



Pilvipalvelut akkreditoinnin näkökulmasta

Reetta Grenman

Standardin asettamat vaatimukset

SFS ISO/IEC 17025:2017

7.11.2 Laboratorion tiedonhallintajärjestelmät, joita käytetään tiedon keräämiseen, käsittelyyn, tallentamiseen, raportointiin, varastointiin tai palauttamiseen, on validoitava toiminnallisuuden suhteen ennen käyttöönottoa. Tämä sisältää myös laboratorion sisäisten käyttöliittymien rajapintojen toimivuuden arvioinnin. Kun tehdään muutoksia – esim. kun muokataan joko laboratorion omaa ohjelmistoa tai muokataan kaupallisesti saatavilla olevaa ohjelmistoa – on muutokset hyväksyttävä, dokumentoitava ja validoitava ennen käyttöönottoa.

HUOM. 1 Tässä asiakirjassa termi *laboratorion tiedonhallintajärjestelmä* käsittää sekä tietokoneistetun ja ei-tietokoneistetun tiedon hallinnan. Jotkin vaatimuksista soveltuvat paremmin tietokoneistettuihin järjestelmiin kuin ei-tietokoneistettuihin järjestelmiin.

HUOM. 2 Kaupallisia ohjelmistoja, joita käytetään siihen tarkoitukseen johon ne on suunniteltu, voidaan pitää riittävästi validoituina.

Standardin asettamat vaatimukset

SFS ISO/IEC 17025:2017

7.11.3 Laboratorion tiedonhallintajärjestelmien on

- a) oltava suojattu luvattomalta käytöltä
- b) oltava suojattu asiattomilta muutoksilta tai katoamiselta
- c) sijaittava ympäristössä, joka täyttää toimittajan tai laboratorion spesifikaatiot tai jos kyseessä ei ole tietokoneistettu järjestelmä, oltava sellaisia, että ne tarjoavat olosuhteet, jotka varmistavat käsin tehtävän kirjaamisen ja sen kopioinnin tarkkuuden
- d) oltava ylläpidettyjä tavalla, joka varmistaa tiedon eheyden
- e) sisällettävä järjestelmähäiriöiden tallentamisen sekä asianmukaiset välittömät ja korjaavat toimenpiteet.

Standardin asettamat vaatimukset

SFS ISO/IEC 17025:2017

7.11.4 Kun laboratorion tiedonhallintajärjestelmää hallitaan ja ylläpidetään toimitilojen ulkopuolella tai ulkopuolisen toimittajan toimesta, laboratorion on varmistettava, että järjestelmän toimittaja tai operaattori noudattaa kaikkia tässä asiakirjassa esitettyjä asiaan liittyviä vaatimuksia.

7.11.5 Laboratorion on varmistettava, että laboratorion tiedonhallintajärjestelmiin liittyvät käyttöohjeet, ohjekirjat ja viitetiedot ovat helposti henkilöstön saatavilla.

7.11.6 Laskutoimitukset ja tiedonsiirrot on tarkistettava asianmukaisesti ja järjestelmällisesti.

Pilvipalveluiden turvallisuus

Mitä organisaatioiden tulisi huomioida pilvipalveluja hyödyntäessä



<https://www.kyberturvallisuuskeskus.fi/fi/ohjeet> -> Muita tietoturvakäytäntöjä

Pilvipalveluiden muodot

- Yksityinen
 - Omaan tarpeeseen hankittu ja tuotettu
- Yhteisö
 - Rajatun organisaatiojoukon hankkima ja käyttämä
- Julkinen
 - Käyttäjäjoukkoa ei ole rajattu
- Hybridi
 - Yhdistelmä edellisistä

Palvelu- ja/tai hankintamalli

- Minkälaista tietoa tai toimintaa pilveen siirretään?
 - Määrittää vaatimukset pilven tyyppille, toiminnalle ja salaukselle
- Iso vai pieni toimija?
 - Kustomointi
 - Toimintavarmuus, jatkuvuus
 - Mahdollisuus omaan auditointiin

Tiedon omistajuus ja käyttöoikeudet

- Pääsääntöisesti omistajuus säilyy tiedon tuottajalla
- Palvelun ehdoista on hyvä sopia tarkasti
- Sopimuksella tulisi varmistaa, että käyttöoikeus säilyy vain itsellä

Tallenteiden elinkaari

- Tieto yleensä talletettuna monessa paikassa samaan aikaan
 - Kannattaa selvittää, missä paikoissa fyysisesti tietoa säilötään
 - Tiedonsiirron turvaaminen
 - Kohdemaan lait ja asetukset
 - Kohdemaan viranomaisten oikeudet tietoon
- Mitä tiedolle tapahtuu, kun se poistetaan
 - Ylikirjoitus, mekaaninen tuhoaminen, tilan vapaaksi merkitseminen? Laitteiden tuhoaminen vai kierrätys

Riskiarvio

- Riskiarviossa on otettava huomioon, että pilvipalvelussa olevaa tietoa käsitellään jonkun muun ylläpitämässä palvelussa
- “Pilvessä tietojen ja laskennan luottamuksellisuus, eheys, saatavuus tai kiistämättömyys eivät välttämättä ole yhtä hyvällä tasolla kuin tiettyä tarkoitusta varten rakennetuissa tietojärjestelmissä.”

Pilvipalvelujen tarjoajan turvallisuus

- Tekninen turvallisuus
 - Käyttäjähallinta
 - Päivitykset
- Henkilöstöpolitiikka
 - Kriittisten henkilöiden turvallisuusselvitykset
- Fyysinen turvallisuus
- Oma käyttöympäristö

Kiitos!

- Reetta.Grenman@finas.fi