FINAS
Finnish Accreditation Service

Opas 1/2014
1.10.2014

Tietotekniikan arviointi akkreditointimenettelyssä

FINAS - akkreditointipalvelu

Espoo 2014

ISBN 978-952-6682-19-8

Alkusanat

Tämän FINAS-akkreditointipalvelun Oppaan 1 tarkoituksena on yhtenäistää tietojärjestelmien arviointia osana akkreditointiin liittyvää arviointia. Oppaassa tuodaan esille tietotekniikan arvioinnin oleellisimpia kohtia ja kuvataan näiden arviointia. Opas 1 on tarkoitettu sekä arvioijien että akkreditointia hakevien ja akkreditoitujen toimielinten käyttöön. Uusi versio Opas 1/2014 korvaa oppaan aikaisemman version S21/2012. Uuden version käyttöönotto on seurausta FINASin opassarjan uudelleen nimeämisestä. Oppaan sisältö ei ole muuttunut aikaisempaan versioon nähden lukuun ottamatta viittausta kumottuun standardiin SFS-EN ISO 15189:2007, joka poistettiin.

Oppaassa olevat viittaukset ovat laboratorioiden akkreditointivaatimuksena käytettävään standardiin SFS EN ISO/IEC 17025:2005 (jatkossa ISO 17025).

Eurooppalaisten laboratorioiden yhteistyöjärjestö Eurolab on julkaissut laboratorioille suunnatun oppaan (Eurolab Technical Report no 2/2006) tietotekniikan hallinnasta. Akkreditointielimet ovat ottaneet oppaan käyttöön arvioidessaan laboratorioita.

FINAS-tiedotteessa 10 "Akkreditointitoiminnan vaatimukset, arviointi-periaatteet ja oppaat" on esitetty kulloinkin voimassa olevat oppaat.

Sisällysluettelo

1 Johdanto

Tietotekniikkaa hyödynnetään nykyään varsin laajasti toimielinten toiminnassa. Siksi akkreditointimenettelyyn liittyvissä arvioinneissa joutuvat kaikki arvioijat, eivät pelkästään tietojärjestelmiin erikoistuneet, ottamaan kantaa toimielimen käyttämiin tietotekniikkaa hyödyntäviin menettelyihin.

Tietojärjestelmien arviointi perustuu muun muassa riskien analysointiin ja arvioinnin lähtökohtana on selvittää aiheuttaako tietojärjestelmien käyttö sellaisia riskejä, joita ei esiintyisi ilman kyseisiä järjestelmiä. Analysoitavat riskit liittyvät akkreditoiduilla/akkreditoitavilla menetelmillä tuotettujen tulosten

- laatuun
- tarkkuuteen
- koskemattomuuteen
- luottamuksellisuuteen
- toimitusvarmuuteen.

Nämä kriteerit voidaan tiivistää seuraaviin kysymyksiin:

1. Ovatko tuloksiin liittyvät toimenpiteet jäljitettävissä (tekijä, menetelmä, laite, raakatulokset, laskentakaavat, tulosten muuttaminen, ajankohta jne.)?
2. Saako tilaaja oikean tuloksen laboratorion ilmoittamalla mittaustarkkuudella (laskeeko järjestelmä oikein, pyöristääkö se oikein, siirtyvätkö mittaustulokset oikein, kohdistuuko tulos oikeaan näytteeseen jne.)?
3. Säilyykö tuloksen koskemattomuus (muuttumattomuus) koko sen ajan, jonka laboratorio takaa, eli voidaanko sama tulos tuottaa uudestaan? (Voiko joku vahingossa tai tahallaan, jälkeä jättämättä, muuttaa tai poistaa tuloksen? Säilyykö tieto tuloksen laskentaan käytetyssä laskentakaavassa vaikka kaavaa olisi myöhemmin muutettu? Ovatko kaikki tulokseen liittyvät tiedot rekonstruoitavissa tietokannasta?)
4. Pääseekö joku ulkopuolinen luvatta käsiksi tuloksiin (suojaukset, lokit, tietokantatyökalujen mahdollinen käyttö jne.)?
5. Miten toimitaan tietojärjestelmien mahdollisten käyttökatkojen yhteydessä? Miten on varmistettu, ettei tietojärjestelmien ongelmista aiheudu kohtuutonta haittaa organisaation toiminnalle? Miten käyttökatkokset vaikuttavat prosessien läpimenoaikoihin ja tulosten ilmoitustapaan, jotka voivat muuttua, kun käytetään korvaavaa järjestelmää?

2 Yleistä tietojärjestelmistä

Yleisimmin käytössä olevat tietojärjestelmän tyypit on ryhmitelty seuraavassa. Siinä on myös rajattu ne osiot, jotka tämän oppaan laatineen työryhmän mielestä kuuluvat tietojärjestelmän arvioinnin piiriin.

2.1 Käyttöjärjestelmät

Käyttöjärjestelmät ovat yleisesti ottaen tunnettuja ohjelmia, jotka toimittaja on validoinut. Mikäli käytetään erilaisia käyttöjärjestelmiä, tulisi mahdollisuuksien mukaan arvioida miten eri järjestelmät mahdollisesti vaikuttavat toisiinsa. Testattaessa ja validoitaessa miten käytettävät ohjelmistot toimivat käyttöjärjestelmässä, tulisi käytettävä versiot kirjata (koskee sekä palvelimia että työasemia) järjestelmien testauspöytäkirjoihin. Lisäksi tulisi kirjata mahdolliset yhteensopivuusrajoitukset eri käyttöjärjestelmien osalta. Tämä on oleellista päivitettäessä tai otettaessa käyttöön uusia käyttöjärjestelmiä.

2.2 Kaupalliset valmisohjelmistot

Yleisiä kaupallisia valmisohjelmistoja ns. hyllytavara-ohjelmia voidaan standardin ISO 17025 (5.4.7) mukaan pitää riittävästi validoituina. Arvioinnissa on kuitenkin kiinnitettävä huomiota siihen, miten tällaisilla ohjelmistoilla tehtyjä sovelluksia on otettu käyttöön sekä miten niitä on testattu ja validoitu.

Esimerkkejä yleisesti käytettävistä valmisohjelmistoista ja niihin liittyvistä mahdollisista riskeistä ovat:

- tekstinkäsittelyohjelmat (vanhojen pohjien kopiointi ja käyttö tulosten raportoinnissa muodostavat riskin, jos vanhaa tietoa kopioituu mukaan)
- taulukkolaskenta (vanhojen pohjien ja laskukaavojen käyttö muodostavat riskin). Taulukkopohjat saattavat sisältää hyvinkin paljon laskentaa, tulosten prosessointia ja automatiikkaa. Taulukkolaskentaohjelmien makrotoimintoihin voidaan liittää muun muassa ohjelmakoodia. Kun yleisen ohjelmistopaketin välineitä käytetään sovelluskehittiminä, tulisi niillä tuotettujen ohjelmien toimivuus arvioida samoin perustein kuin varsinaisilla ohjelmointityökaluilla toteutetut sovellukset.
- tilastopaketit (voidaan olettaa, että ohjelmisto laskee oikein, mutta arvioinnissa on katsottava, miten on varmistettu, että käytetty menetelmä on ratkaistavaan tehtävään nähden oikea ja että tulosten tulkinta on oikea).

Edellä lueteltujen valmisohjelmistojen sovelluksia käytetään yleensä laajasti ja monipuolisesti. Niiden käyttö on usein osana tulosten manuaalista käsittelyä. Näiden työkalujen oikeasta käytöstä tulisi varmistua arvioitaessa toimielimen toimintaa. Tilasto-ohjelmien käytöstä laadunvarmistuksessa ja epävarmuuksien määrittelyssä tulisi olla menetelmäkohtaiset ohjeet. Mainittujen sovellusten käytön arviointi kuuluu oleellisena osana jokaisen arvioijan tehtäviin eikä yleensä edellytä erityistä tietojärjestelmien arviointia.

2.3 Laitteisiin integroidut ohjelmistot

Monet analysaattorit sisältävät analysointiprosessia ohjaavia ohjelmistoja. Nämä ohjelmat tulevat yleensä laitetoimittajalta. Ne ovat usein ns. mustia laatikoita “black box“ tai sulautettuja järjestelmiä (embedded systems), joiden koodi ei ole muiden luettavissa.

Näiden ohjelmistojen toimintaa testataan osana menetelmän testausta yleensä riittävällä määrällä vertailunäytteitä. Laitteen ja sen tietojärjestelmään liittyvän ohjeistuksen tulisi sisältyä menetelmäohjeeseen.

Arviointi tapahtuu menetelmän arvioijan taholta eikä siihen tarvita erityistä tietojärjestelmäarviointia.

2.4 Laboratorioiden tiedonhallintajärjestelmät

Laboratorioissa käytetään nykyään varsin yleisesti tiedonhallintajärjestelmää (Laboratory Information (Management) System = LI(M)S). LIMS on laboratorioiden toiminnanohjausjärjestelmä, johon sisältyy toimeksiantojen käsittely aina tilauksesta/analyysipyynnöstä selosteen/vastauksen lähettämiseen. Tiedonhallintajärjestelmään kuuluu aina tietokanta, jossa säilytetään laboratorion ja sen asiakkaiden kannalta tärkeää ja suojeltavaa tietoa. Laboratorion tiedonhallintajärjestelmä on usein liitetty ulkopuolisiin järjestelmiin (laskutukseen, potilastietokantaan, prosessinohjaukseen, tuotannonohjaukseen, analysaattoreihin jne.).

Erityisessä tietojärjestelmien akkreditointiarvioinnissa tulee keskittyä LIMSiin ja niihin rinnastettaviin järjestelmiin ja niiden tiedonsiirtoon, joka on lähes aina räätälöity laboratoriokohtaisesti.

Laboratorioiden tiedonhallintajärjestelmiä on kahden tyyppisiä:

1. Toimittajien tuotteistamat valmisohjelmistot eli standardijärjestelmät, jotka yleensä ovat laboratoriokohtaisesti parametrisoitavissa eli konfiguroitavissa. Usein valmisohjelmistojen päälle on toteutettu laboratoriokohtaisesti toteutettuja osuuksia.
2. Räätälöidyt ohjelmistot, jotka ovat joko ns. in-house ratkaisuja tai ulkopuolisen toimittajan toteuttamia

Valmisohjelmistot

Mikäli laboratoriossa on käytössä hyvän ja luotettavan toimittajan LIMS, jonka päivityksiin ja tukeen toimittaja on sopimuksin sitoutunut, voidaan arvioinnissa menetellä, kuten muiden valmisohjelmistojen osalta (katso kohta 2.2) varsinkin, jos ohjelmisto on laajasti käytössä vastaavissa labora-torioissa.

LIMS:in arvioinnissa keskitytään sovellukseen eli laboratoriokohtaiseen osaan johon kuuluu:

- konfiguroinnin (parametroinnin) ja siihen liittyvän validoinnin arviointi
- käyttötavan arviointi (järjestelmän käyttöön liittyvä ohjeistus ja sen noudattaminen)
- mahdollisesti räätälöidyt lisäykset perusohjelmaan (validointi, käyttö)
- liitynnät laitteisiin ja muihin ohjelmiin
- toimittajan ja laboratorion väliset sopimukset
- parametroinnin muutoshallinta.

Räätälöidyt LIMS-järjestelmät

Kun laboratoriossa on käytössä kokonaan räätälöity järjestelmä, arvioinnissa on kiinnitettävä huomiota tapaan, jolla laboratorio on validoinut järjestelmän sen vastaanottotestin yhteydessä ja niihin toimintatapoihin, joita käytetään muutosten ja päivitysten testauksessa ennen käyttöönottoa. Oleellista on myös se miten järjestelmän jatkuvuus/käytettävyys on varmistettu, kun järjestelmä on ”ainutkertainen”.

Toiminnallisuuden osalta arviointi tehdään samalla tavalla kuin edellisessä kohdassa valmiina ostetuille LIMS-tuotteille.

2.5 Tietoverkot ja tiedonsiirto

Tulosten ja tietojen välitys joko sähköpostitse tai organisaatioiden välisenä tiedonsiirtona on nykyään jo hyvin yleistä.

Tietoverkkojen perusohjelmistot katsotaan validoiduiksi jo ohjelmistotoimittajan puolesta. Arvioinnissa on kiinnitettävä huomiota siihen, että perusohjelmistot on kirjattu yleisen testauksen yhteydessä, ja käytetyn verkko-ohjelmiston versio sekä verkkokonfiguraatiota kuvaavat tiedostot (parametreineen) on tallennettu.

Sähköpostijärjestelmää arvioitaessa on arvioijan katsottava, miten toimielin on menetellyt muun muassa seuraavissa asioissa:

- kulkevien viestien automaattinen arkistointi, erityisesti lähtevien viestien tallennuksen varmistus (niiden tallennuksessa tulisi huomioida, että viestien lukuoikeudet on suhteutettu toiminnan laajuuteen; ts. mahdollisissa ongelmatilanteissa kopio olisi myös muiden kuin tiedon alkuperäisen lähettäjän saatavilla)
- liitetiedostojen käyttö ja ohjeistus sekä tiedottaminen turvallisuus-riskeistä (virukset, troijan hevoset jne.).

Sähköpostimenettelyille asetetut vaatimukset voivat pääsääntöisesti olla samat kuin muullekin kirjeenvaihdolle.

Tulosten siirtoa järjestelmien välistä tietoverkkoa käyttäen arvioitaessa on selvitettävä, miten toimielimessä on hyödynnetty lokijärjestelmiä ja minkä tyyppinen (suljettu, avoin) käytetty tietoverkko on. Mikäli verkko on avoin, on arvioitava menettelyt pääsykontrollista, palomuurien käytöstä ja tietoliikenteen salauksesta.

Mikäli tuloksia toimitetaan sähköisesti (joko pelkästään tai paperiversioiden lisäksi), arvioijan tulee muun muassa selvittää minkälaiset menettelyt toimielimessä on sähköisten allekirjoitusten käytöstä (kenellä on oikeudet käyttää sähköistä allekirjoitusta ja miten sähköisiä varmennuksia tuottavat koneet on suojattu).

Tietojen mahdollinen siirto eri tietokantojen välillä tulisi myös ottaa arvioinnin piiriin ja katsoa menettelyt sekä arvioida niiden toimivuus.

3 Tietotekniikan hallintaan ja käyttöön liittyviä asioita

3.1 Vastuu tietojärjestelmästä

Mikäli toimielimellä on toimeksiantojen käsittelyyn tarkoitettu tiedonhallintajärjestelmä, on arvioinnissa arvioijan varmistuttava siitä, että tietojärjestelmän hallinnollinen vastuu sekä vastuut, muun muassa järjestelmän käytöstä ja teknisestä ylläpidosta, on määritelty (ISO 17025 4.1.5). Resursseista riippuen voi useasta eri tehtävästä vastata sama henkilö.

Toimielimellä tulee olla nimettynä henkilö (henkilöitä tai työryhmä), joka vastaa järjestelmän käytöstä ja ylläpidosta (esimerkiksi järjestelmäpäällikkö/LIMS-vastaava, järjestelmän seurantaryhmä tms.); muun muassa:

- käyttöoikeuksien jakamisesta
- järjestelmän määrittelystä, hankinnasta, käyttöönotosta ja käytöstä
- sisäisten sovellusohjeiden laatimisesta ja noudattamisesta
- järjestelmän kehittämisestä sekä ylläpito- ja päivitystyön suunnittelusta ja toteutuksesta. Ylläpito käsittää muun muassa työasemien ja ennen kaikkea palvelimien teknisen toiminnan valvontaa, niiden ennakoivaa huoltoa sekä korjausta häiriötilanteessa. Järjestelmästä vastaava huolehtii näiden seikkojen toteuttamisesta ja riittävien voimavarojen saatavuudesta joko oman organisaation sisällä tai hankkimalla tarvittavat palvelut.
- käyttäjien koulutuksesta. Järjestelmästä vastaava huolehtii henkilökunnan käyttäjäkoulutuksen suunnittelusta ja toteutuksesta joko itse tai yhdessä koulutuksesta vastaavan henkilön kanssa. Koulutus voidaan hoitaa itseopiskelulla, järjestämällä sisäisiä kursseja tai hyödyntämällä kurssitarjontaa toimielimen ulkopuolella. Apuna koulutussuunnittelussa voi käyttää muun muassa käyttäjien ja asiakkaiden antamaa palautetta järjestelmästä ja laatuauditointien tuloksia. Osallistumiset koulutukseen kirjataan kuten toimielimen johtamisjärjestelmä edellyttää. Koulutusta suunniteltaessa tulisi huolehtia myös opetuksen laadusta. Tehokkaassa tietojärjestelmä-koulutuksessa oppilaat saavat itse käyttää opetettavaa ohjelma.

Toimielimellä tulisi olla nimettynä henkilö (tai henkilöitä), esimerkiksi käyttö-päällikkö/IT-tuki, joka vastaa järjestelmän toimivuudesta (laitteisto, verkko, tietokanta, tiedonsiirto ym. teknisistä asioista) ja

- joka osaa käyttää järjestelmää vaarantamatta tulosten luottamuksellisuutta ja oikeellisuutta
- jolla on oikeus päättää järjestelmän huollosta ja ylläpidosta

- jolla on kokemusta päätellä ovatko käytetyt menettelytavat tarkoituksenmukaisia
- jolla on kokemusta toteuttaa järjestelmämuutoksia vaarantamatta työn laatua.

Toiminnassa käytettävien tietojärjestelmien tulee olla toimielimen valvonnassa. On mahdollista jakaa tietojärjestelmiä organisaation muiden tahojen kanssa, mutta silloin tulee arvioinnissa selvittää miten on tunnistettu tai tiedostettu muun muassa muualla mahdollisesti tehtyjen muutosten vaikutukset omaan järjestelmään.

Tietojärjestelmät (hankinnat, laitteet, ohjelmistot, salaus, huolto, varmuus-kopiointi, virustentorjunta jne.) saattavat olla yrityksen tietohallinta-organisaation tai ulkopuolisen toimittajan vastuulla, jolloin toimielin ei käytännössä voi juurikaan vaikuttaa näihin toimintoihin. Näillä organisaatioilla on omat johtamisjärjestelmänsä, ja ne hoitavat muutosten hallinnan tämän mukaisesti. Toimielimen on kuitenkin määriteltävä palveluiden ja toimitusten kriteerit sekä varmistuttava ulkopuolisen toimittajan tuottaman palvelun sopivuudesta sen tarpeisiin (ISO 17025 4.6).

3.2 Tietojärjestelmien käyttäjät

Toimielimellä tulee olla menettelytavat tietojärjestelmillä työskentelevien henkilöiden koulutuksesta ja työhön opastamisesta sekä käyttöoikeuksien myöntämisperiaatteista (ISO 17025 5.2). Koulutuksen ja johtamis-järjestelmässä dokumentoidun ohjeistuksen tulisi kattaa ainakin seuraavat asiat:

- tekniset ja hallinnolliset ohjeet pätevään työskentelyyn
- käyttäjien käyttöoikeuksien rajoittaminen tehtäviin joihin on valtuutus ja joihin käyttäjät ovat perehtyneet
- tulisi ylläpitää tietoja käyttöoikeuksien haltijoista kattaen myös toimielimen ulkopuoliset tahot (toimittajan edustajat, sisäinen IT-tuki, jne.)
- käyttöoikeuksien (myös pääkäyttäjien) ja salasanojen tulee aina olla henkilökohtaiset
- salasanojen, joiden vaihtoväli on määritelty, tulisi olla vaihdettavissa vapaasti ja riittävän monimutkaisia

3.3 Tietojen luottamuksellisuuden varmistaminen

Toimielimellä tulee olla menettelyt asiakkaiden luottamuksellisten tietojen suojaamiseksi ja varmistamiseksi myös silloin, kun niitä säilytetään tai siirretään sähköisessä muodossa (ISO 17025 4.13). Säilytyksessä ja siirroissa tulee huomioida erilaiset käytössä olevat tekniset ratkaisut. Tulee huomioida erilaiset laitteet, kuten kannettavat tietokoneet, muistitikut ja älypuhelimet.

Monessa organisaatiossa myös sellaisilla henkilöillä ja tahoilla, jotka eivät ole suoranaisesti mukana akkreditoidussa toiminnassa, on pääsy tai yhteys tietojärjestelmään. Esimerkkejä näistä ovat tietohallinto (sisäinen tai ulkoinen, jos toiminto on ulkoistettu); tutkimus ja kehitys; tuotanto-osasto; myyntiosasto; hoitohenkilökunta; taloushallinto; toinen tietojärjestelmä, joka hakee tai päivittää tietoja jne. Arvioinnissa on arvioijan varmistuttava siitä, että toimielimellä on riittävät menettelyt järjestelmässä olevien tietojen luottamuksellisuuden takaamiseksi.

Toimeksiantoihin ja asiakkaisiin liittyvien tietojen (mikäli tarjouspyyntöjen, tarjousten ja sopimusten katselmusten yhteydessä käytetään sähköisiä menettelyjä tulee nekin huomioida arvioinnissa) suojaaminen voidaan varmistaa esimerkiksi seuraavin toimenpitein:

- jokaisella käyttäjällä (myös pääkäyttäjillä) on henkilökohtainen käyttäjätunnus ja salasana sekä työkuvaan kuuluvat käyttöoikeudet
- pääsy tietoihin määräytyy käyttöoikeuksien perusteella
- laittomat sisäänkirjausyritykset ovat luettavissa järjestelmälokista
- henkilökunnalla on salassapitosopimukset
- perehdyttämiskoulutuksessa korostetaan käsiteltävien tietojen luottamuksellisuutta
- toimielimen ulkopuolisilla käyttäjillä (esim. toimittajilla) on salassapito-sopimukset ja heitä perehdytetään riittävästi toimielimen toiminnassaan määrittelemään tietosuojan tasoon.

Silloin kun toimeksiantopyyntöjä tai tilauksia sekä vastauksia tai tuloksia siirretään sähköisesti, oikeellisuuden toteaminen on huomioitava. Luottamuksellisuuden tulee olla samalla tasolla, olkoon kyse sähköisestä tai paperimuodossa tapahtuvasta tiedonsiirrosta. Tiedon luonne ratkaisee tarvittavan menettelyn.

3.4 Sisäiset auditoinnit

Arvioitaessa sisäisten auditointien menettelyjä tulisi arvioijan varmistua, että sisäiset auditoinnit kattavat myös tietojärjestelmiin liittyvät asiat. Niitä ovat muun muassa sähköisessä muodossa olevien asiakirjojen, tiedotusmateriaalin (mukaan lukien mahdolliset WWW-sivut) ja tiedostojen hallinta, sähköinen tiedonsiirto ja tietojen luottamuksellisuuden säilyminen. Laboratorion olisi hyödyllistä määritellä auditoijien pätevyysvaatimukset myös tietoteknisiin asioihin liittyen.

3.5 Tietojärjestelmien kuvaus johtamisjärjestelmässä

Arvioijan on katsottava miten ja missä laajuudessa tietojärjestelmiin liittyvät tiedot on kuvattu johtamisjärjestelmässä. Kuvauksiin voi sisältyä esimerkiksi:

- yleiskuvaus, mielellään kaaviomuodossa, käytetyistä tietojärjestelmistä sekä niiden keskinäisistä rajapinnoista että rajapinnoista ulkopuolisiin järjestelmiin ja järjestelmien välisestä tiedonsiirrosta. Tässä tulisi yleisellä tasolla kuvata eri järjestelmiä: missä niitä käytetään ja mihin tarkoitukseen sekä niiden käyttämää laitteistoa, verkkoa ja varusohjelmistoja (käyttöjärjestelmät, tietokannat, tiedonsiirto-ohjelmat, jne.). Kuvauksen tulisi sisältää tiedot varajärjestelyistä ja menettelyistä miten toimitaan järjestelmien mahdollisten käyttökatkosten aikana sekä miten käyttökatkoksesta palaudutaan normaaliin tilanteeseen.
- järjestelmäkuvaukset laboratorion käyttämistä järjestelmistä sisältäen seuraavat tiedot:
- toimintakuvaus
- järjestelmärakenteen kuvaus, mielellään graafinen, (laitteisto, varusohjelmat, verkko, sovellukset, liitynnät muihin järjestelmiin)
- järjestelmän vastuuhenkilöt ja heidän toimenkuvansa, myös mahdolliset ylläpitosopimukset toimittajien kanssa
- käyttöoikeustasot, niiden jakoperiaatteet ja ylläpito mukaan lukien salasanakäytäntö
- varmuuskopiointiohjeet
- virustentorjuntaohjeet
- viittaukset järjestelmän dokumentointiin.

3.6 Asiakirjat ja tallenteet sekä niiden säilyttäminen ja arkistointi

Toimielimellä tulee olla menettelytavat (ISO 17025 4.3) siitä miten tietojärjestelmissä ylläpidettäviä asiakirjoja sekä tallenteita (laatu- ja tekniset tal-

lenteet) valvotaan. Menettelyjen ohjeistukseen tulisi sisältyä tiedot ainakin seuraavista asioista:

- asiakirjojen (voimassa olevat ja aikaisemmat versiot) sekä tiedostojen sijaintipaikka
- päivitysoikeudet ja -velvollisuudet
- asiakirjojen versiohallinta (miten erotetaan toisistaan voimassa olevat, valmisteilla olevat ja vanhentuneet versiot)
- arkistointiajan päätyttyä poistettavien asiakirjojen sekä tallenteiden hävittäminen
- asiakirjojen ja tallenteiden suojaus (miten muun muassa varmistetaan voimassa olevien ohjeiden koskemattomuus, sisällön muokkauksen esto hyväksynnän jälkeen)
- toimintatapa järjestelmän versiopäivityksen yhteydessä.

Kaikista johtamisjärjestelmän piiriin kuuluvista asiakirjoista (riippumatta siitä ylläpidetäänkö niitä paperiversioina tai sähköisesti) tulee olla kattava ajantasainen lista tai muu vastaava menettely, josta ilmenee asiakirjojen versio ja jakelu (ISO 17025 4.3.2).

Johtamisjärjestelmään kuuluvien asiakirjojen sekä toiminnassa syntyvien tiedostojen (laatu- ja tekniset tallenteet) säilyttäminen ja arkistointi on toteutettava siten että:

- asiakkaan luottamukselliset tiedot ja omistusoikeus turvataan
- tietokonejärjestelmät ja niissä säilytettävä tieto on ulkopuolisilta suojattu ja tietojen säilyminen on asianmukaisesti varmistettu
- virhettä korjattaessa alkuperäinen kirjaus tai tulos jää jäljelle
- käytettäessä tietojärjestelmää tai automaattisia laitteita tulosten keruuseen, käsittelyyn, tallentamiseen, raportointiin, varastointiin tai palauttamiseen tulee varmistua siitä, että tietojen suojaamiseksi on asianmukaiset ohjeet ja menettelytavat. Niihin tulee sisällyttää ainakin kuvaus siitä, kuinka syötettävien tietojen, tietojen säilyttämisen, tietojen siirron ja -käsittelyn osalta tietojen luottamuksellisuus ja eheys säilyy.

Arkistointi tietojärjestelmissä

Sopivin arkistointitapa määräytyy kunkin tiedon säilytystarpeen perusteella. Toimielimen tulee määritellä muun muassa mittaustietojen ja tulosten säilytysaika (ISO 17025 4.13.2). Arvioinnissa on katsottava miten säilytysaikoja määritettäessä on otettu huomioon esimerkiksi toimielimen ja asiakkaan väliset sopimukset, yleinen lainsäädäntö tai viranomaismääräykset.

Toimielimen on varmistuttava siitä, että tiedot säilyvät tietyn määräajan ja tällöin tulee määritellä tietokantojen ylläpito ja varmuuskopiointi. Varmuuskopiointi tulisi järjestää siten, että tapahtumasta tallentuu riittävä määrä tietoja lokitiedostoihin. Niiden avulla voidaan varmistua siitä, että varmuuskopiointi on sujunut halutulla tavalla. Ohjeissa tulisi käydä ilmi varmuuskopioinnin laajuus, tiheys, kopion säilytysaika ja -paikka, ja mikäli otetaan eri ikäisiä kopioita, niiden määrä. Käytettäessä rinnakkaisjärjestelmää tai -tietokantaa varmuuskopiona, tulee varmuuskopiointi suunnitella siten, että palautettavaksi ja varajärjestelmäksi tarkoitettu tietokanta eivät voi tuhoutua tai saada vääriä tietoja saman ohjelmavirheen tms. seurauksena. Muussa muodossa säilytettävästä tiedosta on yksityiskohtaisesti kuvattava tiedon säilyttämistapa, oletettu säilyvyys sekä ne toimenpiteet, joilla varmistetaan luettavuus ja palautettavuus arkistointiajan lopulla.

Arkistoidut tiedot tulee säilyttää turvallisessa paikassa ja sellaisessa ympäristössä, joka ei vaaranna tietojen säilyvyyttä tai palautettavuutta (ISO 17025 4.13.1.2).

Elektronisen tiedon säilyttäminen

Elektronisen tiedon säilyttämisellä tarkoitetaan kaikkia niitä tapoja ja vaiheita, joissa tietokoneen muistia, massamuistia tai muuta siihen liitettyä apuvälinettä käyttäen tallennetaan tietoa pidemmäksi ajaksi kuin ohjelman suorittaminen vaatii.

Toimielimen tulee huolehtia siitä, että säilytettäväksi tarkoitettuja tietoja voivat tallentaa vain ne henkilöt, joilla on siihen oikeus (ISO 17025 5.2.5). Yleensä se on toteutettu siten, että jokaisella käyttäjällä on oma henkilökohtainen tietojärjestelmän käyttöön oikeuttava käyttäjätunnus ja salasana.

Jos tieto tulee järjestelmään automaattisena siirtona toisesta järjestelmästä, on arvioinnissa varmistuttava siitä, että siirtotapahtumassa toimielin on varmistanut ja tarkistanut tietojen luottamuksellisuuden ja muuttumattomuuden.

Tietojen säilymisen ja muuttumattomuuden varmistamisessa ovat oleellisia menettelyt muun muassa tietojen päälle korjaamisen estämiseksi ja tietojen palauttamismahdollisuuden takaamiseksi.

Kun tuloksia säilytetään sähköisesti, primaaritulokset on suojattava muutoksilta ja tuhoutumiselta (ISO 17025 4.13.1.2). Jokaisesta tehdystä korjauksesta tulee ilmetä korjauksen tekijä ja alkuperäinen tulos (ISO 17025 4.13.2.3); päälle korjaamisen estäminen.

Mikäli kyseessä on ajantasalla pidettävän rekisterin kaltainen tiedon säilyttäminen, tulee tehtyjen muutosten olla jälkikäteen selvitettäessä esimerkiksi tietokoneen lokijärjestelmän avulla.

Joissakin virhetilanteissa joudutaan korjaamaan tietoja suoraan tietokannassa käyttämällä tietokantatyökaluja. Tällöin monessa tapauksessa saatetaan ohittaa järjestelmälokit. Siten niihin ei jää jälkeä tapahtumasta. Arvioinnissa on kiinnitettävä huomiota siihen, miten toimielin on menetellyt tai menettelisi sellaisissa tilanteissa.

Sähköisesti säilytettävien tietojen osalta tulisi kuvata menettelyt, joilla varmistetaan, että tiedot ovat palautettavissa varmuuskopioista. Mikäli johtamisjärjestelmän ohjeita tai muita vastaavia dokumentteja arkistoidaan sähköisesti, tulisi toimielimen varmistua dokumenttien palauttamis-mahdollisuudesta arkistointiajan lopulla. Varmuuskopiointi itsessään ei riitä takaamaan tietojen säilymistä, tietojen palauttaminen tulisi aina testata määräajoin käytännössä. Sovellusohjelmat eivät yleensä ole alaspäin yhteensopivia loputtomasti; toisaalta usein käytetään tuoreinta sovellusohjelman versiota. Johtamisjärjestelmässä tulisi kuvata toimet joilla turvataan aiemmalla versiolla tehdyt tiedostot tms. myös arkistointiajan lopulla.

3.7 Tietojärjestelmän hankinta ja käyttö (myös laitteet ja ohjelmistot)

Tietojärjestelmän hankinta on verrattavissa esimerkiksi ison testauksessa tai kalibroinnissa käytettävän laitteen hankintaan, mutta sen vaikutus toimie-limen toimintaan on yleensä laajempi kuin yksittäisen laitteen vaikutus. Sen vuoksi on arvioinnissa järjestelmähankintamenettelyiden toimivuuteen ja pätevyyteen kiinnitettävä erityistä huomiota.

Järjestelmän määrittely

Mikäli toimielin aikoo uusia tai vaihtaa tietojärjestelmänsä, tehtävään tulisi nimetä työryhmä, jolla tulisi olla riittävästi tietoa tietojärjestelmistä. Työryh-män tulisi olla hyvin perehtynyt toimielimen toimintaan ja tuntea myös akkreditointivaatimukset.

Työryhmän tulisi huolehtia siitä, että toimielimessä tehdään tarveanalyysi uuden järjestelmän ominaisuuksien määrittelemiseksi. Tarveanalyysin voi tehdä toimielin itse tai ulkopuolinen riippumaton taho. Analyysin tuloksena syntynyttä ominaisuusluetteloa tulisi hyödyntää tarjouspyyntöä laadittaessa. Akkreditointivaatimusten asettamat yleiset vaatimukset hankittavalle järjestelmälle olisi hyvä mainita tarjouspyynnössä.

Järjestelmän hankinta ja käyttöönotto

Tietojärjestelmän hankinnasta vastuussa olevan työryhmän tulisi huolehtia siitä, että hankintapäätös voidaan tehdä mahdollisimman kattavan aineiston perusteella. Valmistelevaan työhön voi kuulua muun muassa toimittajalistan laatiminen, haastattelut ja vierailut muissa toimielimissä sekä vertailujen laatiminen eri ohjelmien välillä.

Tietojärjestelmän käyttöönottoa, henkilökunnan koulutusta ja järjestelmän testausta on suunniteltava ja dokumentoitava tavalla, joka vastaa toimielimen johtamisjärjestelmän vaatimuksia.

Toimielimellä tulisi olla kirjalliset ohjeet tietojärjestelmien asennuksesta, validoinnista, ylläpidosta ja huollosta.

Uuden järjestelmän käyttöönottoa tulisi edeltää riittävän pitkä koeajovaihe. Järjestelmän vaihtamisesta vastuussa olevan henkilön tulisi valvoa järjestelmän testaamista ja huolehtia tulosten dokumentoinnista. Hänen tulee lopuksi hyväksyä järjestelmä käyttöön otettavaksi (ISO 17025 5.4.5 ja 5.5.2).

Toimielimellä tulisi olla kokonaisvaltainen kuvaus järjestelmästä. Kuvauksen yksityiskohtaisuus riippuu siitä kuinka suuressa määrin tietojärjestelmä vaikuttaa toimielimen toiminnan laatuun. Kuvaus voi sisältää esimerkiksi:

- tiedot järjestelmän osista (laitteet, varusohjelmistot, sovellusohjelmistot) ja toimittajista
- tiedot järjestelmän sen hetkisestä kokoonpanosta; ohjelmistoversiot ja asennuspäivät ym., (hyvä tapa on kopio hakemistosta, josta näkyy tiedostojen talletuspäivä ja koko)
- järjestelmän toiminnallisen kuvauksen
- kaavion organisaation tietojärjestelmästä sisältäen laitteisto- ja verkkoarkkitehtuurin sekä tiedonsiirron järjestelmän eri osien välillä
- kaaviomuotoisen ja/tai sanallisen kuvauksen toimielimen tietojärjestelmän toiminnoista kattaen kaiken toimielimen hyödyntämän tietotekniikan (tilausten/pyyntöjen vastaanotto, näytteiden kirjaus, tulosten käsittely ja siirto laitteilta/manuaalinen syöttö, laadunvarmistus, hyväksyntämenettelyt, arkistointi, tallennus, raportointi, tiedonsiirto)
- käyttöohjeen
- toimielimen mahdollisesti laatiman sovellusohjeen
- laskentakaavojen ja korjauskertoimien kuvauksen
- menetelmien mittausepävarmuuksien (lähinnä testaus- ja kalibrointilaboratoriot) määrittämistavan.

Järjestelmäkuvausta tulisi päivittää jokaisen merkittävän muutoksen jälkeen.

Ohjelmapäivityksessä tulisi aina varmistua siitä, että uusi ohjelmaversio on hyvin testattu ja dokumentoitu. Virheettömästä toiminnasta järjestelmän eri ohjelmien välillä tulee varmistua ennen päivitystä. Vanhasta ohjelma-versiosta tulee mahdollisuuksien mukaan säilyttää arkistokappale, jotta häiriötilanteen sattuessa on tarvittaessa mahdollisuus palata aikaisempaan versioon. Vanhan version palautus voi vaatia pitkääkin käyttökatkoa, mikä olisi syytä tunnistaa etukäteen. Tietokannasta tulisi ottaa varmuuskopio ennen päivitystä sekä siihen mahdollisesti liittyvää tietokanta-konversiota.

Ennen kuin toimitettava järjestelmä otetaan toimielimessä tuotantokäyttöön, tulisi suorittaa vastaanottotesti, jossa ohjelmisto testataan tehdyn testaus-suunnitelman mukaisesti. Vastaanottotestistä tulisi laatia kirjallinen testaus-pöytäkirja, jonka tilaaja ja toimittajat allekirjoittavat. Siihen tulisi kirjata testauksen kuluessa havaitut puutteet mahdollisimman tarkasti ja niiden korjauksesta tulisi sopia.

Ympäristö

Tietojärjestelmän piiriin kuuluvien laitteiden, etenkin palvelimien tulisi sijaita ympäristössä, joka takaa järjestelmän varman ja turvallisen toiminnan. Toimielimen tulisi ottaa huomioon ainakin seuraavia asioita: kulunvalvonta luottamuksellisuuden takaamiseksi, tilan häiriösuojaus (muun muassa säh-köverkosta tai muista laitteista tulevat kenttähäiriöt), lämpötilan valvonta (seuranta, säätö jne.) sekä virransaannin turvaaminen (esimerkiksi UPS).

Toiminta vikatilanteessa

Toimielimellä on oltava menettelyt sellaisia tilanteita varten, joissa on havaittu toimintahäiriöitä (virheitä tai vikoja) tietojärjestelmissä tai laitteistoissa (ISO 17025 4.9). Menettelyjen tulee kattaa myös tilanteet joissa joudutaan toimimaan manuaalisesti tietojärjestelmän toimintavian vuoksi. Kaikki tieto-kantoihin sattuneet virheet ja niihin tehdyt korjaustoimenpiteet, esimerkiksi tietokantatyökaluja käyttäen, tulisi kirjata lokikirjaan tai vastaavaan tiedos-toon.

3.8 Menetelmien validointi ja mittausepävarmuus

Mikäli akkreditoitaviin/akkreditoituihin menetelmiin liittyy laskentakaavoja, joiden laskemisessa hyödynnetään tietojärjestelmiä, laskentakaavojen va-lidointi sisältyy menetelmien validointiin. Siinä tulisi muun muassa dokumen-

toida käytettävät kaavat ja kertoimet sekä varmistaa laskennan oikeellisuus ja selvittää muun muassa miten tulokset pyöristetään.

Mittaustulosten tarkkuutta arvioitaessa on määritettävä vaikuttavatko esimerkiksi eri laitteista tai järjestelmistä saatujen tietojen käsittely tulokseen. Ohjelmistopäivitysten ja vastaavien muutosten yhteydessä on varmistuttava laskentakaavojen ja tulostarkkuuden säilymisestä esimerkiksi empiirisillä testeillä.

3.9 Tulosten raportointi

Yleistä

Tietotekniikan käytön lisääntymisen myötä tuloksia toimitetaan nykyään paperiversioiden lisäksi paljon sähköpostiliitteenä tai järjestelmien välisenä tiedonsiirtona tai siten, että ne ovat asiakkaan luettavissa suoraan internetin välityksellä. Myös näissä tapauksissa toimielimen on otettava huomioon akkreditointivaatimukset tulosten raportoinnille. Esimerkiksi standardin (ISO 17025 5.10) mukaan asiakkaalle toimitettavan, kalibroinnin ja/tai testauksen tulokset tulee raportoida tarkasti, selkeästi, yksikäsitteisesti ja objektiivisesti sekä mahdollisten menetelmiin liittyvien erityisohjeiden mukaisesti. Tulokset raportoidaan yleensä selosteena tai todistuksena (testausseloste, tutkimusselostus, tutkimustodistus, kalibrointitodistus tms.), joiden tulee sisältää kaikki asiakkaan vaatimat tiedot, kaikki tulosten tulkinnan kannalta välttämättömät tiedot ja kaikki menetelmän vaatimat tiedot. Sisäiselle asiakkaalle tai asiakkaalle, jonka kanssa on kirjallisesti sovittu, voidaan tulokset raportoida yksinkertaistetussa muodossa (kts. ISO 17025 5.10.1).

LIMS -järjestelmien tuottamat selosteet

Tietokantapohjaisista LIMS-järjestelmistä voidaan tuottaa raportteja kiinteisiin raporttipohjiin tai tekemällä ns. ad hoc -hakuja. Selosteet tulostetaan yleensä kiinteitä raporttipohjia käyttäen. Näiden etuna on, että tietty seloste voidaan tulostaa tarvittaessa uudestaan. Tällä tavalla tulostettuja raportteja ei yleensä tallenneta sähköisesti lopullisessa muodossaan vaan oletetaan, että tiedot ovat uusittavissa tulostamalla ne uudestaan tietokannasta. On kuitenkin huomioitava, että mikäli raporttipohjaa kehitetään tai muutetaan tai mikäli järjestelmään tehdään muutoksia tai päivityksiä, selostetta ei enää yleensä voida tulostaa identtisenä muuten kuin säilyttämällä kaikki vanhat raporttipohjaversiot. Ohjelmistopäivitysten jälkeen vanhat versiot raporttipohjista voivat kuitenkin käydä käyttökelvottomiksi. Sisällön oikeellisuus (verrattuna ulkoasuun) on kuitenkin oleellista.

Toimistosovelluksilla tehtävät raportit (tekstinkäsittely, taulukkolaskenta)

Toimielimissä tehdään usein raportteja toimistosovelluksilla (esim. tekstinkäsittely-, taulukkolaskenta- ja tekstitiedostot). Niillä tuotetut raportit saattavat versiopäivitysten yhteydessä myös muuttaa ulkomuotoaan kuten edellisessä kohdassa.

Silloin kun tuloksia toimitetaan asiakkaille editoitavassa sähköisessä muodossa, on otettava huomioon, että asiakas voi muuttaa tuloksia vahingossa. Tällaisissa tapauksissa on tärkeää, että toimielin pystyy osoittamaan lähettämänsä alkuperäisen raportin sisällön.

Toimielimellä tulisi olla menettelyt muun muassa logonsa ja akkreditointitunnuksen käytölle sähköisesti lähetetyssä muokattavassa dokumentissa. On suositeltavaa tallentaa dokumentit vain luettavaksi tarkoitetussa (read-only) muodossa.

Tulosten tulostaminen muun kuin toimielimen toimesta

Toimielimet voivat tarjota asiakkailleen mahdollisuuden hakea itse tuloksia esimerkiksi internetin kautta tai suoraan tietokannasta. Näissä tilanteissa on kiinnitettävä erityistä huomiota toimielimen menettelytapoihin, joilla se on varmistanut, että haettavat tiedot saadaan käyttöön oikein.

Asiakkaat, joilla on mahdollisuus itse hakea tuloksia tietokannasta ovat yleisimmin sisäisiä asiakkaita (tutkijat ja tuotekehittäjät, tuotanto-osastot, myynti, ympäristövalvonta jne., sekä esimerkiksi kliinisissä laboratorioissa hoitohenkilökunta).

Sähköinen allekirjoitus

Perinteisesti toiminnan tulokset raportoidaan vastuullisen henkilön allekirjoittamana. Kun nykyään tuloksia käsitellään ja raportoidaan sähköisesti, käsintehdyn allekirjoituksen sijaan on otettu käyttöön muita varmennusmenettelyjä, joista sähköinen allekirjoitus on yleisesti hyväksytty käyttöön yhteiskunnassamme.

EU on direktiivissään (1999/93) hyväksynyt sähköisen allekirjoituksen virallisissa dokumenteissa. Myös FDA on laatinut ohjeet sähköisten allekirjoitusten käytöstä (CFR 21 Part 11). Helmikuun 2003 alusta tuli Suomessa voimaan laki sähköisestä allekirjoituksesta (24.1.2003/14). Sen jälkeen on tullut myös laki vahvasta sähköisestä tunnistamisesta ja

sähköisistä allekirjoituksista (7.8.2009/617). Siten sähköinen allekirjoitus on oikeudellisesti yhtä pätevä kuin käsin tehty allekirjoitus. Lakien tarkoittama sähköinen allekirjoitus edellyttää laatuvarmenteiden käyttöä. Edellä mainituissa laissa on myös säädetty laatuvarmenteiden sisällön vähittäisvaatimuksista.

Standardissa (ISO 17025 5.10.2) todetaan, että testausselosteessa tai kalibrointitodistuksessa tulee olla sen hyväksyjän nimi, asema ja allekirjoitus tai vastaavat tunnistetiedot. Arvioinnin ja toimielimen toiminnan kannalta tärkein kysymys lienee ”tunnistetietojen” selkeys ja yksiselitteisyys. Arvioinnissa voidaan ottaa lähtökohdaksi, että ”tunnistetiedot” ovat riittävät silloin, kun ne ovat rinnastettavissa allekirjoitukseen. Muiden tunnistetietojen käytöstä tulisi sopia asiakkaan kanssa. On kuitenkin otettava huomioon, että kaikilla sektoreilla ja asiakasryhmillä (esimerkiksi ulkomaiset asiakkaat) ei muunlainen kuin käsin tehty allekirjoitus välttämättä ole kelvollinen.

Testausselosteiden ja kalibrointitodistusten arkistointi

Laboratorion on dokumentoitava missä muodossa, miten ja kuinka pitkäksi aikaa selosteet arkistoidaan. Lisäksi standardissa (ISO 17025 4.13.2.1.) edellytetään, että jokaisesta annetusta selosteesta säilytetään kopio määrätyn ajan. Kopio voi olla esimerkiksi paperikopio, mikrofilmi, muuttumattomana arkistossa säilyvä sähköinen asiakirja tai tietokannasta reprodusoitavissa oleva raportti.

4 Tietotekniikan termejä

Tietotekniikan alaan kuuluvia termejä on valtaisa määrä ja lisäksi termistö muuttuu koko ajan alan kehittymisen myötä. Internetistä löytyy runsaasti linkkejä tietotekniikan sanastoihin, joita ylläpitävät muun muassa monet yliopistot ja korkeakoulut sekä tietotekniikan alan yhdistykset. Julkisessa hallinnossa on yleisesti käytössä Valtionhallinnon tietoturvasanasto (VAHTI, 8/2008), jossa olevia termejä on paljon käytetty tässä oppaassa.

5 Viitteet

SFS-EN ISO/IEC 17025:2005 Testaus- ja kalibrointilaboratorioiden pätevyys. Yleiset vaatimukset.

EUROLAB Technical Report 2/2006 Guidance for the management of computers and software in laboratories with reference to ISO/IEC 17025/2005.