



TIETOSUOJAVALTUUTETUN TOIMISTO

LAADI TIETOTILINPÄÄTÖS

24.4.2012

Opas on päivitetty huhtikuussa 2012, eikä sen tietosuoja-asetuksen mukaisuutta ole arvioitu. Euroopan unionin yleistä tietosuoja-asetusta on alettu soveltaa 25.5.2018, ja sen tuomista oikeuksista ja velvoitteista on kerrottu verkkosivuillamme.

www.tietosuoja.fi

SISÄLTÖ

1. MIKÄ ON TIETOTILINPÄÄTÖS

2. MIKSI TIETOTILINPÄÄTÖS KANNATTAÄ TEHDÄ

- 2.1. Tietotilinpääätös luottamuksen rakentajana
- 2.2. Tietotilinpääätös johdon työvälineenä
- 2.3. Tietotilinpääätös sisäisen ja ulkoisen valvonnan apuvälineenä

3. MITEN TIETOTILINPÄÄTÖS TEHDÄÄN

- 3.1. Tietotilinpääätökseen sisällytettävät tiedot
- 3.2. Organisaation hallussa olevat tietovarannot
- 3.3. Tietojen käsittelyssä noudatettavat menettelytavat ja periaatteet
- 3.4. Tietojen suojaus
- 3.5. Tietojen käsittelyn seuranta ja valvonta
- 3.6. Rekisteröityjen oikeuksien toteutuminen

4. ARVIOINTI JA KEHITTÄMISKOHTEET

1. MIKÄ ON TIETOTILINPÄÄTÖS

Tilinpäätöksellä on pitkä historia organisaatioiden taloudellisen aseman raportoinnin muotona. Tilinpäätösraportointi on laajentunut myös yleisemmin organisaation toiminnan eri osa-alueilla sekä sisäisen valvonnan ja riskienhallinnan järjestämiseen. Taloudellista tilinpäätöstä täydentäviä raportoinnin muotoja ovat yritysten ja yhteisöjen yhteiskunta- ja ympäristövastuuraportit sekä henkilöstötilinpäätös. Tälle kehitykselle luonteva jatkumo on tilinpäätösluonteisen tarkastelun ulottaminen tietovarantoihin, tietojohdamiseen, tietojenkäsittelyyn ja tietoturvallisuuteen.

Tietotilinpäätös voi täydentää lakisääteistä tilinpäätöksiin ja toimintakertomuksiin kuuluvaa raportointia, mutta tarkoituksena ei ole tarpeettomasti lisätä organisaation hallinnollista taakkaa. Tietotilinpäätöksen tarkoituksena on toimia dynaamisena työkaluna, joka tukee organisaation tehokkuutta, vaikuttavuutta ja kilpailukykyä.

Tämän oppaan tarkoituksena ei ole esittää tyhjennävää kaavaa tai luetteloa tietotilinpäätökseen sisällytettävistä tiedoista. Tietotilinpäätökseen sisältö voi vaihdella organisaation toimialasta ja toiminnan laadusta riippuen. Tietotilinpäätös kannattaakin ottaa käyttöön siinä laajuudessa, kun sillä arvioidaan olevan positiivisia vaikutuksia organisaation toimintaan.

Tietotilinpäätös on osa tietojohdamista ja sitä voidaan käyttää organisaation sisäisenä tietojohdamisen raporttina. Tietotilinpäätöksellä voidaan myös raportoida organisaation sidosryhmille tietojen käsittelyä koskevista keskeisistä asioista. Tietotilinpäätös on organisaation sisäisen tarkastelun tuloksena syntyvä raportti, joka esimerkiksi:

- antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta
- kuvaa mitä tietovarantoja organisaation hallussa on
- kuvaa organisaation toimintaan liittyvät tietovirrat
- kuvaa organisaation tietovirtojen yhteentoimivuuden tietojenkäsittelyn kanssa
- kuvaa miten tietosuojat ja -turvat toteutuvat organisaation toiminnassa
- kuvaa miten tietojenkäsittelyyn liittyvä riskienhallinta on toteutettu
- toimii suunnittelun ja toiminnan ohjauksen tukena organisaatiossa
- toimii raportoinnin ja johtamisen tukena organisaatiossa
- toimii kehittämistoimenpiteiden seurannan apuvälineenä
- toimii organisaatiosta ulospäin tapahtuvan sidosryhmäraportoinnin välineenä
- varmistaa sovellettavan lainsäädännön noudattamisen

Useiden tietotilinpäätöksessä käsiteltävien asioiden huomioon ottaminen sisältyy jo tällä hetkellä henkilötietolain periaatteisiin (mm. suunnittelu-, huolellisuusvelvoite ja suojaamisvelvoite). Tietotilinpäätös toteuttaa myös ns. accountability- eli "tilintekovelvollisuus"-periaatetta. Tämän periaatteen mukaan organisaatio itse näyttää, että se noudattaa lakia, hyvää tietojenkäsittelytapaa ja hyvää tiedonhallintatapaa. Tietosuoja koskeva lainsäädäntö saattaa tulevaisuudessa edellyttää tilintekovelvollisuusperiaatteen mukaisten menettelyjen käyttöön ottamista. Organisaatiot voivat kuitenkin jo ennakolta itseohjautuvasti ottaa käyttöönsä tietotilinpäätöksen. Tietotilinpäätöksessä tapahtuva dokumentointi ohjaa myös systemaattisesti läpikäymään asioita ja tarkastelemaan niitä kriittisemmin.

2. MIKSI TIETOTILINPÄÄTÖS KANNATTAA TEHDÄ

Tietojen korkea laatu ja toimivat menettelytavat tietojen käsittelyssä vaikuttavat positiivisesti kaikkiin organisaation toiminnan osa-alueisiin. Tieto on arvokas ja ainoa voimakkaasti kasvava tuotannontekijä. Erilaisten tietovarantojen ympärille kehittyvät jatkuvasti uusia palveluja, jotka ovat tärkeitä koko tietoyhteiskunnan menestymiselle.

Verkko- ja tietoyhteiskunnassa tietojen käsittelyllä on suuri merkitys henkilöiden ja organisaatioiden oikeuksien ja velvollisuuksien toteutumiselle. Esimerkiksi Euroopan ihmisoikeustuomioistuin on päätöksessään NO. 20511/03 arvioinut ihmisoikeussopimuksen soveltuvan myös tietojärjestelmien vaikutusten arviointiin. Julkisen sektorin osalta tietosuoja ja tietoturva ovat myös tulleet pysyviksi osiksi hyvää hallintotapaa. Tietojen käsittely vaikuttaa myös olennaisesti kilpailukykyyn, vaikuttavuuteen ja organisaation tehokkuuteen.

Uusien palvelujen ja sähköisten palveluprosessien edellytyksenä on tietorakenteiden ja tiedonhallintaan liittyvien menetelmien kehittäminen. Tämä luo uusia haasteita tietojen turvalliselle ja vastuulliselle käsittelylle. Esimerkkinä uusista haasteista on tietokonekapasiteetin ja -palveluiden ostaminen ja hyödyntäminen erilaisten ns. pilvipalvelujen välityksellä. Nykyisin onkin olemassa selkeä tarve kokonaisvaltaiseen näkökulmaan tietovarantojen hallinnassa, ratkaisu tällaisiin tarpeisiin on tietotilin päätöksen laatiminen.

Tietotilin päätös kuvaa henkilötietolain mukaisen hyvän tietojenkäsittelytavan noudattamista. Viranomaisten osalta tietotilin päätös kuvaa viranomaisen toiminnan julkisuudesta annetun lain (621/1991) 18 §:ssä tarkoitetun hyvän tiedonhallintatavan noudattamista. Hyvä tiedonhallintatapa edellyttää, että käsiteltävän tiedon saatavuus, suoja ja laatu turvataan. Tietotilin päätöksen avulla voidaan arvioida ja edistää myös tietohallintolaissa (634/2011) tarkoitettua tietojärjestelmien yhteentoimivuutta.

Kokemuksien mukaan tietotilin päätös on erityisen hyödyllinen viranomaisorganisaatioissa, joiden toiminta perustuu suurten tietovarantojen käsittelyyn ja rekisterinpitäjien keskinäiseen yhteistyöhön.

Henkilötietolain keskeisimmät säännökset hyvän tietojenkäsittelytavan näkökulmasta ovat lain 2 luvun keskeiset periaatteet:

- huolellisuus- ja laillisuusvelvoite (5 §)
- henkilötietojen käsittelyn etukäteissuunnittelu (6 §)
- henkilötietojen käyttötarkoitussidonnaisuus ja käsittelyn rajoitukset (7-8 §)
- henkilötietojen laatua koskevat periaatteet (9 §)

Henkilötietolain luku 7 sisältää määräykset tietoturvallisuudesta, tietojen säilytyksestä ja suojaamisesta.

Tietotilin päätöksessä voidaan kuvata myös muun lainsäädännön ja esimerkiksi tietoturvaa koskevien standardien noudattamista.

2.1. Tietotilin päätös luottamuksen rakentajana

Riskien minimointi, hyvän maineen rakentaminen, kansalaisten ja kuluttajien luottamuksen säilyttäminen ovat asioita, joista on tulossa ratkaisevan tärkeitä kaikkien sektoreiden toiminnan menestymiselle. Näiden tavoitteiden edistämiseksi ja kilpailuetuja saadakseen vastuulliset organisaatiot käyttävät toimintaansa tukevia menettelytapoja ja tekevät enemmänkin kuin lainsäädäntöön sisältyvät vähimmäisvaatimukset edellyttävät.

Erityisesti verkkoympäristössä tietosuojaan liittyvät puutteet koetaan ongelmana asioinnin luotettavuuden ja käytettävyyden kannalta. Vääriin käsiin joutuneet henkilötiedot ovat uhka tietojen kohteen eli rekisteröidyn oikeuksille ja tietojen suojauksen laiminlyönnistä vastuullisen organisaation toiminnalle.

Asiakkaiden ja sidosryhmien luottamus organisaation menettelytapoihin tietosuojan ja tietoturvan osalta on toimintaa vahvasti tukeva tekijä. Tietosuojan ja tietoturvan huomioiminen, esimerkiksi verkkopalveluiden yhteydessä on laissa säädetyn velvollisuuden ohella myös oleellinen osa hyvää palvelua.

Tietotilin päätös kertoo eri sidosryhmille, että organisaatio näkee tärkeäksi panostaa tietojen käsittelyssä noudatettaviin menettelytapoihin ja hyvän tietojenkäsittelytavan sekä tiedonhallintatavan noudattamiseen.

2.2. Tietotilin päätös johdon työvälineenä

Tiedonhallinnan kytkeminen osaksi organisaation johtamista on eräs organisaation toiminnan merkittäviä haasteita. Johdolla on välttämätöntä olla kokonaiskuva organisaation informaatioarkkitehtuurista ja organisaation toiminnassaan tarvitsemista tiedoista ja niiden välisistä suhteista.

Tietotilin päätös palvelee organisaation johdon päätöksentekokykyä, asiakkaiden ja sidosryhmien tiedollisia tarpeita. Tietotilin päätös on myös osa tietojohtamista sekä siihen kuuluvaa riskienhallintaa ja sisäistä valvontaa.

Tietoturvallisuuden ja tietosuojan säännöllinen arviointi on osa organisaation tietojohtamista. Arvioinnin tavoitteena on varmistaa tarjottavien palvelujen toimintakyky ja käytettävyyden, tietoaineistojen laatu ja käytössä olevan tietotekniikan turvallisuus. Arvioinnin tavoitteena on myös varmistaa palvelujen tuottamiseen liittyvien tietoturvallisuuden johtamis- ja hallintajärjestelmien toiminta.

2.3. Tietotilin päätös sisäisen- ja ulkoisen valvonnan apuvälineenä

Organisaation on huolehdittava siitä, että sisäinen valvonta on asianmukaisesti järjestetty. Sisäisen valvonnan asianmukaisuudesta ja riittävydestä vastaa organisaation johto. Organisaation oma etu on tehokkaasti valvoa sekä tarkastaa sisäisen ja ulkoisen tarkastuksen keinoin myös tietojenkäsittelyjärjestelmiään; toisaalta asiaan liittyy voimakas yleinen lainvalvontaintressi. Tietotilin päätöksellä voidaan toteuttaa nämä molemmat tarpeet. Tietotilin päätös palvelee myös lainvalvontaviranomaisten tiedonsaantitarpeita.

Tietotilin päätös laaditaan seurantakausittain, joka mahdollistaa tietotilin päätöksessä kuvattujen ja arvioitujen kysymysten johdonmukaisen seurannan. Seurantakausi voi olla kalenterivuosi tai jokin muu organisaation tarpeista johtuva ajanjakso. Tietotilin päätös voidaan nivota sisäisen valvonnan ja riskienhallinnan järjestämisen näkökulmasta osaksi

Opas on päivitetty huhtikuussa 2012, eikä sen tietosuojasetuksen mukaisuutta ole arvioitu.

organisaation yleistä tilinpäätös- tai toimintakertomusmenettelyä, tulosoajasta tai tulosraportointia.

3. MITEN TIETOTILINPÄÄTÖS TEHDÄÄN

Tietotilinpäätöksen tavoitteena on antaa kuvaus tietojen käsittelyn nykytilasta sekä arvio tietosuojan ja tietoturvan toteutumisesta. Tietotilinpäätöksessä kartoitetaan myös tietojen käsittelyyn liittyviä kehittämistarpeita ja niiden edellyttämiä toimenpiteitä.

Tietotilinpäätös voi kuvata esimerkiksi:

- mitä tietovarantoja organisaation hallussa on
- mikä on organisaation tietoarkkitehtuuri
- mikä on organisaation hallussa olevien tietojen laatu ja käytettävyys
- mitä menettelytapoja ja periaatteita tietojen käsittelyssä noudatetaan
- miten tiedot on suojattu
- miten tietojen käyttöä valvotaan
- miten rekisteröityjen oikeudet tietojen käsittelyssä toteutetaan

Tietotilinpäätös sisältää arvioinnin tietojen käsittelyssä havaituista kehittämiskohteista ja kehittämistoimenpiteistä.

Tietotilinpäätöksen tekemiseen voivat osallistua organisaatiossa ainakin tietotekniikasta, tietosuojasta ja tietoturvasta sekä varsinaisesta substanssitoiminnasta vastaavat tahot.

3.1. Tietotilinpäätökseen sisällytettävät tiedot

Tietotilinpäätökseen sisällytettävät tiedot voivat vaihdella organisaation toimialasta ja toiminnan laadusta riippuen. Seuraavassa esimerkkejä asioista, joita voidaan sisällyttää tietotilinpäätökseen.

3.2. Organisaation hallussa olevat tietovarannot

Organisaatiossa tietoja kerätään ja käsitellään monissa tietojärjestelmissä ja sovelluksissa. Organisaation johdolla ei aina ole käsitystä siitä, mitä tietoja organisaation hallussa on. Irrallisten tietojen käsittely erillään olevissa tietojärjestelmissä vaatii runsaasti resursseja ja muodostaa uhan tietosuojan ja tietoturvan toteutumiselle.

Henkilötietojen käsittelyn näkökulmasta on tärkeää arvioida eri käyttötarkoituksiin muodostetut henkilörekisterit, niiden tietosisältö ja perusteet rekisterien pitämiseen. Hyvän tiedonhallintavan näkökulmasta organisaatiolla tulee olla selkeä kuva tietojärjestelmistään ja sen tulee huolehtia tietojen laadusta ja saatavuudesta.

Tietovarantojen suojaustaso, salassa pidettävyys, tietojen arkaluonteisuus on tarkoituksenmukaista arvioida tietovarantojen kartoittamisen yhteydessä. Tietovarantojen välisten tietovirtojen kartoittaminen on tärkeää, koska yhä suurempien tietovirtojen hallinta tuo esille kysymyksiä esimerkiksi tiedon omistajasta. Tietovarantojen ja tietovirtojen kuvaus

Opas on päivitetty huhtikuussa 2012, eikä sen tietosuoja-asetuksen mukaisuutta ole arvioitu.

voidaan tehdä tietotilinpäätöstä varten tai ne voivat olla erikseen ylläpidettynä organisaatiossa arkkitehtuurikuvauksina tai muina vastaavina kuvauksina.

Tietotilinpäätös voi sisältää kuvauksen organisaation keskeisimmistä tietovarannoista ja tietovirroista sekä arvion tiedon laadusta. Tietotilinpäätöksessä voidaan myös kuvata tietojen käsittelyn kannalta tärkeimmät tunnusluvut, esimerkiksi käsiteltyjen tietoyksiköiden lukumäärät, saatujen ja luovutettujen tietojen sekä tietojen luovutustapahtumien lukumäärät. Tiedon laadun arviointi liittyy läheisesti tiedon arvon ja käytettävyyden arviointiin.

Tietojen laatua tietotilinpäätöksessä voidaan arvioida eri näkökulmista, esimerkiksi:

- laadun arvioimiseen liittyvät menettelytavat ja kriteerit
- laadun arvioinnissa saadut tulokset, tietojen:
 - oikeellisuus
 - tarpeellisuus
 - täydellisyys
 - ajantasaisuus

3.3. Tietojen käsittelyssä noudatettavat menettelytavat ja periaatteet

Menettelytapojen osalta voidaan kuvata esimerkiksi:

- tietojen käsittelyyn vaikuttava keskeinen lainsäädäntö
- toimintaperiaatteet
- käytännesäännöt
- tietoturva- ja jatkuvuussuunnitelmat
- muu tietojen käsittelyä koskeva ohjeistus
- tietojen käsittelyn ulkoistamiseen liittyvät menettelytavat ja sopimukset
- tietojärjestelmien ylläpitoon ja hankintaan liittyvät menettelyt ja sopimukset

Tiedon käsittely on syytä arvioida koko tiedon elinkaaren ajalta. Tietojen käsittelyn toimintaperiaatteiden osalta voidaan arvioida esimerkiksi:

- tietojen saamiseen ja luovuttamiseen liittyvät menettelytavat
- käyttöoikeushallinta
- erityisesti sähköiseen tiedonsiirtoon liittyvät tietosuoja- ja tietoturva vaatimukset

Tietotilinpäätöksessä arvioidaan sitä, onko organisaation henkilökunnalla tarvittava tieto käsiteltävien tietojen julkisuudesta, salassapidosta ja tietojen suojaamisessa noudatettavista menettelyistä sekä tietoturvallisuusjärjestelyistä ja tehtävänjaosta. Arvioidaan myös, miten tietojen käsittelyyn liittyvä henkilöstölle annettava ohjaus ja koulutus on järjestetty sekä millä tavoin ohjeet ja koulutus pidetään ajan tasalla.

3.4. Tietojen suojaus

Tietotilinpäätöksessä voidaan kuvata kuinka rekisterinpitäjä toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.

Opas on päivitetty huhtikuussa 2012, eikä sen tietosuojasetuksen mukaisuutta ole arvioitu.

Tietotilinpäätöksessä voidaan arvioida:

- tietojen suojaamiseen liittyvät periaatteet ja menettelytavat
- tietoturvallisuuteen liittyvät keskeiset tavoitteet ja toteutuskeinot
- noudatettavat tietoturvallisuuden hallintaan liittyvät standardit
- sisäiset ja ulkoiset evaluoinnit
- riskienhallinnan menettelytavat
- tietoturvallisuuden organisointi
- vastuut ja kehittämisprosessi, menettelytavat

3.5. Tietojen käsittelyn seuranta ja valvonta

Organisaation tulee varmistaa, että hyvän tietojenkäsittelytavan ja hyvän tiedonhallintavan toteuttamiseksi annettuja säännöksiä ja ohjeita noudatetaan ja valvotaan. Hyvän tiedonhallintatavan edellyttämät toimenpiteet toteutetaan siten, että eri osapuolten oikeusturva toteutuu.

Tietojen käsittelyn valvonta voi olla osa organisaation muuta sisäistä valvontaa ja riskien hallintaa. Myös valvonnan tuloksia ja niiden perusteella tehtyjä toimenpiteitä on syytä arvioida.

Tietotilinpäätöksessä voidaan kuvata muun muassa:

- tietojen käsittelyyn kohdistuvaa riskien arviointia ja hallintaa
- tietovarantojen ja tietovirtojen laadun valvomiseksi tehtyjä toimenpiteitä
- tietojen käsittelyprosessien valvomiseksi tehtyjä toimenpiteitä
- organisaation henkilöstön ja yhteistyökumppaneiden tietojen käsittelytoimenpiteiden valvomiseksi tehtyjä toimenpiteitä
- valvonnan ja seurannan perusteella tehtyjä toimenpiteitä ja kehittämistoimia

Sisäisen valvonnan ohella voidaan kuvata myös ulkoista laillisuusvalvontaa suorittavien viranomaisten sekä tuomioistuinten päätökset seurantakaudella ja niiden vaikutus organisaation toimintaan. Lisäksi tietotilinpäätöksessä voidaan arvioida tietojen käsittelyn valvonnan ja seurannan riittävyttä ja kehittämistarvetta.

3.6. Rekisteröityjen oikeuksien toteutuminen

Rekisteröityjen oikeuksien toteutumista voidaan arvioida henkilötietolain mukaisen tarkastusoikeus- ja virheenkorjauspyyntöjen lukumäärän ja pyyntöihin annettujen vastausten perusteella. Rekisteröityjen informoinnin osalta on syytä arvioida myös rekisteri- ja tietosuojaselosteiden saatavilla pito.

4. ARVIOINTI JA KEHITTÄMISKOHTEET

Tilinpäätöksessä tunnistetaan nykytilanteen analysoinnin kautta ilmeneviä kehittämis- ja mittaamistarpeita sekä niihin liittyvää seuranta- ja raportointia. Kehittämistoimet voivat liittyä esimerkiksi itse tiedon laatuun tai tietojen käsittelyyn liittyvään prosessiin. Kehittämistoimet voivat liittyä myös uuden teknologian menestykselliseen käyttöönottoon ja muutenkin valmiuteen ottaa käyttöön uusia tietotyön välineitä.

Opas on päivitetty huhtikuussa 2012, eikä sen tietosuojasetuksen mukaisuutta ole arvioitu.

Valtionhallinnon organisaation osalta tietotilinpäätökseen voidaan myös sisällyttää tietoja siitä, miten organisaatio on huolehtinut valtioneuvoston asetuksessa (681/2010) säädetyistä vaatimuksista tietoturvallisuuden tason osalta.

Tietotilinpäätöksen perusteella tehdään johtopäätöksiä, esimerkiksi:

- toiminta ja tietojen käsittely on ollut hyvän tietojenkäsittelytavan ja hyvän tiedonhallintatavan mukaista.
- tietojen käsittelyn seuranta ja valvonta on onnistunut lainsäädännön, määräysten ja sisäisen ohjeistuksen mukaisesti.
- tietojen käsittelyn seurannassa ja valvonnassa on havaittu kehittämiskohteita tai poikkeamia, joiden johdosta on ryhdytty erikseen lueteltuihin toimenpiteisiin

Tietotilinpäätöksessä todetaan esimerkiksi:

- ne tietojen käsittelyn osa-alueet, joissa on kehittämiskohteita.
- määritellään kehittämiskohteet ja arvioidaan mitä ratkaisuja niihin on tarjolla.
- arvioidaan edellisellä seurantakaudella toteutettujen kehittämistoimenpiteiden onnistumista.

Tietotilinpäätöstä koskeva raportointi voidaan kohdistaa organisaation johdolle, työntekijöille, asiakkaille ja muille sidosryhmille tai laillisuusvalvontaa harjoittaville tahoille. Tietotilinpäätös voi olla luonteeltaan dynaaminen asiakirja, jonka sisältö voidaan muokata kohderyhmäkohtaisesti. Esimerkiksi tietojen suojauksesta ja valvonnasta voidaan raportoida johdolle yksityiskohtaisesti, kun taas muille sidosryhmille kohdistetussa tietotilinpäätöksessä voimaan samoja asioita kuvata yhteenvedona tai kokonaisarviona.

Henkilötietolaki ja muut tässä esitteessä mainitut lait löytyvät kokonaisuudessaan valtion säädöstietopankista osoitteesta www.finlex.fi. Yleistä informaatiota tietosuojasta ja henkilötietolaista on saatavilla tietosuojavaltuutetun toimiston verkkosivuilta osoitteesta (www.tietosuoja.fi). Myös valtiovarainministeriön (www.vm.fi) asettama valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) ohjeistusta voi käyttää hyväksi tietotilinpäätöstä valmisteltaessa.

Valtion organisaatioiden osalta voidaan käyttää hyväksi myös valtioneuvoston controllerin antamaan sisäisen valvonnan ja riskienhallinnan arviointia ja arviointikehikkoa koskevia ohjeita. Tietotilinpäätös voidaan yhdistää näiden ohjeiden mukaiseen arviointiin sisäisen valvonnan välineenä (Valtioneuvoston controller: Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta, VM 23.12.2005, www.wm.fi). Valtioneuvoston controllerin suositus on hyödynnettävissä myös yksityisellä sektorilla hyvän riskienhallintatavan ja sen arvioinnin suomalaisena lähteenä, joka perustuu kansainvälisesti yleisesti hyväksytyyn COSO-ERM –malliin ja siitä julkiselle sektorille laadittuun INTOSAI GOV -suositukseen.