonetilasta poistuttaessa suojaustason III aineisto (paperimuotoiset aineistot, ulkoiset muistivälineet ja vastaavat) siirretään EURO II -tason kassakaappiin tai vastaavaan tarkoitukseen hyväksyttyyn säilytystilaan, kuten hälytysjärjestelmällä varustettuun holviin (EURO IV).	Huonetilasta poistuttaessa suojaustason II aineisto (paperimuotoiset aineistot, ulkoiset muistivälineet ja vastaavat) siirretään EURO II -tason kassakaappiin tai vastaavaan tarkoitukseen hyväksyttyyn säilytystilaan, kuten hälytysjärjestelmällä varustettuun holviin (EURO IV).	Suojattavalle aineistolle on työtiloissa lukitut kaapit, kassakaapit tai vastaavat.	VAHTI 8/2006, VAHTI 2/2010, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 liite II	Vrt. aineistot tietojärjestelmissä: I 505.0, I 506.0, I 507.0, I 514.0. Säilytystiloille (kassakaapit jne.) on aina huomioitava tarkentavat vaatimukset (esim. luokka, kiinnitys, lisävaatimukset rikosilmoitusjärjestelmälle jne.) KATAKRI:n F-osiosta. Varmuuskopiot: säilytys eri sortumatilassa (I 701.0).	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 603.0 **Hävitetäänkö suojattavia tietoja sisältävät aineistot luotettavasti?** **Katso lisätietoja liitteestä 1 (I 603.0).**	1) Suojattavien sähköisten aineistojen hävittäminen tapahtuu luotettavasti (ylikirjoitus tai tallenteen fyysinen tuhoaminen). 2) Tietojärjestelmien käytön yhteydessä syntyvät suojattavaa tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti. Vrt. I 505.0. 3) Ei-sähköisten suojattavien aineistojen tuhoaminen on järjestetty luotettavasti. Organisaatiossa on paperinrepijä, jonka silpun koko on korkeintaan 2mm x 15mm (DIN 32757/ DIN 4), tai jokin muu hyväksytty menetelmä suojaustason IV aineiston hävittämiseksi (esim. polttaminen).	Perustason vaatimusten lisäksi: 1) Uudet asiakashankkeet (esim. ohjelmistoprojektit) aloitetaan aina "puhtaalla" laitteistolla. Ts. uudet hankkeet aloitetaan aina ympäristössä, jossa ei ole jäännöstietoja edellisistä hankkeista. 2) Eri asiakkaiden tietoja käsitellään erillisillä muisteilla (eri kiintolevyt eri hankkeille). Viranomainen voi tapauskohtaisesti hyväksyä myös ratkaisun, jossa eri hankkeita käsitellään erillisillä loogisilla muistialueilla (esim. virtualisointia hyödyntäen). 3) Organisaatiossa on hyväksytty paperinrepijä suojaustason III aineiston hävittämiseksi. Silpun koko on korkeintaan 2mm x 15mm (DIN 32757/ DIN 4).	Korotetun tason vaatimusten lisäksi: 1) Suojaustason II aineiston hävittäminen hoidetaan toisen henkilön valvonnassa viranomaisen hyväksymällä tavalla, esimerkiksi hyväksytyllä paperinrepijällä, jonka silpun koko on korkeintaan 2mm x 15mm (DIN 32757/ DIN 4). 2) Hävittäminen dokumentoidaan.	1) Suojattavien sähköisten aineistojen hävittäminen tapahtuu luotettavasti (ylikirjoitus tai tallenteen fyysinen tuhoaminen). 2) Ei-sähköisten suojattavien aineistojen tuhoaminen on järjestetty luotettavasti.	COBIT 4.1 DS11, VAHTI 8/2006, VAHTI 2/2010, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 liite III		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 604.0 **Miten suojattavan aineiston kopiointi ja tulostus on järjestetty?**	1) Kopioita käsitellään kuten alkuperäistä asiakirjaa. 2) Kopion voi luovuttaa edelleen vain henkilölle, jolla on käsittelyoikeus aineistoon ja tarve tietosisältöön. 3) Alkuperäiset luokittelumerkinnät säilyvät kopioinnissa ja tulostuksessa (tai vastaavat merkinnät lisätään välittömästi kopioinnin/tulostuksen jälkeen).	Perustason vaatimusten lisäksi: 1) Kopion/tulosteen saa ottaa vain suojaustasolle hyväksytyllä laitteella. 2) Kopiokoneiden ja tulostimien on oltava hyväksytyssä tilassa, eikä niistä saa olla ulkoisia tiedonsiirto- tai huoltoyhteyksiä, ellei niitä ole erikseen viranomaisen toimesta hyväksytty. 3) Tulostimen, kopiokoneen ja vastaavien laitteiden massamuistien tulee olla yksikön turvallisuusvastaavan hallinnassa. 4) Hajasäteilysuojausten on vastattava niille asetettuja vaatimuksia (vrt. F 217.0).	Korotetun tason vaatimusten lisäksi: 1) Kopiointi merkitään sekä alkuperäisen aineiston etusivulle, että diaariin/ rekisteriin jokaisen kopion ehdottoman jäljitettävyyden mahdollistamiseksi. 2) Kopion/tulosteen saa ottaa vain hankkeeseen/ympäristöön erikseen hyväksytyllä laitteella. 3) Tapauskohtaisesti harkitaan tuleeko jokaisesta tulosteesta tai kopiosta jäädä lokimerkintä, josta selviää tulosteen/kopion ottanut henkilö. Huom: Kattaa myös sähköiset kopiot.	Suojattavan aineiston kopiointi ja tulostus on järjestetty riskienarvioinnissa riittävän turvalliseksi katsotulla menettelyllä.	Kansallisen turvallisuusviranomaisen “Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”, VAHTI 2/2010	Joillekin kansainvälisille aineistoille vaaditaan jäljitettävyyttä jo suojaustasolta III lähtien, tarve tarkistetaan tapauskohtaisesti. Suojaustason III vaatimuksessa 3 tulee erityisesti huolehtia siitä, että huoltohenkilöstö (tulostinkorjaaja jne.) ei pääse yksin laitteelle. Vrt. vierailijakäytännöt vaatimuksesta F 209.2.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 605.0 **Pääkysymys: Miten suojattavan aineiston sähköinen välitys on järjestetty?** *Lisäkysymys:* *Onko tietoliikenne (ml. sähköinen viestintä) suojattu riskeihin nähden riittävillä mekanismeilla?*	1) Organisaatiossa pystytään tunnistamaan suojattavat tiedot ja huolehtimaan siitä, että ne välitetään asianmukaisesti suojaten. 2) Yhteys sähköpostipalvelimen ja -asiakasohjelman välillä on suojattu. 3) Mikäli sähköpostissa, telekopioviestinä, pikaviestimissä, IRC-keskusteluissa, VoIP-puheluissa ja vastaavissa käsitellään suojattavaa tietoa, on liikenne (tai viesti) suojattava siten, että suojattavaa tietoa ei pääse vuotamaan ulkopuolisille. 4) Aina, kun liikenne kulkee julkisen verkon (Internet, puhelinverkko, GSM-verkko, tai muu verkko, mikä ei ole ko. suojaustason vaatimusten mukainen) kautta, on liikenne (tai aineisto) salattava luotettavasti siirrettäessä vähintään ST IV –tason (turvallisuusluokitusmerkintä KÄYTTÖ RAJOITETTU) mukaisia tietoaineistoja.	1) Telekopiona aineistoa lähetetään vain, jos telekopiokone on a) varustettu viranomaisen hyväksymällä salaamislaitteella ja b) mikäli telekopiolaite on sijoitettu tilaan, johon pääsy on asiattomilta estetty. 2) Puhelimessa suojaustason III aineistosta keskustellaan vain viranomaisen hyväksymän päästä-päähän -salausratkaisun välityksellä (vrt. I 506.0).	1) Suojaustason II aineistoa ei lähtökohtaisesti välitetä julkisen verkon yli. Viranomainen voi kuitenkin tapauskohtaisesti hyväksyä järjestelmäkokonaisuuden, jolla suojaustason II aineistoa voi siirtää julkisen verkon yli ennalta määriteltyjen päätepisteiden välillä. 2) Suojaustason II tietoa ei tallenneta, eikä siirretä missään muodossa sellaisessa verkossa tai tietolaitteessa, joka ei ole viranomaisen erikseen tähän tarkoitukseen hyväksymä. Tietoa tulee tallentaa vain määritetyn laitteen kautta. 3) Puhelimessa suojaustason II aineistosta keskustellaan vain viranomaisen erikseen kyseiseen käyttötarkoitukseen ja ympäristöön hyväksymään menettelyyn perustuen (vrt. I 506.0).	Organisaatiossa pystytään tunnistamaan suojattavat tiedot ja huolehtimaan siitä, että ne välitetään asianmukaisesti suojaten.	ISO/IEC 27002 10.8, soveltaen PCI DSS 4.1, Kansallisen turvallisuusviranomaisen “Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”, VAHTI 2/2010, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 liite IV	Kattaa puhelimen, telekopion (faksin), sähköpostin, pikaviestimet ja muut vastaavat tiedonsiirtomenetelmät. Suojaustason IV vaatimus 2: Toteutus on usein helpointa käyttämällä liikenteen salaavia protokollia salaamattoman vaihtoehdon sijaan, esim. IMAPS-protokolla IMAP:n sijaan. Vrt. I 502.0 ja I 511.0. Suojaustason IV vaatimus 3: Toteutus on usein helpointa käyttämällä päästä-päähän -salausta sovellustasolla, tai kirjaamalla suojattavat tiedot liitetiedostoon, joka salataan luotettavasti (vrt. I 509.0). Joskus on suositeltavaa käyttää yritystason pikaviestin- tai/ja VoIP-ratkaisuja, joissa palvelin, asiakasohjelmat ja niiden välinen liikenne pysyy luotetun organisaatioverkon tai sen osan sisällä, ja liikenne on salattua.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
	5) Yhteyden on oltava luotettavasti suojattu päästä-päähän. Tapauskohtaisesti voidaan hyväksyä toteutukset, joissa a) liikenne kulkee salaamattomana vain organisaation luotetun verkon tai verkon osan sisällä, b) liikenne salataan palvelimelta-palvelimelle tai organisaatioiden välillä rajalta-rajalle. 6) Sähköpostia/telekopiolaitetta käytettäessä varmistetaan vastaanottajan osoite/numero. 7) Kun suojattava tieto siirretään tietojärjestelmästä toiseen, se suojataan siirron aikana ja vastaanottavassa järjestelmässä tiedon alkuperäisen tason edellyttämällä tavalla. 8) Tapauskohtaisesti arvioidaan tarve (sähköposti)viestin eheyden tarkistukseen, ja lisäksi arvioidaan onko tarpeen saada tietää, kun viesti on vastaanotettu ja/tai avattu.					Suojaustason IV vaatimus 4: Vrt. I 401.0. Suojaustason II vaatimus 1: Aineiston välittäminen julkisen verkon yli edellyttää toimivaltaisen viranomaisen hyväksymää järjestelmäkokonaisuutta. Järjestelmäkokonaisuuteen kuuluvat mm. erikseen hyväksytty tietojärjestelmä asetuksineen, hyväksytty salausratkaisu (ohjelmisto + rauta-alusta), sekä järjestelmän fyysinen sijoituspaikka ja siihen liittyvät suojaukset (pääsynvalvonta, hajasäteilysuojaus, jne.). Vrt. I 401.0	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/poikkeama
I 606.0 **Onko suojattavan aineiston välitys postilla ja/tai kuriirilla järjestetty turvallisesti?**	1) Lähetykset osoitetaan henkilön nimellä. 2) Pakkaus ei saa ulkoisesti paljastaa sen sisältävän suojattavaa materiaalia. Huom: kirjekuoren tai vastaavan on oltava läpinäkymätön. 3) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä henkilöstöä.	Perustason vaatimuksen 1 lisäksi: 1) Suojattavat aineistot lähetetään kirjattuna postina suljetussa, läpinäkymättömässä kaksinkertaisessa kirjekuoressa. Ulommassa kuoressa ei saa olla merkintää suojaustasosta. 2) Organisaation sisäiseen postin käsittelyketjuun saa kuulua vain hyväksyttyä henkilöstöä, jonka perehtymisoikeus ko. tiedon suojaustasoon on hyväksytty ja kirjattu. Henkilöllä on oltava esimiehensä määrittämä, työtehtäviinsä perustuva tarve perehtyä ko. aineistoon. 3) Lähetettäessä aineistoa kuriirin välityksellä, pakkauksen päällä tulee selkeästi ilmoittaa, että pakkauksen saa toimittaa vain kuriirin välityksellä. Kuriiri on koulutettava ja varustettava sekä kuriiritodistuksella, että kuriiripostikirjalla, johon vastaanottaja kuittaa vastaanottamansa lähetyksen.	Korotetun tason vaatimusten lisäksi: 1) Suojaustason II aineistoa ei lähetetä postitse, vaan lähetys toimitetaan perille joko henkilökohtaisesti tai viranomaisten suojaustasolle II hyväksymän kuriirimenettelyn välityksellä. 2) Kuriirimenettelyllä toimitettuna aineistojen on oltava kaksinkertaisessa kuoressa, joista sisäkuoren on oltava sinetöity. Vastaanottajan on tarkistettava sinetöinnin eheys ja ilmoitettava välittömästi, mikäli eheyden vaarantumista epäillään. 3) Organisaation sisäiseen suojaustason II postin käsittelyketjuun kuuluu vain tiedon omistajan hyväksymää henkilöstöä, joiden perehtymisoikeus ko. tiedon turvallisuusluokkaan on hyväksytty ja kirjattu. Henkilöllä on oltava työtehtävään perustuva, esimiehen määrittämä tarve perehtyä ko. aineistoon. Jokainen asiakirjaan perehtynyt henkilö kirjaa koko nimensä ja perehtymispäivämäärän aineiston etusivulle tai erilliseen kuittauskirjaan.	Välitys on hoidettu riskienarvioinnin perusteella riittävän turvalliseksi katsotulla menettelyllä.	ISO/IEC 27002 10.8.3, Kansallisen turvallisuusviranomaisen “Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”, VAHTI 2/2010	Suojaustason III tiedolle suositellaan, että sisempi kuori sinetöidään ja että vastaanottajaa vaaditaan tarkistamaan sinetöinnin eheys. Osaa kansainvälisistä suojaustason III aineistoista ei välitetä koskaan postin välityksellä, tarve tarkistetaan tapauskohtaisesti.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/poikkeama
I 607.0 **Pääkysymys: Pystytäänkö seuraamaan minne ja mistä suojattavat aineistot on välitetty?** *Lisäkysymys:* *Kirjataanko suojattavat aineistot?*	Ei vaatimuksia.	Ei välityksen seurantavaatimusta. Kirjataan. Huom! EU:n turvaluokiteltu tieto rekisteröidään/diarioidaan.	1) Suojaustason II tieto, riippumatta sen muodosta, rekisteröidään diaariin tai rekisteriin ennen välitystä ja vastaanotettaessa. Jos kyseessä on viestintä- ja tietojärjestelmä, kirjaamismenettelyt voidaan suorittaa sen omien prosessien avulla. 2) Suojaustason II tieto rekisteröidään omaan rekisteriinsä tai diaariin. 3) Diaaria/rekisteriä säilytetään, kuten suojaustason II asiakirjaa. 4) Diaarista/rekisteristä tulee käydä ilmi kunkin asiakirjan sen hetkinen haltija tiedon elinkaaren loppuun asti. 5) Suojaustason II tietojen käsittelystä tallennetaan käsittelytiedon sisältävät lokimerkinnät (vrt. I 504.0).	Ei erillissuosituksia.	Kansallisen turvallisuusviranomaisen “Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”, VAHTI 2/2010, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011		

Käyttöturvallisuus, osa-alue I700

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 701.0 **Pääkysymys: Onko huolehdittu, että organisaatiolla on toimintaansa nähden riittävät jatkuvuuden varmistavat suunnitelmat?** *Lisäkysymykset:* *Testataanko toipumisvalmiutta säännöllisesti?* *Turvataanko suojattavat tiedot myös hätätilanteissa?* *HUOM!* *Jatkuvuuden hallinnan yleiset auditointikysymykset on esitetty hallinnollisen turvallisuuden A600-osuudessa.*	1) Järjestelmien käytettävyysvaatimukset on määritetty. 2) On varmistettu, että kriittisten verkkojen (ml. Internet-yhteys), verkkolaitteiden, tietojärjestelmien, palvelinten ja vastaavien vikaantumisesta pystytään toipumaan toimintavaatimuksiin nähden riittävässä ajassa. 3) Suunnitelmissa otetaan huomioon suojattavien tietojen suojaus hätätilanteissa. Suojauksen on katettava tiedon luottamuksellisuus, eheys ja käytettävyys. 4) Suunnitelmiin sisältyy ennalta ehkäiseviä ja vaarantumistilanteen korjaamistoimenpiteitä.	1) Järjestelmien käytettävyysvaatimukset on määritetty. 2) On varmistettu, että kriittisten verkkojen (ml. Internet-yhteys), verkkolaitteiden, tietojärjestelmien, palvelinten ja vastaavien vikaantumisesta pystytään toipumaan toimintavaatimuksiin nähden riittävässä ajassa. 3) Suunnitelmissa otetaan huomioon suojattavien tietojen suojaus hätätilanteissa. Suojauksen on katettava tiedon luottamuksellisuus, eheys ja käytettävyys. 4) Suunnitelmiin sisältyy ennalta ehkäiseviä ja vaarantumistilanteen korjaamistoimenpiteitä.	1) Järjestelmien käytettävyysvaatimukset on määritetty. 2) On varmistettu, että kriittisten verkkojen (ml. Internet-yhteys), verkkolaitteiden, tietojärjestelmien, palvelinten ja vastaavien vikaantumisesta pystytään toipumaan toimintavaatimuksiin nähden riittävässä ajassa. 3) Suunnitelmissa otetaan huomioon suojattavien tietojen suojaus hätätilanteissa. Suojauksen on katettava tiedon luottamuksellisuus, eheys ja käytettävyys. 4) Suunnitelmiin sisältyy ennalta ehkäiseviä ja vaarantumistilanteen korjaamistoimenpiteitä.	1) Järjestelmien käytettävyysvaatimukset on määritetty. 2) On varmistettu, että kriittisten verkkojen (ml. Internet-yhteys), verkkolaitteiden, tietojärjestelmien, palvelinten ja vastaavien vikaantumisesta pystytään toipumaan toimintavaatimuksiin nähden riittävässä ajassa.	ISO/IEC 27002 14.1, ISO/ IEC 24762, ISO/IEC 27031, COBIT 4.1 DS4, VAHTI 8/2006, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 5. artikla, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010	Korkeiden käytettävyysvaatimusten ympäristöille vaaditaan jatkuvuus-/ toipumissuunnitelmaa, ja suunnitelman säännöllistä testaamista. Vrt. dokumentointivaatimus I 702.0, riskienarviointivaatimus A 401.2 ja LVIS-vaatimus F 218.0.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 702.0 **Pääkysymys: Mahdollistaako organisaatiossa saatavilla oleva dokumentaatio vioista, toimintahäiriöistä, hyökkäyksistä ja vastaavista toipumisen?** *Lisäkysymykset:* *Onnistuuko toipuminen, jos järjestelmän tai verkon vastuuhenkilö ei ole käytettävissä?* *Miten nopeasti toipuminen onnistuu? Seurataanko säännöllisesti, että suojattavaa tietoa käsittelevän ympäristön dokumentaatio on ajan tasalla?* *Miten menetellään, mikäli tiedoissa on puutteita?*	1) Verkot, järjestelmät ja niihin liittyvät asetukset on dokumentoitu siten, että viat ja toimintahäiriöt pystytään korjaamaan toimintavaatimusten mukaisesti. 2) Suojattavaa tietoa käsittelevän ympäristön dokumentaatio on yhdenmukainen toteutuksen kanssa. 3) Eroavaisuuksia käsitellään tietoturvapoikkeamina.	1) Verkot, järjestelmät ja niihin liittyvät asetukset on dokumentoitu siten, että viat ja toimintahäiriöt pystytään korjaamaan toimintavaatimusten mukaisesti. 2) Suojattavaa tietoa käsittelevän ympäristön dokumentaatio on yhdenmukainen toteutuksen kanssa. 3) Eroavaisuuksia käsitellään tietoturvapoikkeamina.	1) Verkot, järjestelmät ja niihin liittyvät asetukset on dokumentoitu siten, että viat ja toimintahäiriöt pystytään korjaamaan toimintavaatimusten mukaisesti. 2) Suojattavaa tietoa käsittelevän ympäristön dokumentaatio on yhdenmukainen toteutuksen kanssa. 3) Eroavaisuuksia käsitellään tietoturvapoikkeamina.	Verkot, järjestelmät ja niihin liittyvät asetukset on dokumentoitu siten, että viat ja toimintahäiriöt pystytään korjaamaan toimintavaatimusten mukaisesti.	ISO/IEC 27002 14.1, ISO/IEC 27002 10.1, VAHTI 2/2001, VAHTI 5/2004, VAHTI 8/2006, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010, http://www.interpol.int/public/technologycrime/crimeprev/companychecklist.asp, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	Käytännössä tämä vaatii usein verkon rakenteen, IP-osoitteiden, vyöhykkeiden, segmenttien, palomuurisäännöstöjen, verkkolaitteiden käyttöjärjestelmä-/firmware-versioiden, palvelinten ja tuotantojärjestelmien ohjelmistoversioiden ja asetusten, ja vastaavien tietojen, dokumentointia sillä tarkkuudella, että minkä tahansa vikaantumisesta pystytään toipumaan liiketoimintavaatimusten mukaisesti. Riippuen organisaation toimialasta ja tehtävistä, dokumentaation kattavuudelta saatetaan vaatia sitä, että ulkopuolinen osaa sen perusteella saattaa vikaantuneet verkot ja järjestelmät käyttökuntoon. Tulee myös huolehtia siitä, että dokumentaatio pidetään ajan tasalla. Yksi hyvä tapa ylläpitää dokumentaatiota on wiki, johon päivitetään verkon ja järjestelmien muutokset sitä mukaa, kun niitä tulee. Markkinoilla on myös muita ammattikäyttöön hyvin soveltuvia tuotteita.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 703.0 **Pääkysymys: Onko organisaatiossa selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita?** *Lisäkysymykset:* *Käytetäänkö vain hyväksymisprosessin läpäisseitä verkkoja ja järjestelmiä?* *Käytetäänkö suojattavan tiedon käsittelyyn vain viranomaisen hyväksymiä tiloja, verkkoja ja järjestelmiä? Miten varmistutaan tietojärjestelmien eheydestä?*	1) Käytössä on selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita. 2) Periaatteiden noudattamista valvotaan ja varmistetaan teknisin keinoin (esimerkiksi rajoittamalla asennus- ja asetusten muokkausoikeus vain ylläpitäjille). 3) Turva-asetusten ja -ohjelmien valtuuttamaton muokkaus on estetty peruskäyttäjiltä. 4) Organisaatiossa on olemassa uusien järjestelmien, järjestelmäpäivitysten ja vastaavien hyväksymiskriteerit. Vain hyväksymisprosessin läpäisseitä verkkoja ja järjestelmiä käytetään (vrt. muutoshallinta: A 608.0). 5) Suojattavan tiedon käsittelyyn käytetään vain viranomaisen hyväksymiä verkkoja ja järjestelmiä.	Perustason vaatimusten lisäksi: Suojattavan tiedon käsittely tapahtuu vain viranomaisen hyväksymässä fyysisessä tilassa.	Perustason vaatimusten lisäksi: Suojattavan tiedon käsittely tapahtuu vain viranomaisen hyväksymässä fyysisessä tilassa.	1) Käytössä on selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita. 2) Periaatteiden noudattamista valvotaan ja varmistetaan teknisin keinoin (esimerkiksi rajoittamalla asennus- ja asetusten muokkausoikeus vain ylläpitäjille). 3) Turva-asetusten ja -ohjelmien valtuuttamaton muokkaus on estetty peruskäyttäjiltä.	ISO/IEC 27002 10.3.2, ISO/IEC 27002 12.1.1, ISO/IEC 27002 12.4.1, Kansallisen turvallisuusviranomaisen "Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje", VAHTI 8/2006, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 9.ja 10. artikla, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 704.0 **Onko organisaatiossa otettu käyttöön periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan?**	1) Organisaatiossa on käytössä periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan. 2) Periaatteista ja vaadittavista mekanismeista on tiedotettu henkilöstölle. 3) Turvallisesta etä- ja matkatyöskentelystä on henkilöstön saatavilla ohje. 4) Laitteita, tietoaineistoja tai ohjelmia ei siirretä pois työpaikalta ilman ennalta saatua valtuutusta. 5) Järjestelmien etähallinnassa tai -käytössä käytetään vahvoja todennusmenettelyjä. 6) Suojattavaa tietoa sisältävät välineet on suojattu luvatonta pääsyä, väärinkäyttöä ja turmeltumista vastaan, kun niitä kuljetetaan organisaation fyysisten rajojen ulkopuolelle. 7) Toimitilojen ulkopuolelle vietyjä laitteita ja tietovälineitä ei jätetä valvomatta julkisille paikoille, kannettavat tietokoneet kuljetetaan matkustaessa käsimatkatavarana. 8) Vain luotettavia ja käyttöympäristöön hyväksyttyjä laitteita (esim. työnantajan tarjoama kannettava tietokone) ja etätyöyhteyksiä käytetään.	Suojaustason III järjestelmien etähallinta on lähtökohtaisesti estetty. Etähallinta on sallittu vain viranomaisen erikseen hyväksymällä menettelyllä.	Suojaustason II järjestelmien etähallinta on estetty. Viranomaisten tiedonvälitysjärjestelmissä voidaan tapauskohtaisesti hyväksyä rajattu etähallinta.	1) Organisaatiossa on käytössä periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan. 2) Periaatteista ja vaadittavista mekanismeista on tiedotettu henkilöstölle.	ISO/IEC 27002 10.8.3, ISO/IEC 27002 11.4.2, ISO/IEC 27002 11.7.1, ISO/IEC 27002 11.7.2, ISO/IEC 27002 9.2, ISO/IEC 27002 9.2.5, ISO/IEC 27002 9.2.7, VAHTI 1/2001, VAHTI 2/2003, VAHTI 8/2006	Suojaustasolla IV hyväksyttävä etäkäyttö- ja etähallintaratkaisu edellyttää liikenteen luotettavan salauksen lisäksi tyypillisesti vahvaa käyttäjätunnistusta ja käytön teknistä sitomista työnantajan tarjoamaan etäkäyttölaitteistoon (esim. laitetunnistus). Erityisesti etähallinnassa huomioitava myös etähallintapisteen looginen ja fyysinen sijainti. Suojaustasolla III hyväksyttävä etähallintamenettely huomioi mm. etähallintapisteiden fyysisen ja loogisen pääsynvalvonnan, hallintaan käytetyt laitteistot ja ohjelmistot, hallintaliikenteen salauksen, ja edellä mainittujen elementtien luotettavuuden erityisesti luottamuksellisuuden ja eheyden suhteen.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
						Viranomaisten suojaustason II järjestelmissä voidaan tapauskohtaisesti hyväksyä rajattu etähallinta. Tapauskohtaisesti hyväksyttävällä etähallinnalla tarkoitetaan tässä yhteydessä lähes poikkeuksetta turvapäivitysten ja haittaohjelmatunnistekantojen keskitettyä jakelua. Jotta etähallinta voidaan hyväksyä, tulee viranomaisen tekemässä järjestelmällisessä ja kokonaisvaltaisessa riskienarvioinnissa päätyä aina tulokseen, jossa etähallinta on paikallista hallintaa merkittävästi pienempi riski. Tällaisen etähallinnan hyväksyminen edellyttää aina myös päivityspalvelimen sisällyttämistä samaan tietojärjestelmään ja sen fyysistä eristämistä muista järjestelmistä.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 705.0 **Ovatko kehitys-/ testaus ja tuotantojärjestelmät erilliset?**	1) Kehitys-/testaus- ja tuotantojärjestelmien on oltava erilliset. 2) Ennen uuden järjestelmän käyttöönottoa, testidatat, oletus- ja testikäyttäjätilit ja vastaavat poistetaan. 3) Suojattavaa tietoa ei kopioida testaus- tai kehitysympäristöön, mikäli niiden suojaustaso on alhaisempi kuin tuotantoympäristön.	1) Kehitys-/testaus- ja tuotantojärjestelmien on oltava erilliset. 2) Ennen uuden järjestelmän käyttöönottoa, testidatat, oletus- ja testikäyttäjätilit ja vastaavat poistetaan. 3) Suojattavaa tietoa ei kopioida testaus- tai kehitysympäristöön, mikäli niiden suojaustaso on alhaisempi kuin tuotantoympäristön.	1) Kehitys-/testaus- ja tuotantojärjestelmien on oltava erilliset. 2) Ennen uuden järjestelmän käyttöönottoa, testidatat, oletus- ja testikäyttäjätilit ja vastaavat poistetaan. 3) Suojattavaa tietoa ei kopioida testaus- tai kehitysympäristöön, mikäli niiden suojaustaso on alhaisempi kuin tuotantoympäristön.	1) Kehitys-/testaus- ja tuotantojärjestelmien on oltava erilliset. 2) Ennen uuden järjestelmän käyttöönottoa, testidatat, oletus- ja testikäyttäjätilit ja vastaavat poistetaan.	ISO/IEC 27002 10.1.4, PCI DSS 6.3.2, PCI DSS 6.3.4, PCI DSS 6.3.5, PCI DSS 6.3.6	Tuotantojärjestelmän on oltava erillinen, jotta kehitys- tai testaustoimet eivät aiheuta tuotantokatkoksia tai turvallisuuspuutteita. Tuotantodataa voidaan kopioida kehitys-/testausympäristöön, mikäli data sanitoidaan siten, että luottamuksellisuus ei vaarannu. Vrt. muutoshallinta: A 608.0.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 706.0 **Pääkysymys: Miten varmistetaan, että verkossa ja sen palveluissa ei ole tunnettuja haavoittuvuuksia?** *Lisäkysymykset:* *Onko tietoturvatiedotteiden seuranta vastuutettu?* *Onko turvapäivitysten asentamiseen luotu menettelytavat?* *Valvotaanko niiden toteutumista?*	1) Viranomaisten (esim. CERT-toimijat), laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeelliset turvapäivitykset asennetaan hallitusti. 2) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat skannataan vuosittain haavoittuvuuksien löytämiseksi.	Perustason vaatimuksen 1 lisäksi: Skannaus suoritetaan vähintään puolivuosittain ja aina merkittävien muutosten jälkeen.	Perustason vaatimuksen 1 lisäksi: Skannaus suoritetaan vähintään puolivuosittain ja aina merkittävien muutosten jälkeen.	Viranomaisten (esim. CERT-toimijat), laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeelliset turvapäivitykset asennetaan hallitusti.	ISO/IEC 27002 12.6.1, ISF-SOGP CI3.6, PCI DSS 6.1, PCI DSS 6.2, PCI DSS 11.2, VAHTI 8/2006, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf, http://www.sans.org/critical-security-controls/control.php?id=10 Tietoturva-tiedotteita: http://cert.fi/palvelut/postituslistat.html, http://www.securityfocus.com/archive/1	Esimerkkejä käytännön toteutuksesta: Sähköpostiin on tilattu CERT-toimijoiden sekä valmistajien tiedotukset. Tiedotuksista poimitaan sellaiset, jotka vaikuttavat organisaation järjestelmien turvallisuuteen, ja ne asennetaan käyttöjärjestelmiin, verkkolaitteisiin (lähinnä firmwaret), palvelinsovelluksiin jne. Päivitysten vaikutukset tulisi mahdollisuuksien mukaan testata ennen tuotantoympäristöön asennusta. Testaus voidaan suorittaa esimerkiksi eristetyssä testiympäristössä tai pienellä käyttäjäjoukolla. "Merkittäviin muutoksiin" voidaan laskea esimerkiksi verkkotopologian muutokset, uusien järjestelmien mukaan tuonnit ja/tai vanhojen merkittävät päivitykset, palomuurien ja vastaavien suodatussääntöjen merkittävät muutokset, jne.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 707.0 **Miten varmistutaan siitä, että työskentelytauoilla tai työskentelyn jälkeen laitteet eivät jää ilman riittävää suojaa?**	1) Käyttäjät velvoitetaan seuraavantapaiseen käytäntöön: a) Työasema, pääte, kannettava tietokone tai vastaava lukitaan aina (esim. salasanasuojatulla näytönsäästäjällä tai muulla menettelyllä), kun laitteelta poistutaan. b) Aktiiviset istunnot päätetään työn päättyessä ja pitemmillä tauoilla (esim. etäyhteydet ja palvelinistunnot puretaan). c) Laitteesta/järjestelmästä kirjaudutaan ulos työn päättyessä. 2) Mikäli suojattavaa tietoa sisältävä laite joudutaan jättämään tilaan, jossa siihen on fyysinen pääsy ei-luotetuilla (arvioitava tapauskohtaisesti: esim. organisaation ulkopuolisilla), suojaus on aktivoitava laitteelta poistuttaessa (esim. sammuttamalla kannettava tietokone, jolloin salaus aktivoituu).	Perustason vaatimuksen 1 lisäksi: Suojaustason III aineistoa sisältävää laitetta ei lähtökohtaisesti jätetä tilaan, jossa siihen on pääsy ei-luotetuilla.	Perustason vaatimuksen 1 lisäksi: Suojaustason II aineistoa sisältävää laitetta ei lähtökohtaisesti jätetä tilaan, jossa siihen on pääsy ei-luotetuilla.	Käyttäjät velvoitetaan seuraavantapaiseen käytäntöön: a) Työasema, pääte, kannettava tietokone tai vastaava lukitaan aina (esim. salasanasuojatulla näytönsäästäjällä tai muulla menettelyllä), kun laitteelta poistutaan. b) Aktiiviset istunnot päätetään työn päättyessä ja pitemmillä tauoilla (esim. etäyhteydet ja palvelinistunnot puretaan). c) Laitteesta/järjestelmästä kirjaudutaan ulos työn päättyessä.	ISO/IEC 27002 11.3.2	Vrt. työasemien ja vastaavien automaattinen lukittuminen: I 502.0	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 708.0 **Onko käytössä ns. puhtaan pöydän politiikka? Koskeeko sama periaate myös näyttöjä?**	1) Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka on käytössä. 2) Huolehditaan siitä, ettei neuvottelutiloihin jää suojattavaa tietoa sisältäviä asiakirjoja tai muita muistiinpanoja kokousten jälkeen.	1) Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka on käytössä. 2) Huolehditaan siitä, ettei neuvottelutiloihin jää suojattavaa tietoa sisältäviä asiakirjoja tai muita muistiinpanoja kokousten jälkeen.	1) Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka on käytössä. 2) Huolehditaan siitä, ettei neuvottelutiloihin jää suojattavaa tietoa sisältäviä asiakirjoja tai muita muistiinpanoja kokousten jälkeen.	1) Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka on käytössä. 2) Huolehditaan siitä, ettei neuvottelutiloihin jää suojattavaa tietoa sisältäviä asiakirjoja tai muita muistiinpanoja kokousten jälkeen.	ISO/IEC 27002 11.3.3, VAHTI 8/2006		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 709.0 **Pääkysymys: Onko huolehdittu riittävästä työtehtävien eriyttämisestä niin, ettei synny ns. vaarallisia työyhdistelmiä?** *Lisäkysymys:* *Onko huolehdittu siitä, että kriittiset ylläpitotoimet vaativat kahden tai useamman henkilön hyväksynnän?*	Ei vaatimuksia.	1) Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. 2) Vaarallisia työyhdistelmiä tulee välttää. Mikäli niitä kuitenkin syntyy, on niitä varten oltava valvontamekanismi. 3) On määritettävä järjestelmäkohtaisesti ne kriittiset toimet, joihin erityisvalvonta kohdistetaan.	1) Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. 2) Vaarallisia työyhdistelmiä tulee välttää. Mikäli niitä kuitenkin syntyy, on niitä varten oltava valvontamekanismi. 3) On määritettävä järjestelmäkohtaisesti ne kriittiset toimet, joihin erityisvalvonta kohdistetaan.	Tehtävät ja vastuualueet on riskienarvioinnin mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä.	ISO/IEC 27002 10.1.3, VAHTI 8/2006, COBIT 4.1 PO4.10	Tyypillinen vaatimus erityisesti kansainvälistä turvaluokiteltua tietoa käsittelevälle järjestelmälle on se, että järjestelmälle vaaditaan erilliset roolit (ja henkilöt) järjestelmän ylläpitoon (security administrator) ja lokien tarkkailuun (audit administrator). Esimerkki valvontamekanismista: Kriittiset ylläpito- ja vastaavat toimet vaativat kahden tai useamman henkilön hyväksynnän (two man rule). Vrt. muutoshallinta (A 608.0) ja kirjausketjut (I 504.0).	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 710.0 **Onko riittävästä varmuuskopioinnista huolehditu?**	1) Toimintavaatimuksiin nähden riittävästä varmuuskopioinnista on huolehdittu. 2) Varmuuskopiot säilytetään eri fyysisessä sijainnissa kuin varsinainen järjestelmä. 3) Varmuuskopioihin pääsy on estetty muilta kuin valtuutetuilta käyttäjiltä. 4) Suojattavaa tietoa sisältävät varmuuskopiot säilytetään tiedon tason edellyttämässä tilassa ja tarvittaessa salakirjoitettuna.	Perustason vaatimusten lisäksi: Varmistusmedioista on olemassa listat.	Perustason vaatimusten lisäksi: Varmistusmedioista on olemassa listat.	1) Toimintavaatimuksiin nähden riittävästä varmuuskopioinnista on huolehdittu. 2) Varmuuskopiot säilytetään eri fyysisessä sijainnissa kuin varsinainen järjestelmä. 3) Varmuuskopioihin pääsy on estetty muilta kuin valtuutetuilta käyttäjiltä.	ISO/IEC 27002 10.5.1, PCI DSS 9.5, COBIT 4.1 DS4, COBIT 4.1 DS11, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	Varmuuskopiointi tulee aina mitoittaa toimintavaatimuksiin. Toimintavaatimuksiin nähden riittävä varmuuskopiointi huomioi ainakin seuraavat: 1) Varmistusten taajuus on riittävä varmistettavan tiedon kriittisyyteen nähden. Edellyttää selvitystä siitä, kuinka paljon dataa voidaan menettää (recovery point objective, RPO). 2) Palautusprosessin nopeus on riittävä toimintavaatimuksiin nähden. Edellyttää selvitystä siitä, kuinka kauan palautuminen voi kestää (recovery time objective, RTO). 3) Varmuuskopioinnin ja palautusprosessin oikea toiminta testataan säännöllisesti. 4) Palautusprosessin dokumentointi on riittävällä tasolla. 5) Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä (eri sortuma-/palotila, välimatka varmuuskopion ja varsinaisen tilan välillä, jne.)	

LIITE 1: TARKENNUKSIA AUDITOINTIKYSYMYKSIIN

A 401.1

1) Suojattavien kohteiden tunnistaminen voidaan todentaa esimerkiksi siten, että listataan suojattavat kohteet ja niihin kohdistuvat suojaamistarpeet eheyden, luottamuksellisuuden ja käytettävyyden osalta.
2) Vastaavasti uhat esimerkiksi siten, että pyydetään listaamaan tunnistetut uhat per suojattava kohde.
3) Voidaan todentaa pyytämällä listaus suojattavista kohteista ja niiden vastuuhenkilöistä.
4) Erityisesti varmistettava, että organisaatiolle kriittisten järjestelmien suojaukset ovat riittäviä.

A 401.2

Perustaso (IV):
1 & 2) Voidaan todentaa esimerkiksi kuvailemalla käytetty menetelmä ja näyttämällä menetelmän tuottamat päivätyt "tulosraportit". Esimerkkejä: http://www.pk-rh.fi/.
3 & 4) Erityisesti varmistettava, että organisaatiolle kriittisten järjestelmien suojaukset ovat riittäviä.

A 608.0

Vaatimuksen voi toteuttaa esimerkiksi siten, että merkittävimpien muutosten prosessiin kuuluu muutosten tunnistaminen ja kirjaaminen, muutosten suunnittelu ja testaus, muutosten mahdollisten vaikutusten arviointi mukaan lukien turvallisuusvaikutukset ja ehdotettujen muutosten virallinen hyväksymisprosessi.
Hyväksyttävä muutoshallintamenettelytoteutus riippuu merkittävästi organisaation/kohteen koosta sekä käsiteltävän tiedon suojaustasosta. Erityisesti kansainvälistä turvaluokiteltua tietoa käsittelevissä verkoissa/järjestelmissä muutokset tulee yleensä lisäksi etukäteishyväksyttää tiedon omistajalla tai sen valtuuttamalla taholla (yleensä turvallisuusjärjestelyt hyväksyvä viranomainen, Security Accreditation Authority, Suomessa Viestintäviraston NCSA-FI). Tyypillisesti järjestelmähyväksynnän yhteydessä määritellään yksityiskohtaiset ehdot sille, millaiset muutokset sallitaan ilman etukäteishyväksyttämistä.

F201.0

Lattiasuositus tasoille III ja II: betoninen ontelolaattarakenne + erillinen pintavalu.
Seinärakennesuositus tasoille III ja II: betonivaluharkkorakenne terästettynä tai vähintään 15 cm paksuinen teräsbetoni. Seinä-, lattia- ja kattorakenteiden toteutuksessa on syytä huomioida myös rakenteellisen paloturvallisuuden vaatimukset.

F 205.0

Ovirakenteet: murtosuojattujen ovien osalta on suosituksena käyttää ns. kombi-ovia, joissa on huomioitu ääneneristyksen lisäksi myös paloturvallisuusvaatimukset

F209.1

Voidaan käytännössä toteuttaa esimerkiksi siten, että kaikkien työntekijöiden, toimittajien ja ulkopuolisten käyttäjien pääsy- ja käyttöoikeudet katselmoidaan säännöllisin väliajoin, esim. 6 kuukauden välein. Lisäksi muutoksissa, kuten ylennyksissä, alennuksissa, työnkierron yhteydessä ja erityisesti työsuhteen päättymisen yhteydessä oikeuksien muuttamiseen/poistamiseen on oltava selkeä ja toimiva menettelytapa. Tämä voi tapahtua esimerkiksi siten, että esimies ilmoittaa muutoksista etukäteen vastuuhenkilöille, jolloin kaikki oikeudet saadaan pidettyä sopivina. Tämä voi tarkoittaa käytännössä esimerkiksi sitä, että käyttö- ja pääsyoikeudet poistetaan/muutetaan keskitetystä hallintajärjestelmästä tai yksittäisistä järjestelmistä erikseen.

F217.0

Elektronisten laitteiden vientikielto voidaan joissain tilanteissa korvata esim. irrottamalla akut. Käsiteltäessä kansainvälisen yhteisön (esim. EU) turvaluokiteltua tietoa, hajasäteilysuojaus vaaditaan pääsääntöisesti suojaustasolta III (Confidential) lähtien. Käsiteltäessä kansallista tai yksittäisen toisen valtion turvaluokiteltua tietoa, hajasäteilysuojaus edellytetään yleensä joko suojaustasolta III (Confidential) tai suojaustasolta II (Secret) lähtien. Hajasäteilyltä suojautuminen on hoidettava toimitilan fyysisen sijainnin valinnalla, vuorauksella tai käyttämällä suojattuja laitteistoja ja kaapelointeja.

F218.0

Määrityksellä "toimintavaatimusten mukaisesti" tarkoitetaan sitä, että mikäli järjestelmän käytettävyysvaatimukset ovat korkeat, soveltuvia varmistuksia vaaditaan. Varmistukset voivat käytännössä tarkoittaa esimerkiksi tärkeiden laitteiden ja laitetilojen suojaamista ympäristötekijöitä vastaan (mm. murto, palo, lämpö, kaasut, pöly, tärinä, vesi). Varmentavia toimia voivat olla myös toimintakriittisten laitteistojen kahdentaminen ja/tai varustaminen häiriöttömällä sähkönsyötöllä (UPS). Korkeiden käytettävyysvaatimusten järjestelmille vaaditaan varmennusten toiminnan säännöllistä testaamista.

I 401.0

Suojaustason IV käsittely-ympäristöjä on mahdollista kytkeä Internetiin ja muihin ei-luotettuihin verkkoihin, kunhan suojaustason muut vaatimukset täyttyvät. Tyypillinen käyttötapa suojaustason IV käsittely-ympäristölle on organisaation "toimistoverkko".
Suojaustason III käsittely-ympäristöt ovat lähtökohtaisesti fyysisesti ei-luotetuista verkoista/järjestelmistä eristettyjä kokonaisuuksia. Suojaustason III käsittely-ympäristöihin ei pääsääntöisesti kytketä mitään muita verkkoja/järjestelmiä. Viranomainen voi tapauskohtaisesti hyväksyä suojaustason III käsittely-ympäristön fyysisen kytkemisen erikseen tarkastettuun ja hyväksyttyyn verkkoon/järjestelmään. Tällaiset erikseen hyväksytyt verkot/järjestelmät jakautuvat pääsääntöisesti neljään käyttötilanteeseen:

A. Tiedonsiirtojärjestelmät
Suojaustason III järjestelmä/verkko voi olla tiedonsiirtojärjestelmä kahden tai useamman fyysisen pisteen välillä. Tällöin jokaisen kytketyn pisteen tulee olla turvallisuustasoltaan vastaavalla tasolla. Verkkotason rajapinta on useimmiten muotoa [fyysisesti eristetty verkko/työasema] - [rauta- tai ohjelmistopalomuuri] – [suojaustasolle hyväksytty salauslaite] - [rautapalomuuri] - [Internet] – [rautapalomuuri] - [suojaustasolle hyväksytty salauslaite] - [rauta- tai ohjelmistopalomuuri] - [fyysisesti eristetty verkko/työasema]. Ks. hyväksytyt salausratkaisut vaatimuksesta I 509.0. Vastaava järjestely voidaan viranomaisten järjestelmissä tapauskohtaisesti hyväksyä myös suojaustasolla II.

B. Palvelujärjestelmät
Suojaustason III järjestelmä/verkko voi olla esimerkiksi tietokantapalvelu, jota käytetään useasta fyysisestä pisteestä. Verkkotason rajapinta on tällöin vastaava kuin käyttötilanne A:ssa.

C. Yhdyskäytäväratkaisut
C1. Suojaustason III tiedon käsittely-ympäristöön voidaan siirtää tietoa alemman suojaustason ympäristöstä erillisen, vain yksisuuntaisen liikenteen sallivan datadiodin kautta. Vastaava järjestely voidaan viranomaisten järjestelmissä hyväksyä tapauskohtaisesti myös suojaustasolla II.
C2. Suojaustason III tiedon käsittely-ympäristöstä käsin tapahtuva loppukäyttäjän alemman suojaustason ympäristöjen tiedon käsittely voidaan toteuttaa terminoidulla yhdyskäytäväratkaisulla (esim. tietyt virtuaalityöpöytäympäristöt). Vastaava järjestely voidaan tapauskohtaisesti hyväksyä viranomaisten tietyissä erityisjärjestelmissä myös suojaustasolta II suojaustasolle III.
C3. Suojaustason III tiedon käsittely-ympäristössä alemman tai vastaavan suojaustason verkon käyttö voi tapahtua tiukasti rajatun, liikennettä ja sisältöä suodattavan yhdyskäytäväratkaisun kautta, missä sisällönsuodatus tapahtuu palvelinten välisessä tietoliikenteessä protokolla- ja/tai sovellustasolla.

D. Muut käsittely-ympäristöt
Muut suojaustason III käsittely-ympäristöt ovat yleisimmin organisaation tuotekehitysverkkoja ja muita suojaustason III tiedon käsittely-ympäristöjä. Yleisin järjestelmä, jonka viranomainen voi hyväksyä kytkettäväksi tällaiseen ympäristöön, on vain tätä ympäristöä palveleva päivityspalvelin. Päivityspalvelimelta voidaan sallia keskitetty turvapäivitysten ja haittaohjelmatunnisteiden jakelu tietyin rajauksin. Jaeltavat päivitykset ja tunnistekannat tuodaan päivityspalvelimelle pääsääntöisesti ilmaraon yli. Tapauskohtaisesti voidaan hyväksyä myös ratkaisu, jossa jaeltavat päivitykset ja tunnistekannat haetaan suoraan Internetistä. Tällöin päivityspalvelin tulee koventaa äärimmilleen, sallia yhteydet Internetiin verkko- ja sovellustasoilla vain valmistajien päivitystenjakopalveluihin, ja yhteys suojaustason III verkkoon rajata vain päivitysten jakelussa välttämättömiin yhteyksiin. Jälkimmäinen rajaus voidaan tehdä joko vain yhteen suuntaan liikennettä sallivan datadiodin tai muun luotettavaksi katsottavan ratkaisun kautta.
Suojaustason III verkkoon kytkettäväksi järjestelmäksi voidaan tapauskohtaisesti hyväksyä myös CD-levy tai USB-muisti.
Yrityksille voidaan pääsääntöisesti hyväksyä vain käyttötapaus D:n käsittely-ympäristöjä. Suojaustason III ympäristöksi voidaan tapauskohtaisesti hyväksyä niin sanottu monihankeverkko, jossa on tietyin rajoituksin mahdollista käsitellä useamman hankkeen tietoja. Suojaustasolla II edellytetään aina hankekohtaista erillisympäristöä.
Tapauskohtaisissa hyväksynnissä viranomaisena oltava tiedon omistaja tai omistajan valtuuttama taho. Esimerkiksi kansainvälisten turvaluokiteltujen tietoaineistojen tapauksessa edellytetään turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA, Security Accreditation Authority, Suomessa Viestintäviraston NCSA-FI) tarkastusta ja hyväksyntää.

I 402.0

Suojaustason IV vaatimus 2 on työasemilla ja kannettavilla tietokoneilla usein helpointa toteuttaa sovelluspalomuurilla, johon on määritetty sallitut ohjelmistot ja estetty muiden liikennöinti.
Suojaustason IV vaatimuksessa 5 kannattaa huomioida, että tietyissä kansainvälistä aineistoa käsittelevissä verkoissa on mahdollista sallia vain etukäteishyväksyttyihin kohteisiin (whitelisting) suuntautuva web-selailu.
Palvelunestohyökkäysten vaikutuksia voidaan pienentää muun muassa 1) riittävän tiedonsiirto-, verkkolaite- ja palvelinkapasiteetin varmistamisella, 2) varayhteyksillä (fyysisesti eri reittiä tuleva yhteys, eri operaattorilta tuleva yhteys, vaihtoehtoiset tiedonsiirtomediat kuten radiolinkki- ja satelliittiyhteydet), 3) tekemällä operaattorin kanssa sopimus jatkuva-aikaisesta tai erillisestä ilmoituksesta käynnistyvästä operaattorin suorittamasta haitallisen liikenteen puhdistamisesta (data scrubbing). Roskapostitulvan haitallisia vaikutuksia voidaan pienentää suodatuksilla (operaattoriverkossa, organisaatioverkon reunalla, työasemissa) sekä asettamalla liitetiedostoille suurin sallittu koko.

Vrt. verkkolaitteiden koventamisvaatimukset: I 405.0.

I 405.0

Verkon aktiivilaitteilla tarkoitetaan tässä yhteydessä palomuureja, reitittimiä, kytkimiä, langattomia tukiasemia ja vastaavia laitteita/järjestelmiä. Vrt. I 502.0, erityisesti lähteet. Mikäli verkkolaitteen hallinta ei ole mahdollista käyttäjän yksilöivällä käyttäjätunnuksella, tulee yhteiskäyttöisten (ylläpito-)tunnusten käyttöön olla sovittu turvalliset käyttösäännöt (ks. I 501.0). Mikäli ympäristön koko (lähinnä verkkolaitteiden, erityisesti reitittimien määrä) on suurehko, todennuksen järjestämiseen suositellaan kahdennettujen AAA-palvelimien (erityisesti TACACS+, RADIUS, tai Kerberos) hyödyntämistä. Huomattava lisäksi, että oletussalasanojen vaihto kattaa myös SNMP:n yhteisösalasanat (Community Strings).

Suojaustason IV vaatimuksen 6 menettelylle on valmistajakohtaisia nimeämiskäytäntöjä, mm. “private VLAN” ja/tai “protected port.”

Suojaustason III vaatimus 1:n toteuttamisessa suositellaan käytettävän kaikkien syötettyjen hallintakomentojen nauhoittamista.

Huom: vrt. lokitusvaatimus I 504.0, suodatusvaatimus I 402.0 sekä myös I 508.0.

I 502.0

Perustasolla (IV):

Työasemat ja kannettavat tietokoneet:

1) Alusta sisältää vain järjestelmän tarvitsemia ohjelmistokomponentteja.
2) Käyttöjärjestelmään ja sovellusohjelmistoihin on asennettu tarpeelliset turvapäivitykset.
3) Järjestelmiin asennuksen yhteydessä automaattisesti luoduille tileille (esim. “administrator” ja “guest”) on oikeudet rajattu minimiin tai poistettu käytöstä.
4) Oletussalasanat on vaihdettu.
5) Työasemat lukittuvat automaattisesti, jos niitä ei käytetä vähään aikaan (minimivaatimus: salasanasuojattu näytönsäästäjä aktivoituu 10 minuutin käyttämättömyyden jälkeen).
6) Käyttöoikeudet asetettu F 209.1:n mukaisesti.
7) Lokimenettelyt asetettu (lisätietoa: I 504.0).
8) Käyttöjärjestelmän tunnettuja turvallisuusuhkia sisältävät automaattisen ohjelmakoodin suorituksen mahdollistavat ominaisuudet on kytketty pois päältä (erityisesti PDF-tiedostojen automaattinen esikatselu sekä “autorun” ja ”autoplay”-toiminnallisuudet).
9) Ohjelmistot, erityisesti web-selaimet, PDF-lukijat, toimisto-ohjelmistot ja sähköpostiohjelmistot, ovat turvallisesti konfiguroituja.

9.1) Sähköpostiohjelmistot: a) Ajettava koodi oletuksena estetty. b) HTML-muotoisen sähköpostin lähettäminen estetty ja sen vastaanottamisessa viestit muunnetaan tekstimuotoon. c) Sähköpostin automaattinen esikatselu poistettu käytöstä. d) Liitetiedostoja ei avata automaattisesti. e) Sähköpostin liitteinä sallitaan vain erikseen määritellyt tiedostotyypit. Muiden käyttö on teknisesti estetty esimerkiksi ne pois suodattamalla ja asiaankuuluvasti aiheesta viestiin merkitsemällä. f) Roskapostiksi tulkittava liikenne suodatetaan pois tai merkitään vähintään varoitus esim. viestin otsikkokenttään.

9.2) PDF-lukijat, tekstinkäsittelyohjelmistot ja vastaavat: ajettavan koodin (erityisesti JavaScript ja makrot) suorittaminen on oletuksena estetty.

Palvelimet, työasemavaatimusten lisäksi:

1) Alustan komponenttien, prosessien (esim. palvelinprosessit), hakemistojen ja lisäohjelmien käyttöoikeudet on asetettu tarkoituksenmukaisiksi vähimpien oikeuksien periaatteen mukaisesti.
2) Palvelimet on konfiguroitu valmistajien ja luotettujen tahojen ohjeiden mukaisesti.
3) Sähköpostipalvelimet eivät salli a) releöintiä (open relay), b) osoitteen ja listan jäsenyyden tarkistusta (komennot “VRFY” ja “EXPN”), c) suojaamattomia käyttäjäyhteyksiä (vaaditaan TLS/SSL tai vast.), d) liian suuria liitetiedostoja.

Verkkolaitteet: I 405.0.
Verkkotulostimet, puhelinjärjestelmät ja vastaavat:
Soveltaen vastaavat vaatimukset kuin työasemilla ja palvelimilla: palvelut (erityisesti verkkopalvelut) karsittava tarvittaviin, oletushallintatunnukset vaihdettava, tarpeelliset turvapäivitykset asennettava.

Korotettu taso (III)
Työasemat, kannettavat tietokoneet ja palvelimet:

1) Tarjottavat (erityisesti verkko-)palvelut on minimoitu ja rajattu vain välttämättömiin. Verkkojaot poistettu aina käytöstä, kun laite kytkeytyy ei-luotettuun verkkoon.
2) Käyttöjärjestelmät ja muut ohjelmistot konfiguroidaan siten, että päivitykset haetaan vain tähän tarkoitukseen tarkoitetuista lähteistä ja kaikki tarpeeton verkkoliikennöinti on poistettu käytöstä.
3) BIOS-asetukset on asetettu turvallisuutta tehostaviksi ja asetusten muuttaminen on estetty valtuuttamattomilta käyttäjiltä: a) BIOS-asetuksiin pääsy on suojattu salasanalla. b) On sallittu vain ensisijaiselta kovalevyltä käynnistys. c) Tarpeettomat palvelut ja portit on poistettu käytöstä.

Korotetun tason (III) vaatimuksella 2 pyritään siihen. että esimerkiksi sovellusten tuottama päivitysten ”huhuilu” saadaan minimoitua, ja siten parannettua luvattoman liikenteen havainnointikykyä. Käytännössä tämä tarkoittaa mm. sitä, että mikäli sovellusten ei haluta päivittävän itseään automaattisesti (tai se ei ole käyttöoikeuksien puolesta mahdollista), sovellukset konfiguroidaan olemaan ”huhuilematta” verkkoon tarpeettomasti.

I 503.0

Suositellaan, että torjuntaohjelmistojen tuottamia havaintoja seurataan keskitetyllä hallintajärjestelmällä.
Järjestelmissä, joita ei kytketä julkiseen verkkoon, haittaohjelmatunnisteiden päivitys voidaan järjestää esimerkiksi käyttämällä hallittua suojattua päivitystenhakupalvelinta, jonka tunnistekanta pidetään ajan tasalla esimerkiksi erillisestä Internetiin kytketystä järjestelmästä tunnisteet käsin siirtämällä (esim. kerran vuorokaudessa). Erityisesti II-tason järjestelmissä päivitykset joudutaan usein asentamaan käsin. Kummassakin tapauksessa tulee varmistua päivitysten eheydestä (lähde, tarkistussummat, jne.).
Suojaustasoja III ja II koskevat vaatimukset pyrkivät pienentämään erityisesti USB-muistien välityksellä leviävien haittaohjelmien riskiä. Tapauskohtaisesti voidaan edellyttää esimerkiksi sitä, että järjestelmään kytketään vain erikseen määritettyjä luotettavaksi todennettuja muistitikkuja (ja vastaavia), joita ei kytketä mihinkään muuhun järjestelmään. Tapauskohtaisesti voidaan hyväksyä esimerkiksi järjestely, jossa vain organisaation tietohallinnon (tai vast.) jakamia muistivälineitä voidaan kytkeä organisaation järjestelmiin, ja että kaikkien muiden muistivälineiden kytkeminen on kielletty ja/tai teknisesti estetty. Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, on määriteltävä menetelmät, jolla pienennetään tämän aiheuttamaa riskiä. Menetelmänä voidaan tapauskohtaisesti hyväksyä esimerkiksi se, että ei-luotetusta lähteestä tuleva muisti kytketään eristettyyn tarkastusjärjestelmään, jonne siirrettävä tieto siirretään, ja josta siirrettävä tieto viedään edelleen luotettuun järjestelmään erillistä muistivälinettä käyttäen. Huom: Järjestelyn on huomioitava suojaustasolla III vähintään muistialueen tarkastaminen. Suojaustasolla II on huomioitava myös muistivälineen kontrolleritason räätälöinnin uhat.

I 504.0

Kattavuusvaatimuksen voi useimmin toteuttaa siten, että varmistaa, että ainakin työasemien, palvelinten, verkkolaitteiden (erityisesti palomuurien, myös työasemien sovellusmuurien) ja vastaavien lokitus on päällä. Verkkolaitteiden lokeista on pystyttävä jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta (vrt. I 405.0).
Tapahtumalokeja olisi syytä kerätä järjestelmän toiminnasta, käyttäjäaktiviteeteista, turvaan liittyvistä tapahtumista ja poikkeuksista. Eräs suositeltu tapa lokien turvaamiseksi on ohjata keskeiset lokitiedot keskitetylle ja vahvasti suojatulle lokipalvelimelle, jonka tiedot sitten varmuuskopioidaan säännöllisesti.
Se, mitä lasketaan säilytysvaatimuksen “keskeisiin tallenteisiin” vaihtelee käyttöympäristöstä riippuen. Tähän kuuluvat aina keskeisten verkkolaitteiden ja palvelinten lokitiedot. Käyttöympäristöstä ja turvatasosta riippuen myös esimerkiksi työasemien ja vastaavien lokitiedot kuuluvat tähän erittäin usein.
Toteutus työasemissa/palvelimissa vaatii usein lokituksen päälle laittamista ja oletusarvojen muuttamista säilytysajan/-tilan suhteen. Esimerkiksi Windows-ympäristöissä tämä tarkoittaa yleensä valvontakäytäntöihin (Audit Policy) vähintään seuraavien päälle laittamista (epäonnistuneet ja onnistuneet tapahtumat):
- Valvo tilien kirjautumistapahtumia (Audit account logon events)
- Valvo tilienhallintaa (Audit account management)
- Valvo kirjautumistapahtumia (Audit logon event)
- Valvo objektin käyttöä (Audit object access)
- Valvo käytäntöjen muutoksia (Audit policy change)
- Valvo oikeuksien käyttöä (Audit privilege use)
- Valvo järjestelmätapahtumia (Audit system events)

Lisäksi tulee lokien säilytystilaa ja -aikaa kasvattaa riittäviksi. Suositus: lokeille varataan aluksi tilaa vähintään 500 Mt tai muu ko. ympäristössä riittäväksi arvioitava määrä. Riittävän ajan määritys voidaan tehdä esimerkiksi siten, että arvioidaan yhden kuukauden lokikertymän perusteella riittävä tila vaadittavalle säilytysaikajaksolle. Huom: tilalle on syytä varata reilusti ”puskuria”, sillä poikkeavat tilanteet ja myös tietyt hyökkäystyypit kasvattavat lokimäärää merkittävästi.
Suojaustason III vaatimuksen 2 toteuttamisen osana voidaan hyödyntää muun muassa automatisoituja komentojonoja (skriptejä), joilla tarkastellaan lokitietoihin ja tiedostojärjestelmiin tapahtuneita muutoksia. Windows-ympäristöissä useimmat keskeiset tiedot voidaan kerätä esimerkiksi wmic-työkalun (Windows Management Instrumentation Command-line) avulla. Vastaavasti useimmissa Unix-/Linux-ympäristöissä keskeiset tiedot on tyypillisesti kerättävissä ja tarkasteltavissa järjestelmän tukemilla skripteillä ja työkaluilla (esim. last) seuraavista sijainneista:
- /var/run/utmp
- /var/log/wtmp
- /var/log/btmp
- /var/log/messages
- /var/log/secure

Verkkoliikennöinnin osalta tarkkailuun on useita soveltuvia toteutusmahdollisuuksia keskeisten verkkosolmujen tasolla tapahtuvasta tarkastelusta aina työasema-/palvelinkohtaisiin sensoreihin sekä näiden yhdistelmiin.
Tietyissä kansainvälistä turvaluokiteltua tietoa käsittelevissä verkoissa lokitarkkailua edellytetään jo suojaustasolta IV lähtien.
Järjestelmäkohtaisia ohjeita löytyy lisää esimerkiksi I 502.0:n lähdekentässä kuvatuista lähteistä.

I 505.0

Vaatimukset palvelinten salauksesta voidaan tietyissä palvelinympäristöissä korvata jollain muulla viranomaisen tapauskohtaisesti hyväksymällä menettelyllä. Menettelylle edellytetään aina fyysisen ja loogisen pääsynhallinnan sekä tallennemedioiden hallinnan poikkeuksellisen luotettavaa toteutusta.
Eri suojaustasojen tietojen erottelulla tavoitellaan sitä, että vain alemman tason tietoon oikeutetuilla ei olisi pääsyä ylemmän tason tietoihin. Eri tasojen tietoa voidaan säilyttää samassa paikassa, mikäli kaikilla paikkaan pääsevillä on oikeus kaikkeen paikasta löytyvään tietoon (esim. yhden käyttäjän kannettavan tietokoneen kiintolevy).
Suojattavan tiedon omistajat varaavat usein itselleen tarkastusoikeuden kaikkiin verkkoihin/järjestelmiin, joissa heidän omistamaansa tietoa käsitellään. Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltävään tietoon. Erityisesti monihankeverkoissa ja muissa vastaavissa ympäristöissä, joissa on tarve käsitellä useamman eri omistajan tietoa, tulee varmistua siitä verkon/järjestelmän rakenne mahdollistaa tarkastukset siten, että tiedon omistajat eivät pääse käsiksi toistensa tietoihin tarkastuksen yhteydessä. Suojaustason IV tiedoille riittää useimmissa ympäristöissä loogisen tason erottelu (esim. hankepalvelinvirtualisointi).
Suojaustasosta III lähtien edellytetään tyypillisesti fyysisen tason erottelua ja/tai tiedon/tietoliikenteen salaamista yhteiskäyttöisissä laitteissa.
Toteutussuositus väliaikaistietojen hävitykseen: logon- tai logoff-skriptein tuhotaan ylikirjoittaen tiedostot yleisimmistä käytetyistä dokumenttiformaateista yleisimmistä hakemistoista, jonne tilapäistiedostoja syntyy. Käytännössä esim. %HOMEPATH%/Local Settings/Temp alihakemistoineen, joista ylikirjoitetaan .doc*, .dot*, .xls*, .ppt*, .pdf, .rtf, .txt, acc*, .htm*, .mht, .xml, .jpg, .jpeg, .png, .tif*, .gif, .bmp, .zip, .gz, .tgz, .rar, .part, .tmp.
Palvelimissa ja muissa ympäristöissä, missä järjestelmää ei uudelleenkäynnistellä usein, suositellaan ylikirjoitus ajastamaan tapahtumaan automaattisesti tietyin aikavälein, esim. kerran vuorokaudessa.

I 510.0

Kattaa myös TLS-/SSL-avaimet. Vrt. I 509.0. Avaintenvaihdon aikavälin vaatimus arvioidaan tapauskohtaisesti käyttöympäristöstä ja -tarkoituksesta riippuen.
Tilanteissa, joissa suojattavaa aineistoa joudutaan lähettämään ei-luotetun verkon yli, ja pisteiden välillä ei ole suojattua ja viranomaisen hyväksymää pysyvää tiedonsiirtokanavaa, suositellaan salausavaimen muodostamiseen seuraavaa käytäntöä:
Pisteiden välillä sovitaan 15-merkkinen yhteinen salausavaimen osa. Sopiminen on tehtävä kasvotusten, tai jollain muulla viranomaisen luotettavaksi hyväksymällä menettelyllä. Lähetettäessä aineistoa päätepisteiden välillä, lähettäjä lisää salausavaimen perään keksimänsä lähetyskohtaisen 10-15 -merkkisen lähetysavaimen, ja salaa lähetettävän aineiston muodostuneella 25-30 -merkkisellä salausavaimella. Lähettäjä voi lähettää lähetysavaimen tämän jälkeen vastaanottajalle esimerkiksi tekstiviestillä. Huom: salausavaimen jälkimmäinen osio tulee vaihtaa jokaiseen lähetykseen.
Em. käytäntö ja käytetty salausratkaisu tulee aina etukäteishyväksyttää tiedon omistajalla tai omistajan valtuuttamalla taholla. Tämä taho on esimerkiksi kansainvälisten tietoaineistojen tapauksessa Kansallinen salaustuotteiden hyväksyntäviranomainen (CAA, Crypto Approval Authority, Suomessa Viestintäviraston NCSA-FI).
Puhtaasti ohjelmistopohjaiset salausratkaisut ovat tyypillisesti hyväksyttyjä IV- ja joissain tilanteissa erityisehdoilla myös III-tasoilla. II-tasolla ja useimmin myös III-tasolla edellytetään tyypillisesti enemmän alustan luotettavuudelta.

I 513.0

Korotetun tason vaatimus on aiheellinen mm. seuraavissa tilanteissa:
palvelin – palvelin –yhteyksissä luokituksen kasautumisvaikutuksen takia III-luokkaan nousseet, suuren määrän SY IV –tietoa sisältävät järjestelmät, joita ei voi olla tarve käyttää ei-luokitelluista verkoista, kuten Internetin yli (vrt. I 401.0:n III-tason 4. kohta)

I 603.0

Toteutussuositus väliaikaistietojen hävitykseen: logon- tai logoff-skriptein tuhotaan ylikirjoittaen tiedostot yleisimmistä käytetyistä dokumenttiformaateista yleisimmistä hakemistoista, jonne tilapäistiedostoja syntyy. Käytännössä esim. %HOMEPATH%/Local Settings/Temp alihakemistoineen, joista ylikirjoitetaan .doc*, .dot*, .xls*, .ppt*, .pdf, .rtf, .txt, acc*, .htm*, .mht, .xml, .jpg, .jpeg, .png, .tif*, .gif, .bmp, .zip, .gz, .tgz, .rar, .part, .tmp.

Palvelimiin ja muihin vastaaviin järjestelmiin, joita ei käynnistellä päivittäin, suositellaan, että väliaikaistiedostojen ylikirjoitus automatisoidaan ja ajastetaan tapahtumaan säännöllisesti, esimerkiksi kerran vuorokaudessa.
Muistettava myös käytöstä poiston yhteydessä: I 507.0.

Suojaustason III vaatimukset 1 ja 2: vrt. tiedon omistajien tarkastusoikeus, joka kuvattu tämän liitteen I 505.0:aa selventävässä kohdassa.

Kansainvälisen suojaustasojen IV-II aineistojen hävittämisessä tulee erikseen tarkistaa vaadittavat menettelytavat ja vaatimukset. Esimerkiksi paperinrepijöiden vaatimukset vaihtelevat jonkin verran riippuen tiedon omistajasta. Tiettyjen kansainvälisten aineistojen tuhoamiseen edellytetään myös toisen henkilön valvontaa ja tuhoamisen dokumentointia jo suojaustasolla III.

LIITE 2:
KANSALLISEN TURVALLISUUSAUDITOINTIKRITEERISTÖN ENSIMMÄISEN JA TOISEN VERSION VÄLISET MUUTOKSET

KATAKRI:n toisessa versiossa on toteutettu johdantokappaleessa mainittujen uudistusten lisäksi alla luetellut yksityiskohtaiset muutokset. Näiden ohella kriteeristö on täydentynyt liitteessä 1 esitetyillä lisäkommenteilla sekä erityisesti tietoturvallisuuden osion entistä kattavammilla lähdeviittauksilla.

1) Hallinnollinen turvallisuus:
   - joitakin aikaisemman hallinnollisen tietoturvallisuusosion kysymyksiä siirretty hallinnollisen turvallisuuden osioon (A501.1, A204.0, A401.0, A408.0, A409.0, A410.0, A105.1, A608.0, A806.0, A807.0, A803.1).
   - uusi kysymys: A 306.0 (käsittely-ympäristö)

2) Henkilöstöturvallisuus:
   - joitakin aikaisemman tietoturvallisuusosion kysymyksiä siirretty henkilöstöturvallisuuden osioon (P 407.0, P 408.0).
   - poistettu viranomaisten osalta henkilöluottotietojen tarkistusvaatimus, jätetty yritysten harkintaan luottotietolain puitteissa

3) Fyysinen turvallisuus:
   - joitakin aikaisemman tietoturvallisuusosion kysymyksiä siirretty fyysisen turvallisuuden osioon (F209.1, F216.0, F217.0, F218.0, F219.0)
   - ikkunakalvovaatimus pois IV-tasolta (F202.0, F203.0)
   - liitteessä 1 suosituksia seinä, lattia- ja kattorakenteista. Testit jatkuvat näiltä osin edelleen, kuten myös ikkunapuitteiden osalta.
   - poistettu standardiviittaukset kassakaappien osalta IV-tasolla (F208.0)
   - lisätty äänieristysvaatimus IV-tasolle ovien ja muiden rakenteiden osalta (F205.0, F207.0)
   - lisätty rikosilmoitinjärjestelmän toimintakuntoisuusvaatimus tasolle IV (F305.0)

4) Tietoturvallisuus:
   - osa kysymyksistä siirretty muihin osioihin (ks. taulukko osion alussa)
   - perustason vaatimusasettelua laskettu joiltakin osin vastaamaan paremmin valtionhallinnon tietoturva-asetuksen linjauksia
   - eräiden kysymysten kysymyksenasettelua täsmennetty
   - uusia kysymyksiä:
     - I 409.0 (ipv6)
     - I 410.0 (reitityksen turvallisuus)
     - I 514.0 (hankittavien laitteistojen turvallisuus).

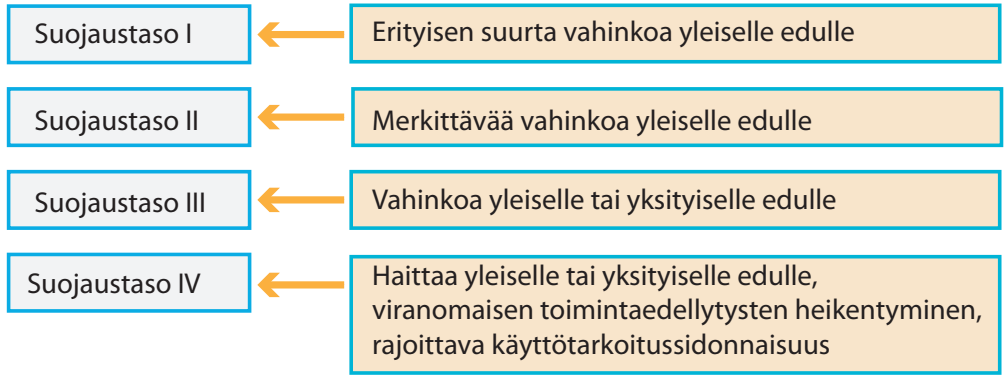
LIITE 3: SUOJAUSTASOT JA MUITA MÄÄRITELMIÄ

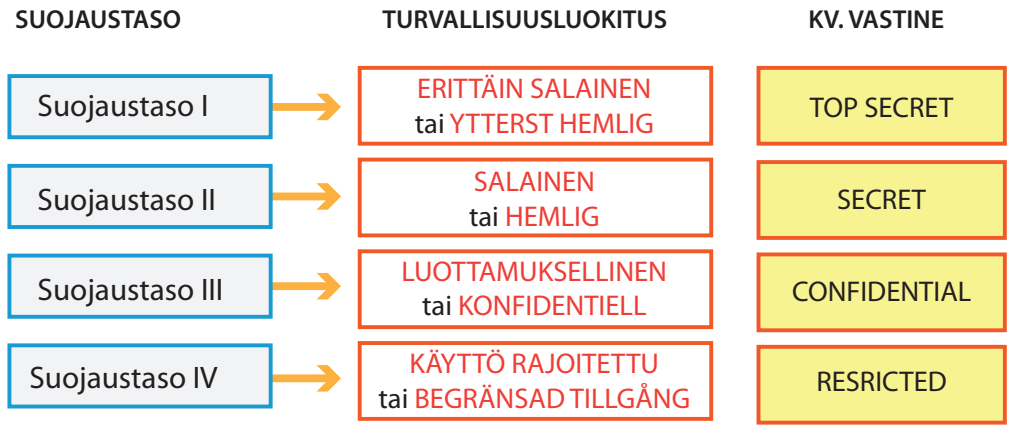
1. Suojaustasot ja turvallisuusluokkamerkinnät

1.10.2010 voimaan tullut Valtionhallinnon tietoturva-asetus määrittää suojaustasot yksinkertaistettuna seuraavasti:

- mitä tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa?

- Suojaustasomerkintöjä voidaan täydentää turvallisuusluokitusmerkinnöillä silloin, kun turvallisuusluokittelulle on erityiset perusteet (vahinkoa kv. suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle, TTA 12§):





2. Käytettäviä termejä

arkaluonteiset henkilötiedot (henkilötietolaki, 11§)

- rotu tai etninen alkuperä
- henkilön yhteiskunnallinen, poliittinen tai uskonnollinen vakaumus tai ammattiliittoon kuuluminen
- rikollinen teko, rangaistus tai muu rikoksen seuraamus
- henkilön terveydentila, sairaus tai vammaisuus taikka häneen kohdistetut hoitotoimenpiteet tai niihin verrattavat toimet
- henkilön seksuaalinen suuntautuminen tai käyttäytyminen
- henkilön sosiaalihuollon tarve tai hänen saamansa sosiaalihuollon palvelut, tukitoimet ja muut sosiaalihuollon etuudet.

asiakirjan käsittely

- Vastaanottaminen, laatiminen, tallettaminen, katselu, muuttaminen, luovuttaminen, kopiointi, siirto, välittäminen, hävittäminen, säilyttäminen, arkistointi, asiakirjaan (usein sähköisin apuvälinein) kohdistuvat toimenpiteet

biometriset tunnistetiedot

- Henkilön tunnistamiseksi käytettävät ja henkilön yksilöivät tiedot

kansainvälinen tietoturvallisuusvelvoite

- Suomea sopimuspohjaisesti sitova kansainvälisen osapuolen salassa pidettävän asiakirjan suojausvelvoite

salassa pidettävä asiakirja

- asiakirja, joka on JulL:n 5§ tai muiden lakien mukaan pidettävä salassa

tietoturvallisuus

- salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä
- saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä

valtionhallinnon viranomainen

- valtion hallintoviranomaiset ja muut virastot, laitokset tuomioistuimet ja muut lainkäyttöviranomaiset

yrityksen sensitiivinen tieto

- yrityssalaisuus tai liike- ja ammattisalaisuus

Kansallinen turvallisuusauditointikriteeristö

ISBN: 978-951-25-2245-3 nid.
ISBN: 978-951-25-2246-0 pdf

www.defmin.fi