KPMG IT Sertifiointi Oy

Sosiaali- ja terveydenhuollon järjestelmien tietoturvallisuuden sertifiointi ja tietoturvavaatimukset

5.5.2015

kpmg.com/fi/it-sertifiointi

KPMG
cutting through complexity

Esittäjän taustat

- KTM 12/2004 Lapin yliopisto / Oulun yliopisto
- CISA, CISSP, CISM, CGEIT, CRISC ISMS Lead Auditor, KATAKRI Lead Auditor
- KPMG:llä elokuusta 2005
- Vastaa hallinnollisen tietoturvallisuuden palveluista, jonka alla mm. KPMG IT Sertifiointi / virallinen arviointilaitostoiminta
- Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen -kirja 2009

Hyväksytyt tietoturvallisuuden arviointilaitokset

Päivitetty 04.02.2015

Alla olevassa taulukossa on esitetty Viestintäviraston hyväksymät tietoturvallisuuden arviointilaitokset.

Arviointilaitosten hyväksyntä perustuu lakiin tietoturvallisuuden arviointilaitoksista 1405/2011

Päätös annettu	**Arviointilaitoksen nimi ja y -tunnus**	**Pätevyysalue** (suojaustaso ja kriteeristö *)	**Laitoksen oman tiedonkäsittelyn taso** **)	**Muut ehdot** (esim. määräaikaisuus)
2.2.2015	KPMG IT Sertifiointi Oy, Y-tunnus: 2469464-1, PL 1037, 00101 Helsinki	Suojaustaso IV VAHTI KATAKRI II ISO/IEC 27001:2013	Suojaustaso III	

FINAS
Finnish Accreditation Service
S045 (EN ISO/IEC 17021)

KPMG IT SERTIFIOINTI OY

KPMG IT CERTIFICATION LTD

Sisältö

01

Tausta

Tausta

- Kaikkien KanTa-palveluun liittyvien järjestelmien ja välittäjätahojen tietoturvan ja tietosuojan toteutuminen tulee varmistaa.
- Järjestelmän käyttöönotto vaatii tietoturvallisuuden arviointilaitoksen antamaa **todistusta vaatimuksenmukaisuudesta** sekä toimittajan laatimaa **omavalvontasuunnitelmaa**.
- Jos järjestelmä tai välityspalvelu on liitetty valtakunnallisiin tietojärjestelmäpalveluihin ennen 1.1.2015, saa niitä käyttää liittymisen yhteydessä annetulla auditointilausunnolla todetun määräajan loppuun saakka. Määräajan jälkeen, tai jos järjestelmään tehdään olennaisia muutoksia, sertifiointi tulee toteuttaa uudelleen.
  - Olennaiset muutokset ovat muutoksia, jotka muuttavat tietojärjestelmän toimintaa suhteessa määräyksen liitteenä olevien vaatimusten toteutumiseen.
- Jos välityspalvelulta puuttuu uuden lainsäädännön mukainen sertifiointi (arviointilaitoksen toteuttama ulkoinen auditointi), on sertifiointi hankittava 31.7.2015 mennessä.
- Arviointi suoritetaan käyttämällä Terveyden ja hyvinvointilaitoksen (THL) vahvistamaa vaatimuskriteeristöä ”Tietoturvavaatimukset A-luokkaan kuuluville järjestelmille ja järjestelmien käyttöympäristöille”.

02

Sertifiointiprosessi

Sertifiointihakemus

- Ennen sertifiointihakemuksen jättämistä sertifiointia hakevan organisaation tulee olla **hyväksytysti suorittanut Kansaneläkelaitoksen yhteistestauksen**.
- Täytetty sertifiointihakemus tulee lähettää vähintään kaksi viikkoa ennen toivottua tarkastusajankohtaa.
  - Sertifiointihakemuksen liitteeksi tulee liittää Kansaneläkelaitoksen antama raportti yhteistestauksen hyväksytystä suorittamisesta.

Sertifiointiprosessin kulku

- Dokumentaation katselmointi
- Tarkastus
  - Tarkastusmenetelmänä käytetään työpajaa
  - Vaatimuksesta riippuen vaatimuksen toteutuminen todennetaan vaatimuskriteeristön mukaisesti joko haastattelemalla (H), dokumentaatioon tutustumalla (D), toiminnollisuutta testaamalla (T) tai muuten validoimalla tai teknisellä testauksella (V).
- Tietoturvallisuuden arviointilaitoksella on oikeus saada hakijalta kaikki arvioinnin edellyttämät tiedot vaatimuksenmukaisuustodistuksen laatimiseksi ja ylläpitämiseksi.

Raportointi

- Sertifioinnin tuotoksena syntyy **vaatimuksenmukaisuustodistus** sekä **vaatimuksenmukaisuuden tarkastusraportti**.
- Raportointi suoritetaan kolmeportaisella asteikolla
  - Vaatimus täyttyy
  - Vaatimus täyttyy kompensoivalla menetelmällä
  - Vaatimus ei täyty
- Vaatimuksenmukaisuustodistuksen myöntämisen edellytyksenä on, että kaikki järjestelmän tai välityspalvelun kannalta olennaiset kontrollit täyttyvät tai täyttyvät kompensoivalla menetelmällä.

Todistuksen myöntäminen ja voimassaolo

- Mikäli tietojärjestelmä täyttää tietoturvavaatimukset, voidaan vaatimuksenmukaisuustodistus ja tarkastusraportti luovuttaa tietojärjestelmäpalvelun tarjoajalle.
- Vaatimuksenmukaisuustodistus **voidaan myöntää myös rajoitettuna**, jollei tietojärjestelmäpalvelun tarjoaja korjaa tarkastuksessa havaittuja poikkeamia sovitussa määräajassa.
- Vaatimuksenmukaisuustodistus on voimassa enintään viisi (5) vuotta.
- Tietoturvallisuuden arviointilaitos ilmoittaa Sosiaali- ja terveysalan lupa- ja valvontavirastolle (Valvira) sekä Kansaneläkelaitokselle tiedot kaikista myönnetyistä, muutetuista, täydennetyistä, määräajaksi tai kokonaan peruutetuista tai evätyistä vaatimuksenmukaisuustodistuksista.

Käyttöönoton jälkeinen seuranta ja ilmoitusvelvollisuus

- Tietojärjestelmäpalvelun tarjoajan on ilmoitettava tietoturvallisuuden arviointilaitokselle tietojärjestelmän merkittävistä poikkeamista sekä tietojärjestelmän muutoksista.
- Vaatimuksenmukaisuustodistus on uudistettava, jos tietojärjestelmään tehdään merkittäviä muutoksia tai olennaisia vaatimuksia on muutettu.
  - Tietojärjestelmäpalvelun toimittajan tulee toimittaa arviointilaitokselle muutosloki ennen uuden versiopäivityksen käyttöönottoa tuotannossa.
- Vaatimuksenmukaisuustodistus voidaan peruuttaa määräajaksi tai kokonaan, jollei järjestelmäpalvelujen tarjoaja korjaa puutteellisuuksia asetetussa määräajassa.

Uudelleen sertifiointi

- Järjestelmän olennaisten muutosten jälkeen suoritettava uudelleen sertifiointi noudattaa normaalin sertifioinnin periaatteita.
- Sertifioinnissa käydään läpi kaikki ne vaatimukset johon muutokset ovat vaikuttaneet sekä muut tarpeelliseksi nähdyt vaatimukset esimerkiksi edellisessä auditoinnissa kompensoivilla menetelmillä täyttyneet kohdat.

03

Tietoturvavaatimukset

12Y: Lokitietojen muuttumattomuus

- ”Lokitietojen muuttumattomuus tulee varmistaa. Vaatimus koskee käyttölokia ja teknistä lokia.”
- Tärkeintä on varmistaa, että ne henkilöt joiden toimintaa lokitetaan eivät pääse muuttamaan lokitietoja.
- Lokitietojen muuttumattomuus tulee varmistaa myös teknisten virheiden osalta.
- Lokitietojen muuttumattomuuden varmistamiseen voidaan toteuttaa useilla eri tavoilla, mutta lähtökohtana on, että tiedot tallennetaan tietokantaan johon järjestelmällä on ainoastaan kirjoitusoikeudet. Lokitiedot tulee myös siirtää mahdollisimman reaaliaikaisesti toiseen sijaintiin (esim. erillinen lokipalvelin).

14Y Tekninen loki

- Lokitiedot tulee tallentaa yhteyksien muodostamisesta (sisään ja ulos). Sisältöä ei ole määritelty tarkemmin. Ohjeistuksena voi käyttää Vahti 3/2009 liitteen 1 tarkastuslistaa.

40Y: Turvallisen ohjelmoinnin periaatteet järjestelmän toteutuksessa

1. kuinka **tietoturvatietous** on huomioitu järjestelmän kehitysprosessin aikana
    - Ohjelmistokehittäjien tietoturvatietoisuus (sisäiset ja ulkoiset koulutukset, sertifikaatit, jne.)
2. kuinka **tietoturvauhat ja riskit on tunnistettu ja kontrolloitu**
    - CE-merkintään laajempi riskikartoitus
3. kuinka rajapinnat on testattu **viallisilla syötteillä** sekä **suurilla syötemäärillä**
    - Todennetaan testausraportista. (ulkopuolinen tai sisäinen)
4. kuinka valvotaan helposti ongelmia aiheuttavien **funktioiden** ja **rajapintojen** käyttöä
5. kuinka katselmoidaan **arkkitehtuuri** ja **lähdekoodi**
    - Dokumentaatio katselmoinnista
6. kuinka tarkastetaan ohjelmakoodi esim. **automaattisella staattisella analyysillä**
7. kuinka ohjelmakoodien **versionhallinta** on toteutettu, kuinka vanhempiin ohjelmistoversioihin on tarvittaessa päästävissä ja kuinka ohjelmakoodin muutosten dokumentointi on toteutettu

48Y: Hallintayhteydet järjestelmään

- ”Mikäli järjestelmään ylläpidollisista tai muista syistä sallitaan etäyhteyksiä, yhteydet järjestelmään tulee olla **salattuja päästä päähän** (ylläpitäjän koneelta ylläpidettävään järjestelmään asti) esim. VPN-tunnelilla. **Lisäksi etäyhteyksien käyttäjät tulee tunnistaa käyttämällä luotettavaa vahvaa tunnistautumismenetelmää (ei pelkästään salasanaa ja käyttäjätunnusta)** Hallintayhteydet järjestelmään tulee joko salata vahvasti tai rakentaa käyttäen omaa suojattua verkkoa hallintayhteyksille. **Vaatimus koskee myös sisäverkon yhteyksiä**.”
- Vahvan tunnistautumismenetelmän toteutustapa on vapaa (esim. toimikortti, SMS, SecurID).

Lisätietoja sertifioinnista antavat

Mika Karjalainen
Tietoturva-asiantuntija
020 760 3219
mika.karjalainen@kpmg.fi

Mika Iivari
Senior Manager
020 760 3495
mika.iivari@kpmg.fi

KPMG IT Sertifiointi Oy
PL 1037, 00101 Helsinki
(Töölönlahdenkatu 3 A)
P: 020 760 3000
F: 020 760 3399
kpmg.fi