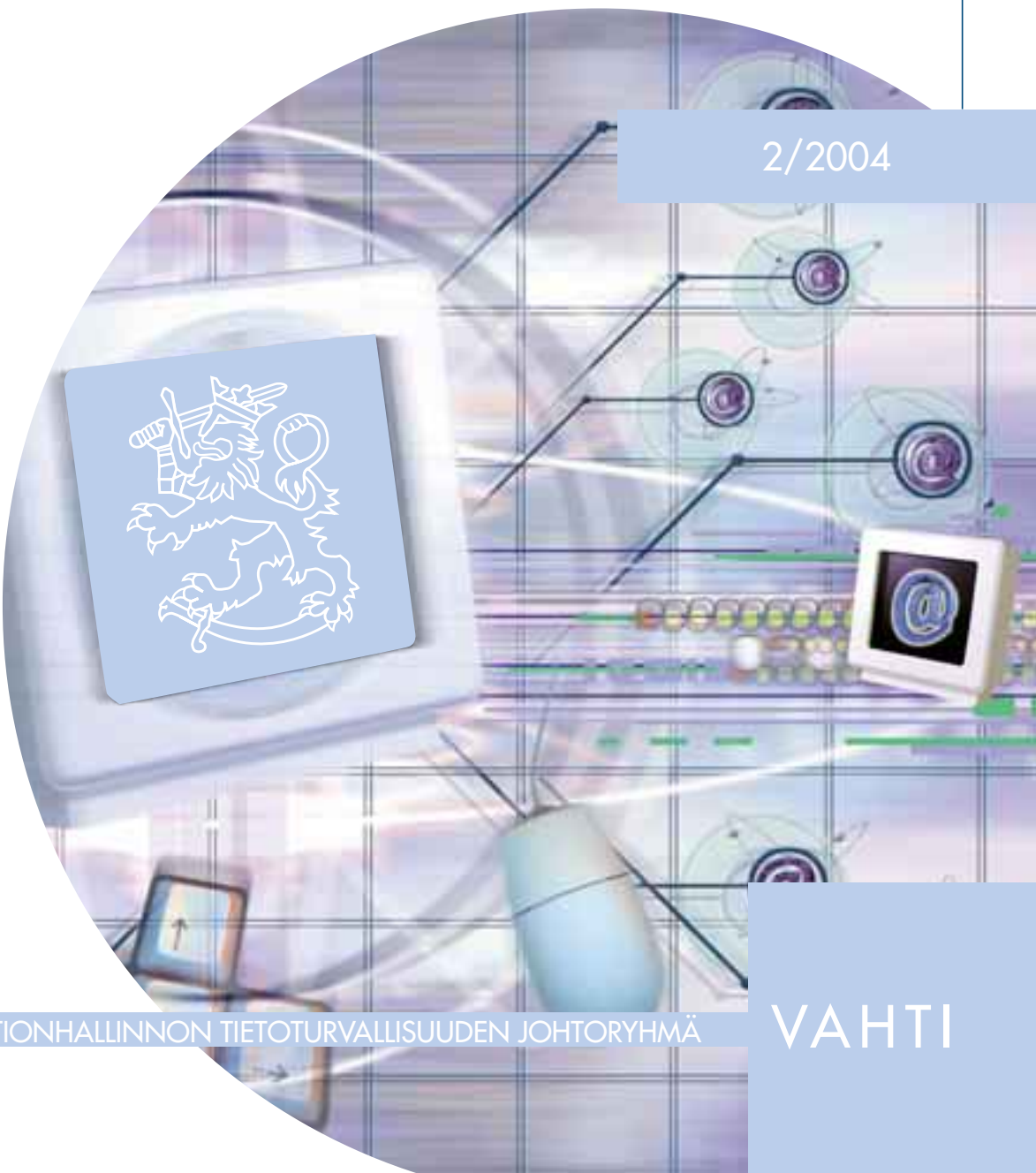
VALTIOVARAINMINISTERIÖ

TIETOTURVALLISUUS JA TULOSOHJAUS



2/2004

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

TIETOTURVALLISUUS JA TULOSOHJAUS

2/2004

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
vahtijulkaisut@vm.fi

ISSN 1455-2566
ISBN 951-804-432-5

Edita Prima Oy
HELSINKI 2004

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 11/01/2004

SUOSITUS
20.4.2004

Ministeriöille, virastoille ja laitoksille

TIETOTURVALLISUUS JA TULOSOHJAUS

Valtiovarainministeriö antaa oheisen tietoturvasuosituksen (jäljempänä suositus), joka on laadittu valtiovarainministeriön asettaman ja johtaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta. Suositus täydentää laajaa olemassa olevaa valtiovarainministeriön antamaa tietoturvaohjeistoa ja korvaa aiemman VM:n tietoturvasuosituksen "Tietoturvallisuuden tulosohjaus ja kehittämisvälineet" (VM:n VAHTI-julkaisu 2/1997).

Tietoturvallisuus edistää hallinnon palveluiden laatua, tehokkuutta sekä tuottavuutta. Tietoturvallisuuden riittävä taso on välttämätön edellytys organisaation toiminnan jatkuvuudelle ja toimintakyvyn varmistamiselle. Tietoturvallisuuden tulosohjauksen kehittämisellä on korkea prioriteetti valtion tietoturvallisuuden kokonaiskehittämisessä, jota on kuvattu muun muassa valtionhallinnon tietoturvallisuuden kehitysohjelmassa (VM:n VAHTI-julkaisu 1/2004).

Suosituksessa on esitetty tiiviissä muodossa tietoturvallisuuden kehittämisen keskeiset periaatteet sekä niiden yhteys tulosohjaukseen, virastojen johtamiseen ja toiminnan arviointiin. Tietoturvallisuus on tärkeä osa normaalia palvelujen ja toiminnan kehittämistä, joten sen tulee olla mukana myös tulosohjauksessa. Keskeistä on tietoturvallisuuden sitominen tulossopimuksissa ja –ohjauksessa organisaatioiden toiminnallisiin tavoitteisiin.

Suositus tulee Valtionhallinnon tietoturvallisuuden johtoryhmän Internet-sivuille, jotka ovat osoitteissa *www.vm.fi/vahti ja www.vm.fi/tietoturvallisuus*. Suositusta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi).

Lisätietoja antavat neuvottelevat virkamiehet Mikael Kiviniemi ja Matti Salminen (etunimi.sukunimi@vm.fi)

Ministeri Ulla-Maj Wideroos

Ylijohtaja Jorma Karjalainen

Liite Tietoturvallisuus ja tulosohjaus (VAHTI 2/2004)

TIETOTURVALLISUUS JA TULOSOHJAUS

Tiivistelmä

Tietoturvallisuuden riittävä taso on välttämätön edellytys toiminnan jatkuvuudelle ja uskottavuudelle. Tietoturvallisuus lisää virastojen ja laitosten palvelukykyä sekä parantaa toiminnan tehokkuutta ja laatua. Tietoturvallisuuden merkitys organisaation johtamisessa ja toimintakyvyn varmistamisessa sekä häiriöttömän ja tuloksellisen toiminnan ylläpitämisessä on jatkuvasti korostunut. Suosituksessa on esitetty tiiviissä muodossa tietoturvallisuuden kehittämisen keskeiset periaatteet ja niiden yhteys tulosohjaukseen ja virastojen johtamiseen sekä toiminnan arviointiin. Suosituksessa tietoturvallisuutta ja tietohallintoa tarkastellaan osana virastojen ja laitosten johtamista, palvelujen tuottamista ja laadunhallintaa.

Tietoturvallisuuden avulla taataan organisaatiossa käsiteltävän tiedon eheys, käytettävyys ja luottamuksellisuus. Tietoturvallisuus on käsitteenä laaja. Sen eri osa-alueet, kuten hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus, muodostavat kattavasti dokumentoituna ja hyvin johdettuna vahvan perustan organisaation toiminnan jatkuvuudelle ja luotettavuudelle sekä tehokkuudelle ja tuloksellisuudelle.

Tietoturvallisuus ja sen jatkuva parantaminen ei ole itseisarvoista toimintaa, mutta turvallisuudella on keskeinen merkitys esimerkiksi luotettavien sähköisten palvelujen tarjoamisessa. Kansalaisten ja palvelujen käyttäjien näkökulmasta tarkasteltuna hallinnon tehtävänä on tuottaa sellaisia sähköisiä palveluja, joiden turvallisuuteen asiakas voi luottaa, ja joita tuotettaessa otetaan huomioon kansalaisten perusoikeudet.

Suosituksessa tietoturvallisuutta käsitellään seuraavan jaottelun mukaisesti:

- määritellään tietoturvallisuus kokonaisuutena
- esitetään turvallisuuteen liittyvät yleiset periaatteet käyttäen perustana OECD:n aiheesta laatimaa suositusta
- tarkastellaan taustatekijänä kansallisen tietoturvastrategian linjauksia
- sijoitetaan tietoturvallisuus ministeriön ja viraston väliseen tulosohjauskehykseen

- kuvataan tietoturvallisuuden käsittely viraston sisäisenä ohjausprosessina sisältäen politiikan ja ohjeistuksen sekä seurannan ja arvioinnin.

Suosituksen liitteet sisältävät esimerkin tietoturva-asioiden käsittelystä tasapainoiseen tuloskorttiin (BSC) perustuvassa ohjausmallissa (Liite 1) sekä laatujärjestelmään perustuvassa arvioinnissa (Liite 2).

Tietoturvallisuus ja tulosohjaus -suosituksen keskeinen sisältö on tiivistetty seuraavaan kahdeksaan kohtaan:

Suositus 1. Tietoturvallisuus on osa hallinnon tulosohjausta, jossa viraston tai laitoksen toimintaa tarkastellaan kokonaisuutena ja tulostavoitteiden asettamisessa käytetään useita eri näkökulmia (vaikuttavuus, tehokkuus, laatu ja henkiset voimavarat). Tulosohjauksella pyritään osaltaan vahvistamaan hyvää hallintotapaa.

Suositus 2. Tietoturvallisuus on laaja toiminnallinen kokonaisuus, jonka perustana ovat organisaation turvallisuuskulttuuri ja ihmisten toiminta.

Suositus 3. Valtionhallinnossa noudatetaan OECD:n suosittamia turvallisuuskulttuurin periaatteita.

Suositus 4. Kansallinen tietoturvastrategia luo yhteistä perustaa tietoturvallisuuden laaja-alaiselle kehittämistyölle.

Suositus 5. Tietoturvallisuus on osa normaalia toiminnan kehittämistä, riskienhallintaa ja tulosohjausta, jossa voidaan hyödyntää sekä laadullisia että määrällisiä tietoja ja niihin perustuvia mittareita.

Suositus 6. Tietoturvallisuuden parantamisessa virastojen ja laitosten on ensisijaisesti turvattava keskeiset päätehtävänsä ja määriteltävä koko toimintaa ohjaava tietoturvapolitiikka. Tietoturvallisuudesta vastaavat osaltaan kaikki organisaatiossa työskentelevät.

Suositus 7. Tietoturvallisuus on osa julkisten palvelujen kehittämistä, jossa keskeistä on palvelujen käytettävyys, kansalaisten perusoikeudet ja hyvä tiedonhallintatapa.

Suositus 8. Johdon tehtävänä on käynnistää sisäisiä ja ulkoisia arviointeja, vahvistaa arviointiosaamista sekä huolehtia siitä, että arviointitulokset käsitellään asianmukaisella tavalla osana johtamista ja tulosohjausta.

SISÄLLYS

1 JOHDANTO

Organisaation tietoturvallisuuteen vaikuttavat monet yhteiskunnan muutostekijät:

- tietotekniikan merkitys kasvaa jatkuvasti organisaatioiden toiminnassa ja sen ylläpidossa sekä ihmisten arkielämässä
- tietotekniikka monimutkaistuu ja sen käyttö laajenee jatkuvasti yhteiskunnan eri toimialoille
- tietoturvauhkien samanaikainen yleistyminen
- kansalaisten tietoisuus tietotekniikan merkityksestä ja taidot sen hyödyntämisessä ovat merkittävästi lisääntyneet.

Tietoturvallisuus on keskeinen osa organisaatioturvallisuutta. Käsitteenä se ei rajaudu vain teknisiin ratkaisuihin, vaan siihen kuuluvat myös palvelujen kehittäminen ja tietotekniikan käyttäjien asenteet, tiedot ja taidot. Tämän suosituksen tarkoituksena on esittää selkeä tietoturva-asioiden käsittelymalli työvälineineen, jonka avulla keskeisiä tietoturvakysymyksiä voidaan tarkastella osana toiminnan johtamista ja tulosohjausta. Suositus on suunnattu virastojen ja laitosten johdolle. Tietoturvallisuuden kokonaisuutta tarkastellaan ministeriöiden sekä virastojen ja laitostason välisen tulosohjauksen näkökulmasta ja myös organisaation sisäisenä toimintaprosessina.

Tietoturvallisuuden merkitys on yhä keskeisempi organisaation toimintakyvyn ylläpitämisessä ja varmistamisessa. Turvallisuudessa ilmenevät puutteet vaikuttavat koko organisaation toimintaedellytyksiin. Toiminnan häiriintyminen tai suoranainen lamaantuminen, tietovuodot ja erilaiset muut häiriötekijät vievät organisaatiolta uskottavuutta ja johtavat vakaviin ongelmiin, jotka estävät tuloksellisen toiminnan. Tietoturvallisuuden puutteet verkottuneessa yhteiskunnassa johtavat helposti myös organisaation asiakkaiden ja yhteistyöorganisaatioiden toiminnan vaarantumiseen. Kansalaisten luottamus hallintoon saattaa kärsiä toistuvien tietoturvaongelmien myötä. Ongelmat voivat johtaa myös juridisiin vastuisiin, koska organisaatiot ovat yhä enemmän vastuussa myös sidosryhmiensä tietoturvallisuudesta.

Suositus on laadittu valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimeksiannosta ja ohjauksessa. Sen valmistelussa on kuultu virastojen ja laitosten näkemyksiä. Tehtävään nimetyn työryhmän kokoonpano on ollut seuraava:

Puheenjohtaja:	Ari Uusikartano, Kauppa- ja teollisuusministeriö
Jäsenet:	Reijo Aarnio, Tietosuojavaltuutettu
	Kalervo Jakonen, Tullihallitus
	Lea Krohns, Väestörekisterikeskus
	Markku Mattila, Opetusministeriö
	Matti Salminen, Valtiovarainministeriö, sihteeri
	Kristel Sarlin, Teknillinen korkeakoulu

VAHTI päätti suosituksen julkaisemisesta kokouksessaan maaliskuussa 2004.

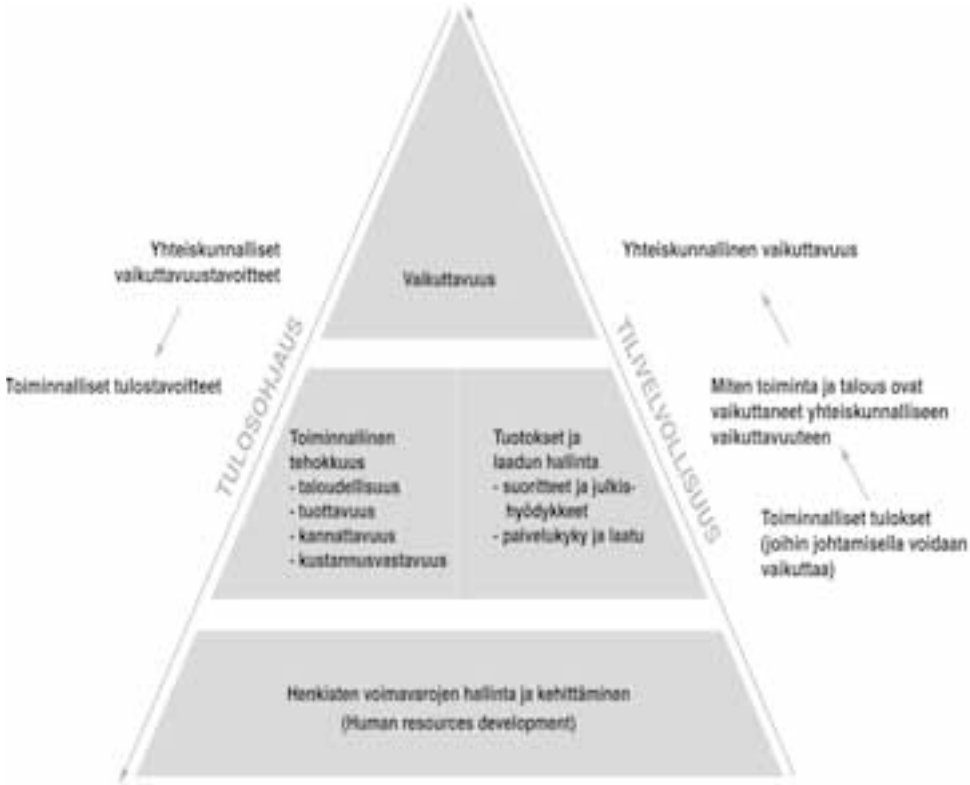
2 TULOSOHJAUKSEN TERÄVÖITTÄMINEN

Suositus 1. Tietoturvallisuus on osa hallinnon tulosohjausta, jossa viraston tai laitoksen toimintaa tarkastellaan kokonaisuutena ja tulostavoitteiden asettamisessa käytetään useita eri näkökulmia (vaikuttavuus, tehokkuus, laatu ja henkiset voimavarat). Tulosohjauksella pyritään osaltaan vahvistamaan hyvää hallintotapaa.

Hallitus on eduskunnalle 16.9.2003 annetussa hallituksen esityksessä (HE 56/2003) laiksi valtion talousarviosta annetun lain muuttamisesta sitoutunut laaja-alaiseen kehittämisohjelmaan tulosohjauksen ja tilivelvollisuuden terävöittämiseksi. Laki (1216/2003) valtion talousarviolain muuttamisesta on tullut voimaan 1.1.2004. Talousarviolain säännöksiä tarkentava asetus valtion talousarviosta annetun asetuksen (1243/1992) muuttamisesta on hyväksytty valtioneuvostossa 7.4.2004 ja asetus tuli voimaan 15.4.2004. Lainsäädännön tarkoituksena on merkittävällä tavalla terävöittää hallinnon tulosohjausta ja tilivelvollisuutta. Parempi tulosohjaus ja tilivelvollisuus edellyttävät käytännössä mm. valtion tilinpäätösraportoinnin uudistamista sekä tilivelvollisuuden toteuttamiseen liittyvien menettelyjen samoin kuin laskentatoimen ja johtamisen kehittämistä.

Uudistetussa valtion talousarviolaissa tuloksellisuuden peruskriteerit on määritelty uudelleen. Tulosohjauksessa ja raportoinnissa on erotettu selkeästi laaja-alainen *yhteiskunnallinen vaikuttavuus ja toiminnallinen tuloksellisuus*, johon viraston tai laitoksen johtamisella voidaan välittömästi vaikuttaa. Toiminnan tuloksellisuus muodostuu siten

- yhteiskunnallisesta vaikuttavuudesta
- toiminnan tehokkuudesta
- tuotoksista ja laadunhallinnasta sekä
- henkisten voimavarojen hallinnasta.



Kuva 1. Tuloksellisuuden peruskriteerit.

Näitä tuloksellisuuden peruskriteereitä on havainnollistettu kuvassa 1.

Ministeriöiden vastuu hallinnonalojensa ja politiikkasektoreidensa ohjaajina ja tulosvastuun toteuttajina korostuu. Ministeriöiden on arvioitava alaistensa tilinpäätösvelvollisten yksiköiden tilinpäätökset ja tilintarkastuskertomukset ja annettava niistä perusteltu julkinen kannanotto. Tilinpäätöskannanotossa on otettava kantaa siihen, antaako tilinpäätös oikean ja riittävän kuvan taloudesta ja toiminnan tuloksellisuudesta, onko tulostavoitteet saavutettu ja mihin toimenpiteisiin tulosvastuullisissa virastoissa ja laitoksissa ja ministeriössä on tilinpäätöksen ja siitä annettujen tilintarkastuskertomusten ja muiden arviointien perusteella aihetta ryhtyä.

Johdon vastuuta sisäisestä valvonnasta ja *riskienhallinnasta* vahvistetaan kaikilla hallinnon tasoilla. Virastojen ja laitosten johdon on tilinpäätöksen yhteydessä annettava vahvistus- ja arviointilausuma siitä, onko sisäinen valvonta talousarviolaissa ja -asetuksessa tarkoitetulla tavalla riittävää ja asianmukaista ja mitä olennaisia kehittämistarpeita siinä on. Johdon valvonta- ja kehittämisvastuu kattaa luonnollisesti myös tietohallinnon ja tietoturvallisuuden. Tiliviraston taloussäännössä annetaan mm.

tarkemmat määräykset tiliviraston taloushallinnon ja siihen liittyvien järjestelmien tietoturvallisuudesta.

Tulosohjauksen lähtökohtana on, että viraston tai laitoksen tulostavoitteissa painottuvat toiminnan taloudellisuutta ja tuottavuutta sekä laatua ja palvelukykyä ja muita välittömiä vaikutuksia koskevat asiat. Myös yhteiskunnalliset vaikuttavuustavoitteet ohjaavat virastojen tulostavoitteiden asettamista. Valtioneuvoston tasolla voidaan tehdä valintoja laajoista toimenpidekokonaisuuksista ja vaikuttaa näin koko yhteiskunnan sosiaaliseen ja taloudelliseen kehitykseen. Tällaisista laajoista vaikutusketjuista on myös määriteltävissä erillisiä tietoturvallisuuteen vaikuttavia tekijöitä, jotka selvästi kytkeytyvät tietyn viraston tai laitoksen palveluihin tai tuotoksiin. Tulostavoitteilla on mahdollisimman tiivis yhteys varsinaiseen toimintaan, jolloin tulosten aikaansaaminen riippuu viraston tai laitoksen omasta toiminnasta ja sen johtamisesta.

3 TIETOTURVALLISUUDEN PERUSTAN MÄÄRITTELYÄ

3.1 Tietoturvallisuus kokonaisuutena

Suositus 2. Tietoturvallisuus on laaja toiminnallinen kokonaisuus, jonka perustana ovat organisaation turvallisuuskulttuuri ja ihmisten toiminta.

Tietoturvallisuus on käsitteenä laaja kokonaisuus, josta on esitetty lukuisia määrittelyjä riippuen kulloinkin tarkasteltavasta turvallisuuden osa-alueesta. Tietoturvallisuus ei käsitteenä koske vain teknisiä ratkaisuja, kuten ohjelmia ja laitteita, vaan siihen kuuluvat keskeisimmät turvallisuustekijät liittyvät *ihmisten toimintaan* ja turvatoiminnan yleisiin järjestelyihin. Tietoturvallisuuden vaikutukset ulottuvat koko organisaation toimintaan, kuten palvelujen laatuun, tuottavuuteen ja taloudellisuuteen.

Tietoturvallisuuden osa-alueiden tarkastelussa käytetään yleisesti seuraavaa jaottelua, jossa on kuvattu myös niiden keskeistä sisältöä:

- *hallinnollinen tietoturvallisuus* (johtamisen, tietoturvatoiminnan järjestelyjen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostama kokonaisuus)
- *henkilöstöturvallisuus* (henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisuusjärjestelyihin, henkilöstön suojaamiseen ja palvelussuhteeseen liittyvät turvallisuustekijät)
- *fyysinen turvallisuus* (tietotekniikan vaatiman fyysisen käyttöympäristön suojaus ja esim. toimitilajärjestelyt)
- *tietoliikenneturvallisuus* (tiedonsiirtoyhteyksien käytettävyyteen, tiedonsiirron suojaamiseen ja salaamiseen, käyttäjän tunnistamiseen ja verkon varmistamiseen liittyvät tekijät)
- *laitteistoturvallisuus* (laitteistojen käytettävyyteen, toimintaan, ylläpitoon sekä laitteiden ja tarvikkeiden saatavuuteen liittyvät tekijät)

- *ohjelmistoturvallisuus* (ohjelmistojen suojausominaisuuksiin, valvonta- ja lokimenettelyihin sekä ylläpitoon ja päivityksiin liittyvät seikat)
- *tietoaineistoturvallisuus* (tiedon ja tietoaineiston käytettävyys, oikeellisuus, salassa pitäminen, turvallinen käsittely sekä tietojätteen hävittäminen)
- *käyttöturvallisuus* (tietotekniikan turvallisen käytön vaatimat toiminta-olosuhteet, kuten valvonta, käyttöoikeudet, tuki- ja huoltopalvelut sekä häiriökäsittely).

Organisaation toiminnassa tietoja pyritään turvaamaan, koska tiedot ja niihin liittyvät järjestelmät ovat organisaation toiminnan ja toimintakyvyn säilymisen olennainen osa. Tiedonkäsittelyä turvataan, jotta voitaisiin välttyä tahallisilta ja tahattomilta uhkatekijöiltä, jotka saattavat uhata tiedon eheyttä, käytettävyyttä tai luottamuksellisuutta. Uhkakuvissa tietovarantojen käyttö voi keskeytyä, estyä tai varannot voivat tuhoutua. Tietoa voidaan varastaa tai sen sisältöä muuttaa eri tavoin käsittelemällä. Tätä ehkäisemään tietoturvallisuuden perustana täytyy olla organisaation omaan toimintakulttuuriin tukeutuva *turvallisuuskulttuuri*, jonka ytimessä ovat tietojärjestelmiä ja tietoja käsittelevät ihmiset.

3.2 Turvallisuuskulttuurin periaatteet

Suositus 3. Valtionhallinnossa noudatetaan OECD:n suosittamia turvallisuuskulttuurin periaatteita.

Taloudellisen yhteistyön ja kehityksen järjestö OECD julkisti suosituksensa tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteiksi vuonna 2002. Paitsi suoranaisesti järjestelmäteknisinä linjauksina suositusten voidaan katsoa kattavan koko tiedonkäsittelyn kentän. Julkaisussa listataan yhdeksän periaatetta, joiden varaan organisaatioissa tarvittavan uuden turvallisuuskulttuurin tulisi kehittyä. Seuraavassa on lyhyesti esitetty nämä periaatteet (ks. Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet, turvallisuuskulttuurin kehittäminen. OECD:n suositus. Suomenkielinen käännös. Valtiovarainministeriö 2002).

Periaatteista ensimmäinen on *turvallisuustietoisuus*. Yhteiskunnan eri tahojen on oltava tietoisia tietoturvallisuuden tarpeesta ja siitä, mitä kukin voi omassa toimintaympäristössään tehdä turvallisuuden edistämiseksi.

Seuraavana periaatteena on *vastuullisuus*. Kaikki yhteiskuntatahot ovat osaltaan vastuussa tietoturvallisuudesta. Tämä edellyttää tietoisuuden lisäämistä valistamalla, tiedottamalla ja kouluttamalla.

Vastatoimien merkitys korostuu tietoturvauhkien kohdatessa verkottuneita organisaatioita yhä nopeammalla aikataululla. Kaikkien tahojen on toimittava viipymättä ja yhteistyöhenkisesti ehkäistäkseen ja havaitakseen turvallisuuden loukkaukset ja vastatakseen niihin.

Seuraavina periaatteina suosituslistassa ovat *eettisyys* ja *demokratia*. Koska tietojärjestelmät ja verkot ulottuvat kaikkialle yhteiskunnassa, jokaisen toimijan on ymmärrettävä oma vastuunsa, toimittava eettisesti ja kunnioitettava toistensa oikeutettuja etuja. Tietoturvauhkien torjuntaa ja tietoturvallisuutta on toteutettava tavalla, joka vastaa demokraattisen kansalaisyhteiskunnan hyväksymiä arvoja ja periaatteita. Näitä ovat mm. ajatusten ja ideoiden vaihdon vapaus, tiedon vapaa kulku, tietojen ja viestien luottamuksellisuus, henkilötietojen asianmukainen suojaus sekä avoimuus.

Riskien arvioinnissa niin yritysten kuin julkishallinnon yhteisöjenkin on kyettävä suorittamaan sisäinen arviointi oman toimintansa haavoittuvuuksista ja uhista. Riskien arviointi mahdollistaa hyväksyttävän riskitason määrittelyn ja sen avulla voidaan valita sopivat riskien hallintakeinot ja siirtyä analyysin perusteella *turvallisuuden suunnitteluun ja toimeenpanoon* sisällyttäen turvallisuus toimintojen olennaiseksi osaksi.

Turvallisuuden hallinnan tulee perustua edellä käsiteltyyn tapaan riskien arviointiin ja ennakointiin. Organisaation tietoturvapolitiikan, -toimien ja -menettelyjen tulee olla siten yhteen sovitettuja ja yhdenmukaisia, että ne muodostavat yhtenäisen turvallisuusjärjestelmän.

Viimeisenä periaatteena listataan *uudelleenarviointi*. Tietoturvallisuuden tasoa ja myös uusia uhkia on jatkuvasti arvioitava uudelleen, jotta tietoturvallisuuden ja käytännön menettelyjen ajantasaisuus voidaan taata.

3.3 Kansallinen tietoturvastrategia

Suositus 4. Kansallinen tietoturvastrategia luo yhteistä perustaa tietoturvallisuuden laaja-alaiselle kehittämistyölle.

Valtioneuvosto teki 4.9.2003 periaatepäätöksen kansallisesta tietoturvastrategiasta. Sen mukaan kansalaisten ja yritysten luottamusta tietoyhteiskuntaan voidaan lisätä parantamalla erityisesti tietoturvallisuutta ja yksityisyyden suojaa. Strategian avulla Suomesta pyritään rakentamaan tietoturvallinen yhteiskunta. Sen tavoitteena on

- edistää kansallista ja kansainvälistä tietoturvallisuustyötä
- edistää kansallista kilpailukykyä ja suomalaisten tieto- ja viestintäalan yritysten toimintamahdollisuuksia

- parantaa tietoturvallisuusriskien hallintaa
- turvata perusoikeuksien toteutuminen ja kansallinen tietopääoma sekä
- lisätä turvallisuustietoisuutta ja osaamista.

Näihin tavoitteisiin sisältyvät myös ne käytännön toimenpiteet, joilla yksittäisen organisaation tietoturvallisuuden perustaa voidaan vahvistaa. Strategia pyrkii siis osaltaan rakentamaan organisaatioille parempaa toimintaympäristöä ja toimii myös hallituksen tietoyhteiskuntaohjelman keskeisenä osana.

Valtionhallinnon tietoturvallisuuden lisäämisessä perustana on ollut jo ennen kansallista tietoturvastrategiaa annettu valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta 11.11.1999. Periaatepäätöksen tarkoituksena on parantaa organisaatioiden toimintojen ja tiedonkäsittelyn tietoturvallisuuden sekä henkilötietojen tietosuojan tasoa. Lisäksi päätös täsmentää tietoturvallisuuden työnjakoa ja vastuita sekä yksilöi keskeisiä viranomaisten tehtäviä.

4 TIETOTURVALLISUUDEN KÄSITTELY TULOSOHJAUKSESSA

4.1 Tietoturva-asiat osana tulosohjausprosessia

Suositus 5. Tietoturvallisuus on osa normaalia toiminnan kehittämistä, riskienhallintaa ja tulosohjausta, jossa voidaan hyödyntää sekä laadullisia että määrällisiä tietoja ja niihin perustuvia mittareita.

Tulosohjauksessa tietoturva-asiat nousevat yleensä esille erilaisten kehittämisohjelmien ja yksittäisen hankkeiden yhteydessä. Näissä tapauksissa se helpommin huomioidaan myös investointina budjetoinnissa. Tietoturvallisuus on kuitenkin toimintaa läpileikkaava ja siihen keskeisesti vaikuttava kokonaisuus muutenkin kuin erityistapauksissa. Johdon on oltava perillä organisaation toiminnan tavoitteista ja nähtävä organisaation perustehtäviin liittyvät riskit turvallisuuden eri osa-alueilla. Tämä on olennainen osa valtion talousarviolain 24 b §:n tarkoittamaa sisäisen valvonnan järjestämistä, jonka asianmukaisuudesta ja riittävyydestä vastaa viraston ja laitoksen johto.

Tietoturvariskit korostuvat erityisesti toiminnan muutostilanteissa, joita voivat olla esimerkiksi ostopalvelujen hankinta, toimintojen ulkoistaminen tai erilaiset organisaatio- ja toimitilajärjestelyt. Viraston toimintaympäristössä tai palvelutuotannossa tapahtuvien muutosten vaikutukset on siten tarpeen arvioida myös tietoturvanäkökulmasta. Johdon tehtävänä on arvioida erilaisten riskianalyysien avulla, mitä vaikutuksia organisaation toimintaan ja palveluihin tietoturvallisuuden puutteellisella hoidolla saattaa olla.

Kun viraston tai laitoksen toimintatapoja ja -kulttuuria halutaan tietoturvallisuuden osalta muuttaa, on hyödyllistä tarkastella myös budjetointia, joka on keskeinen osa tulosohjausta. On asetettava kysymys, kuinka keskeisesti tietoturvallisuuden osalta tehdyt valinnat ja linjaukset näkyvät budjetoinnissa ja toiminnassa voimavarojen kohdentamispäätöksinä.

Tulosohjauksessa viraston tai laitoksen asemaa tarkastellaan kokonaisuutena ja tulostavoitteiden asettamisessa käytetään useita eri näkökulmia (esim. resursointi-, asiakas-, prosessi- ja osaamisnäkökulmat; ks. liite 1). Tietoturvallisuuden tulosohjauksessa voidaan hyödyntää sekä laadullisia että määrällisiä tietoja esimerkiksi seuraavien kysymysten avulla:

- Kehitetäänkö tietoturvallisuutta osana viraston toimintaa ja palvelustrategiaa?
- Miten tietoturvariskit on tunnistettu asiakkaiden ja toimintaprosessien näkökulmasta?
- Miten lainsäädännön edellyttämät vaatimukset tietoturvallisuuden osalta on toteutettu?
- Kuinka viraston tietojenkäsittelyn tärkeysluokka on huomioitu tietoturvallisuutta kehitettäessä? Onko viraston tietojärjestelmät luokiteltu?
- Raportoidaanko tietoturvaan liittyvät häiriötilanteet? Kenelle raportoidaan? Onko virastossa tehty toiminnan riskikartoitus?
- Miten tietoturvallisuuden kehittämistoimenpiteiden vaikutuksia valvotaan ja arvioidaan? Onko virastolla käytössä mittaristo?
- Miten huolehditaan henkilöstön tietoturvaosaamisen ylläpidosta?

4.2 Tietoturva-asiat organisaation sisäisessä ohjauksessa

Suositus 6. Tietoturvallisuuden parantamisessa virastojen ja laitosten on ensisijaisesti turvattava keskeiset päätehtävänsä ja määriteltävä koko toimintaa ohjaava tietoturvapolitiikka. Tietoturvallisuudesta vastaavat osaltaan kaikki organisaatiossa työskentelevät.

Tullakseen luontevaksi osaksi organisaation toimintaa turvallisuusasioiden on oltava kiinteä osa organisaation toimintakulttuuria. Viraston tulee luonnollisesti mieltää omat *keskeiset tehtävänsä* ja ryhtyä toimenpiteisiin *ensisijaisesti niiden turvaamiseksi*. Tulosneuvotteluissa sovittuja asioita tarkastellaan myös tietoturvanäkökulmasta ja niiden vastuut otetaan huomioon organisaation sisäisessä työnjaossa. Panostamista tietoturvallisuuteen on tarkasteltava myös budjetoinnin ja sen seurannan näkökulmasta. Tietoturvallisuuden keskeisyys ja sen optimaalinen toteutustaso riippuu luonnollisesti organisaation tehtävistä ja käsiteltävän tiedon luonteesta. Jokaisen viraston ja laitoksen on tunnistettava ja määriteltävä *tietoturvallisuutensa tavoitetaso* ja myös pyrittävä siihen.

Tietoturvallisuuteen liittyvät asiat ovat automaattisen tietojenkäsittelyn jatkuvan lisääntymisen myötä korostuneet osana turvajärjestelyjen kehittämistä. Organisaation

turvallisuusjärjestelyjä kehitettäessä turvallisuusuhkien tunnistaminen ja huomioon ottaminen on organisaation eri toimijoille ennen kaikkea *oppimisprosessi*. Kun asioiden sisäistäminen on tapahtunut, ne tulevat osaksi toimintaa.

Lähdettäessä kuvaamaan tietoturvallisuusasioiden läpivientiä organisaation toiminnassa nousee keskeiseen asemaan *tietoturvapolitiikka*. Siinä johto linjaa lyhyesti ne keskeiset tavoitteet, joihin tietoturvatoiminnalla pyritään. Politiikka sisältää myös vastuutuksen organisaation eri tasoilla turvallisuusasioiden hoidosta. Tietoturvallisuus ei ole yksin johdon tai teknisen henkilöstön asia, vaan siitä vastaavat eri tasoilla kaikki organisaatiossa työskentelevät.

Tietoturvapolitiikka toimii perustana, jonka varaan erilaiset *turvallisuussuunnitelmat ja -ohjeistukset* rakentuvat. Turvallisuusasiat on luontevaa sisällyttää myös osaksi organisaation laatujärjestelmää, jolloin turvallisuuden parantamista voidaan tarkastella osana laajempaa kokonaisuutta. Tietoturvakysymyksillä on siten selkeä yhteys organisaation toimintakykyyn, palvelujen kehittämiseen ja laadunhallintaan. Tietoturva-asioiden käsittelyä osana organisaation laatujärjestelmää on kuvattu liitteessä (ks. liite 2).

4.3 Tietoturvallisuus osana julkisten palvelujen kehittämistä

Suositus 7. Tietoturvallisuus on osa julkisten palvelujen kehittämistä, jossa keskeistä on palvelujen käytettävyys, kansalaisten perusoikeudet ja hyvä tiedonhallintatapa.

Julkisten palvelujen siirtyessä yhä enemmän tietoverkkoihin korostuu tietoturvallisuuden merkitys jokaiselle palvelun käyttäjälle ja virkamiehelle, kansalaiselle ja yritykselle. Viranomaisen tuottamien palvelujen näkökulmasta tietoturvallisuuden perustekijöiden on oltava kunnossa ja mietittynä, koska ne muodostavat keskeisen perustan, jolle *palvelujen käytettävyyttä* rakennetaan. Turvallisuuteen liittyy olennaisena osana myös käytettävyys, jolloin palveluja suunniteltaessa on selvitettävä mm. asiakkaiden valmiudet hyödyntää uusia palvelutuotteita. Tietoturvan kehittäminen on samalla osa palvelujen ylläpitoa ja uudistamista.

Vuoden 2004 alusta voimaan tullut uusi *hallintolaki* (434/2003) säätää hyvän hallinnon perusteista. Hallintolaki velvoittaa viranomaisia entistä parempaan asiakaspalveluun ja hallintomenettelyyn. Samoin laissa sähköisestä asioinnista viranomaistoiminnassa (13/2003) on säädetty viranomaisten ja asiakkaiden oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa. Lain tarkoituksena on lisätä asioinnin sujuvuutta ja joutuisuutta samoin kuin tietoturvallisuutta hallinnossa ja tuomioistuimissa sekä edistää sähköisten tiedonsiirtomenetelmien käyttöä. Kansalaisten ja palvelujen

käyttäjien näkökulmasta hallinnon tehtävänä on tuottaa sellaisia sähköisiä palveluja, joiden turvallisuuteen asiakas voi luottaa ja jotka ottavat huomioon *kansalaisten perusoikeudet.*

Julkisuuslain 18 §:n mukaan viranomaisen tulee *hyvän tiedonhallintatavan* luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä. Julkisten verkkopalvelujen laadun parantamiseksi on useissa maissa (esim. Alankomaat, Tanska, Norja, Iso-Britannia, Kanada ja Suomi) luotu ohjeita ja arviointikriteeristöjä, joiden avulla voidaan arvioida verkkopalvelujen laatua erityisesti niiden käyttäjien näkökulmasta.

Suomessa *julkisten verkkopalvelujen laatukriteeristö* otetaan käyttöön vuoden 2004 aikana. Siinä on otettu huomioon myös tietoturvallisuutta koskevat seikat. Erityisesti tietoturvallisuuden mittaamiseen kehitetyistä kriteeristöistä on löydettävissä esimerkkejä myös Internetistä (ks. esim. National Institute of Standards and Technologyn (NIST) mittaristojulkaisu: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf).

4.4 Riskienhallinta ja tietoturvallisuuden arviointi

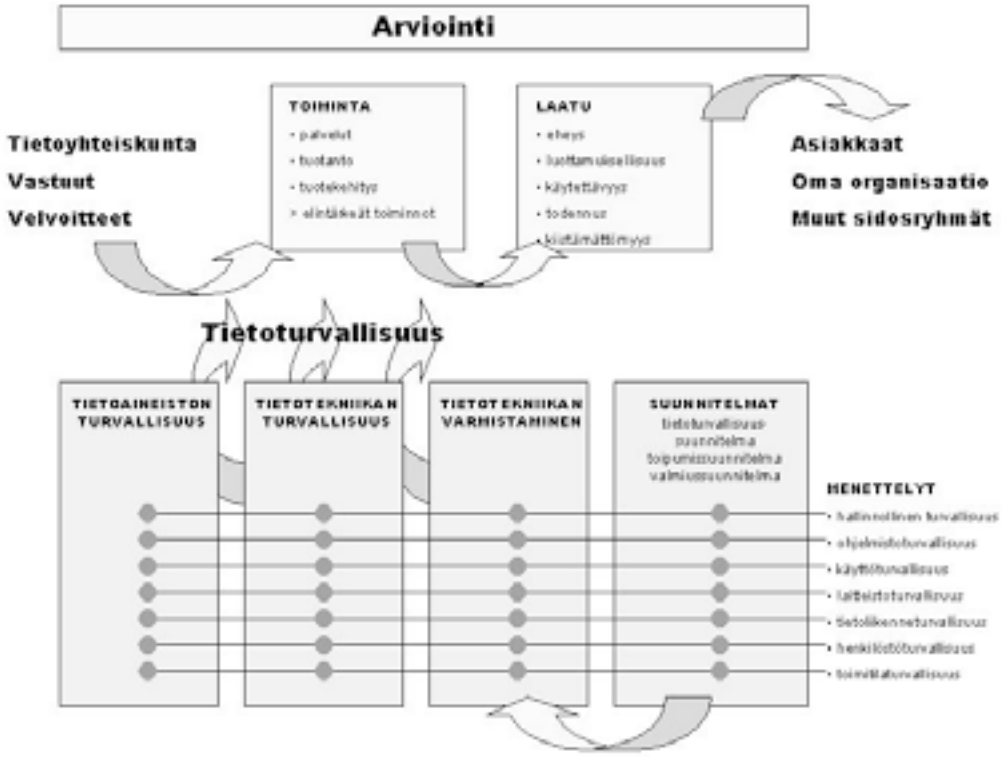
Suositus 8. Johdon tehtävänä on käynnistää sisäisiä ja ulkoisia arviointeja, vahvistaa arviointiosaamista sekä huolehtia siitä, että arviointitulokset käsitellään asianmukaisella tavalla osana johtamista ja tulosohjausta.

Tietotekniikan ulottuessa yhä syvemmin toimintaan ja palveluihin, huoli tietojärjestelmien turvallisuudesta kasvaa. Tietoteknisiä toimintoja ulkoistetaan, uusia tietojärjestelmiä ja niihin pohjautuvia palveluja rakennetaan ja teknisesti tarkasteltuna järjestelmät monimutkaistuvat. Nämä seikat lisäävät tarvetta tietää, ovatko järjestelmät turvattuja, mitä puutteita tai ongelmia niissä on, mitä seurauksia puutteiden olemassaolosta voi aiheutua ja mitä näiden uhkien torjumiseksi pitäisi tehdä. Sisäinen valvonta ja arviointi ovat olennainen osa virastojen ja laitosten normaalia johtamistoimintaa ja riskienhallintaa.

Tietoturvallisuuden kehittämiseen kuuluu siten keskeisesti *seuranta ja arviointi*. Organisaation tiedonkäsittelyn riskit sekä tietoturvallisuuden tila ja johtaminen on arvioitava systemaattisesti. Toimintaa varten luodut menetelmät ja mittaristot antavat työkaluja jatkuvaluonteiseen arviointitoimintaan. Arviointi voi olla sisäistä itsearviointia tai organisaatioiden keskinäistä vuorovaikutteista toimintaa esimerkiksi eri viranomaisten välillä tai ulkoistamiseen liittyvää sopimuspohjaista toimintaa.

Arviointi on luonteeltaan jatkuva ja pysyvä toiminto, jota käytetään tietoturvallisuuden kehittämiseen ja laadun parantamiseen. Siten arviointeja tehdään lähtien organi-

saation sisäisistä tarpeista, eikä vain vastaamaan ulkopuolisiin vaateisiin. Tarkoituksena on saada arvioitavissa kohteissa aikaan myönteisiä muutoksia havaitsemalla mahdolliset puutteet ja heikkoudet, jotta niitä voidaan tietoisesti ryhtyä korjaamaan. *Tietoturvallisuuden hallintajärjestelmän arviointisuosituksessa* (VAHTI 3/2003) ja *Riskien arviointisuosituksessa* (VAHTI 7/2003) on kuvattu arvioinnin keskeiset käsitteet ja menettelyt sekä tarjotaan apuvälineitä arviointien tekemiseen. Toiminnan laadun arvioinnin ja tietoturvallisuuden välistä yhteyttä on suosituksessa havainnollistettu oheisella kuvalla (kuva 2).



Kuva 2. Tietoturvallisuuden ja laadun arviointikokonaisuus.

Tietoturvallisuuden arviointien suorittamiseksi tarvitaan arviointimenetelmien nykyistä laajempaan soveltamista ja virastokohtaisten mittareiden ja arviointikäytäntöjen kehittämistä.

Tietoturvariskien hallinnan riittävyyden arviointi on osa laajempaa riskienhallinnan arviointia. Valtioneuvosto hyväksyi talousarviosta annetun asetuksen muutokset 7.4.2004. Asetus tuli voimaan 15.4.2004. Asetuksessa edellytetään, että ylimmän johdon on annettava myös arviointi- ja vahvistuslausuma sisäisestä valvonnasta ja siihen kuuluvasta riskienhallinnasta (65 §:n 1 momentin 7 kohdan säännös).

ESIMERKKI 1: TIETOTURVALLISUUS KAUPPA- JA TEOLLISUUSMINISTERIÖN JA TE-KESKUSTEN TULOSKORTTIMALLISSA (BSC)

Yleistä

Kauppa- ja teollisuusministeriön yleishallinnollisessa ohjauksessa toimii 15 alueellista Työvoima- ja elinkeinokeskusta (TE-keskukset). Niiden päätöksenteon ja tulosohjauksen kehittämisessä on sovellettu Balanced Scorecard –mallia (BSC, tasapainoinen tuloskortti). Päätöksenteon, johtamisen ja tulosohjauksen tarvitsema tieto tulee olla mm.:

- relevanttia
- olennaiseen keskittyvää
- ristiriidatonta ja loogista
- analyysiin soveltuvaa.

BSC-mallissa organisaation tulos aikaansaadaan kohdistamalla toimintaa strategiassa linjattujen suuntaviivojen mukaisesti seuraavin toimenpitein:

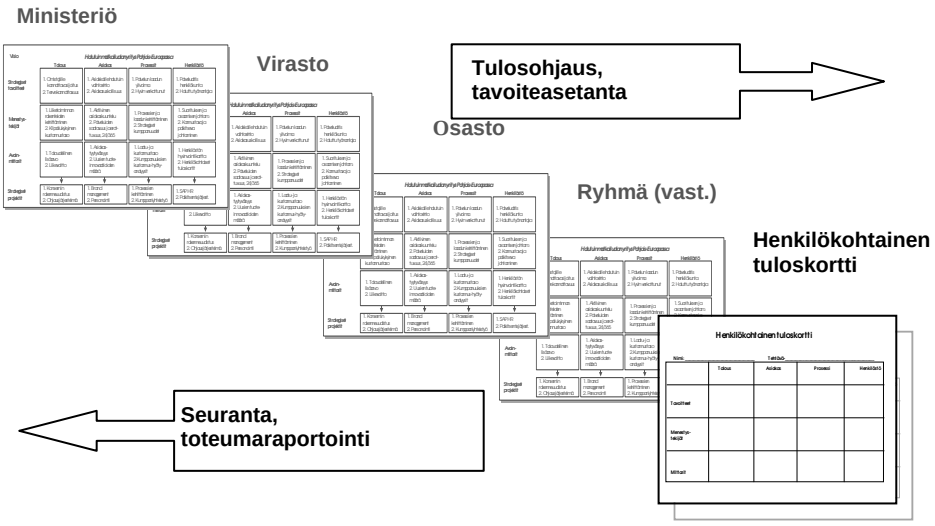
- muunnetaan strateginen lähtökohta operationaaliseksi toiminnaksi/termeiksi
- muokataan organisaatio strategiaa tukevaksi
- tehdään strategiasta jokaisen organisaatiossa työskentelevän tehtävä
- tehdään strategiasta jatkuva prosessi
- johto toimii muutoksen läpiviejänä.

Mallissa toiminnan strategiset painopistealueet kuvataan erillisille tuloskorteille, joita ministeriössä on käytössä neljä (vaikuttavuus, prosessit ja rakenteet, resurssien hallinta sekä uudistuminen ja työkyky) ja TE-keskuksissa viisi (vaikuttavuus, asiakkuus, prosessit ja rakenteet, resurssit ja henkilöstö).

BSC-viitekehyksessä tarkastellaan sekä organisaation sisäisiä että ulkoisia prosesseja. Sisäisesti organisaation ydin- ja tukiprosesseja tehostetaan ja uudistetaan tavoitteena suorituskyvyn parantaminen ja sitä kautta saavutettavat laatu- ja tehokkuushyödyt. Ulkoisesti vastaaviin tavoitteisiin pyritään organisaatioiden välisiä rajaaitoja ohentamalla käyttäen välineenä yhteistyötä ja erilaisten toimijoiden osaamisen parempaa hyödyntämistä.

Tuloskorteille kuvataan kullakin painopistealueella tarkasteluajanjaksona edistettäväksi valitut *tavoitealueet tai yksittäiset tavoitteet*, niihin kohdennettavat *toimenpiteet* tai *hankkeet* sekä kustakin haluttu *toteuma*, jonka saavuttamista seurataan määritetyin määrällisiin (kvantitatiivisiin) tai laadullisiin (kvalitatiivisiin) seikkoihin kohdetuvin

mittarein. Tuloskortit voidaan *ketjuttaa* organisaatioiden välillä. TE-keskusten tulostoteumalla on seurannaisvaikutuksia sitä ohjaavan ministeriön elinkeino-osaston tuloskorttiin ja sitä kautta koko ministeriön tavoitteiden toteutumiseen. Edelleen yksittäisen TE-keskuksen kortti voidaan purkaa osasto- tai hankekohtaisiksi korteiksi ja viedä pisimmälle mentynä jopa vuosittaisena tavoiteasetantana yksittäisen kehityskeskustelun tasolle esimiehen ja alaisen välillä. Riippuen tasosta ja tarkastelunäkökulmasta tarkastelussa käytetään näkökulmana johtamis-, asiakas- ja teknistä näkökulmaa.



Tietoturvallisuuden käsittely ministeriötasolla

Tietoturvallisuuden huomiointi BSC-tulosohjaukseen voidaan mallintaa pyrkimällä vastaamaan seuraavaan kysymykseen: *Kuinka tietoturvallisuus vaikuttaa TE-keskusten tarjoamien palvelujen kehittämiseen (toiminnan uudistaminen), tuottamiseen (laatu, kustannukset) ja jakeluun (saatavuus)?*

KTM:n elinkeino-osaston tuloskortissa on vuotta 2004 koskevaksi tulosjohtamisen tasolla määritetty myös TE-keskuksia koskeviksi *kriittisiksi menestystekijöiksi* seuraavia:

- tulosjohtamisprosessi toimii tuloksellisesti (taloudellisesti ja tehokkaasti) siten, että toiminta ja prosessit edistävät ja tukevat ministeriön strategiaa ja vaikuttavuustavoitteita
- yksikköjen toiminta muuttuu tulosohjauksen kautta tuloksellisemmaksi ja vaikuttavammaksi.

Käytettävinä *arviointikriteereinä* ovat tällöin:

- tehokkuuden kasvu
- vaikuttavuuden kasvu ja
- tulosohjauksen laadullinen toimivuus saadun palautteen perusteella.

Arviointikriteerit kattavat useamman vuoden seurannan vaikuttavuusseurannan mahdollistamiseksi, mutta asetetuille tavoitteille on myös asetettu erilaisia kalenterivuoteen kohdennettavia sektorikohtaisia kehittämishankkeita.

Tietoturvallisuuden käsittely TE-keskusten vuosittaisissa tulostavoitteissa

TE-keskusten *vaikuttavuus*-korttiin tietoturva-asioilla on välillinen vaikutus. Suoranaisia kehittämis- ja seurantakohteita voidaan sen sijaan liittää *asiakkuus*-korttiin tarkastellen sitä palvelun laadun näkökohdasta. Mittareita ovat tällöin asiakastyytyväisyyteen (palvelukysely, sisäinen seuranta) liittyen esim. palvelujen vasteaika ja poikkeamat.

Prosessit ja rakenteet –korttiin liityvät keskeisimmät turvallisuuden seurantatekijät, eli toiminnan tuottavuus ja taloudellisuus. Tässä yhteyksissä käytettävillä kysymyksillä arvioidaan turvauhista syntyvät kustannusvaikutukset sekä määritellään kehittämishankkeet ja niihin liittyvät kytkennät tietoturvallisuuteen. Mittausta voidaan myös suorittaa laatuarviointikriteerein määrittäen mm. poikkeamat. *Resurssit*-korttiin turvallisuusasiat kytkeytyvät tarvittavina rahallisina ja henkilöresursseina; tavoitetilassa strategialähtöisesti. *Henkilöstö*-kortilla turvallisuusasioiden osaamiseen liittyvät toimenpiteet ovat kehittämisen keskeinen osa-alue. Tällöin voidaan mm. määritellä tavoitteellinen osaamistaso verraten sitä toteumaan. Muita tähän liittyviä tekijöitä ovat mm. tietoturvallisuuden johtamiseen ja turvallisuuden valvontaan liittyvät määrälliset ja laadulliset mittarit.

Tietoturvallisuuden vieminen yksikkö- ja henkilötasolle

Tuloskorttien ketjuttuessa tavoiteasetanta siirtyy kullakin osa-alueella yksikkö- ja lopulta henkilötasolle esim. kehityskeskustelumenettelyjen kautta. Tällöin kullekin kehittämisen osa-alueille määritetyt hankkeet täsmentyvät käytännön toimenpiteiksi ja henkilökohtaisen vastuutuksen tasolle. Lähimmän esimiehen rooli korostuu kokonaisuuden määrittelyssä ja kunkin tavoitteen konkretisoinnissa henkilökohtaisiksi tulostavoitteiksi.

Prosessien ja resurssien kautta tarkasteltuna tavoitteena voivat esimerkiksi tällöin olla:

- kattava haittaohjelmatorjunta (mittarina katkosten määrä, verkon ja työasemien suojausaste)
- ajantasainen suunnittelu (ohjeistuksen kattavuus, testatut toimintatavat poikkeamatilanteissa)
- riittävä osaaminen (arvioinnit, koulutus).

Mittaamisessa käytetään tilanneseurannassa myös asiakokonaisuuksien viemistä numeeriseen asteikkoon (esim. tarkastelu arvovälillä 1 – 10).

Kokonaisuudessa ratkaisevana tekijänä on toimintakulttuurin kehittäminen; jokaisen organisaatiossa työskentelevän on miellettävä roolinsa tietoturvallisuuden edistämisessä. Tätä edistääkseen ministeriön toimesta on järjestetty eri TE-keskusten koko henkilöstölle koulutuspäiviä tietoturvallisuudesta. Yksinomaan ohjausprosessin kehittäminen ei luonnollisestikaan riitä, vaan tarvitaan myös osaamisen kehittämistä ja verkostoitumista.

ESIMERKKI 2: TIETOTURVALLISUUS VÄESTÖREKISTERIKESKUKSEN LAATUJÄRJESTELMÄSSÄ

Yleistä

Väestörekisterikeskus (VRK) on sisäasiainministeriön hallinnonalalla toimiva virasto, joka kehittää ja ohjaa väestökirjanpitoa sekä pitää yllä valtakunnallista väestötietojärjestelmää yhdessä maistraattien kanssa. VRK vastaa myös väestötietojärjestelmän valtakunnallisista tieto- ja verkkopalveluista. Lisäksi sen tehtäviin kuuluvat varmennepalvelut, sähköinen henkilökortti, vaalien äänioikeusrekisteri, julkishallinnon yhteyspalveluhakemisto (Julha) sekä holhousrekisteri.

VRK on keskeinen rekisteriviranomainen ja sen tarpeet ja vaatimukset tietoturvallisuuden kehittämisen ja ylläpidon suhteen ovat korkeat. Virasto sai SFS-Sertifiointi Oy:n myöntämän tietoturvasertifikaatin syyskuussa 2002 ensimmäisenä valtionhallinnon organisaationa. Samanaikaisesti virastolle myönnettiin lisäksi varmennepalvelutoiminnan laatusertifikaatti.

Sertifiointihankeen tausta ja käytetty standardi

Vuoden 2001 alussa käynnistetyt tietoturvahanke ja varmennepalvelujen laatuprojekti ovat olleet keskeinen osa viraston visiosta (alansa johtava tietokeskus) lähtevää toiminnan kehittämisstrategiaa. Koska VRK:ssa käsitellään henkilötietoja ja myönnetään sähköisiä varmenteita, on tietoturvallisuus luonnollisesti toiminnan lähtökohta. Sertifioinnin ansiosta tietoturvallisuuden ja tietosuojan kehittäminen ja ylläpito on organisoitu entistä paremmin. Osana sertifiointiprojektia virastolle syntyi selkeä ja johdonmukainen tietoturvallisuuden hallintajärjestelmä.

VRK:n saama tietoturvasertifikaatti on BS 7799:1999 -standardin mukainen. Se on tietoturvajohtamisen kansainvälisesti hyväksytty tapa toimia, jolle voi hakea sertifikaattia. Kokonaisuuteen sisältyvät mm. tietoturvallisuuspolitiikka, tietoturvallisuuden organisointi, suojattavien kohteiden luokitus ja valvonta, henkilöstöturvallisuus, fyysinen tietoturvallisuus, tietoliikenteen ja käyttötoimintojen hallinta, pääsyoikeuksien valvonta, järjestelmien kehittäminen ja ylläpito sekä liiketoiminnan jatkuvuuden hallinta ja vaatimustenmukaisuus. Standardi perustuu ”best practices” –ajatteluun ja myös VRK:ssa lähtökohtana on ollut omaksua organisaation kannalta parhaimmat käytännöt.

Hankkeen läpivienti

Sertifikaattiin tähtäävä toiminta käynnistyi VRK:ssa tietoturvaryhmän perustamisella vuoden 2001 alussa. Tämän jälkeen hyväksyttiin viraston tietoturvapolitiikka ja laadittiin toimintasuunnitelma. Projektin alussa johto määritteli vaatimusperustan tietoturvallisuudelle. Tämän jälkeen projekti kuvasi tietojärjestelmät ja toimintatavat, määritteli tietoturvan hallintajärjestelmän, arvioi riskit ja laati niiden hallintasuunnitelman. Lisäksi valittiin tarvittavat suojamekanismit sekä laadittiin standardin soveltamissuunnitelma. Lopuksi hankkeessa luotiin vielä jatkokehitys- ja seurantasuunnitelma. Projektiryhmän ja tietoturvapäällikön rinnalla viraston johdon rooli oli projektin eri vaiheissa keskeinen. Tietoturvaryhmä suoritti sisäisen auditoinnin huhtikuussa 2002, jonka jälkeen johto katselmoi viraston auditointivalmiuden. Ulkoisen auditoinnin suoritti SFS-Sertifiointi Oy kesäkuussa 2002. Auditoinnissa ilmenneiden lievien poikkeamien korjaukset tarkastettiin pari viikkoa auditoinnin jälkeen.

Kokemuksia kehityshankkeesta

Viraston henkilöstön osuus tietoturvallisuuden toteutumisessa on ensiarvoisen tärkeää ja siksi jatkuva koulutus ja asioiden kertaaminen on välttämätöntä. Lisäksi tietoturvallisuuden ohjeistukseen on panostettu ja kaikki keskeiset ohjeet löytyvät ajantasaisina VRK:n intranetista. Itse sertifiointiprosessi koski koko henkilöstöä ja sen kuluessa organisaatiossa jouduttiin kehittämään monia jokapäiväiseen työhön liittyviä toimintatapoja.

Sertifikaatit eivät ole pysyviä, vaan niiden säilyttäminen edellyttää säännöllisesti toteutettavan ja vähintään vuosittain tapahtuvan seurannan. Organisaation on ylläpidettävä ja kehitettävä tietoturva- ja laatujärjestelmiään sekä varmistettava, että prosessit, työsuoritukset ja palvelut toteutetaan sertifioidun järjestelmän mukaisesti mm. seuraavien vuosittaisten toimenpiteiden avulla:

- dokumentaation ylläpito
- tietoturvapolitiikan päivittäminen
- sisäinen auditointi ja johdon katselmointi
- ulkopuolinen auditointi
- tietoturvatiedostojen kerääminen
- raportointi johtoryhmälle
- uhkakartoitus.

Vaatimusstandardin BS7799-2: 2002 uusi versio on suomennettu ja VRK tulee siirtymään siihen kevään 2004 seurannassa. Uudessa standardissa korostuu tietoturvallisuuden jatkuvan parantamisen merkitys. Riskejä arvioidaan ja seurataan vuosittain ja keskeistä on, että arvioinnin perusteella valittujen turvamekanismien ja soveltamissuunnitelman välillä on selkeä yhteys. Johdon vastuu tietoturvallisuudesta korostuu entisestään.

Sertifioinnin vaikutuksia ja saavutettuja hyötyjä

Prosessin aikana viraston henkilöstön asenteissa ja turvatietoisuudessa tapahtui merkittävää kehittymistä. Tämä on keskeistä, sillä n. 80 % tietoturvan riskeistä liittyy tavalla tai toisella ihmisiin. Monet toimenpiteet ovat yksinkertaisia arkisiin asioihin liittyviä työtapojen muutoksia (esim. puhdas näyttö, työpöytä tai seinä). Tärkeää on, että hallitaan oikea suoritus ja toimintamalli eri tilanteissa ja saavutetaan erilaisten uhkien ymmärtäminen. Erilaisia toiminnallisia hyötyjä voidaan luetella seuraavasti:

- lopputuloksena on selkeä kokonaisuus (dokumentit ja ohjeistus), jota voidaan jatkuvasti parantaa yhteistyössä henkilöstön kanssa
- kehittämissuunnitelma ohjaa toimintaa; asiat priorisoidaan organisaation tarpeiden mukaisesti
- päätökset määräajassa toimenpiteistä joita jatkossa tehdään (esim. jatkokehitys- ja seurantasuunnitelma)
- luottamuksen lisääntyminen; asiat on mietitty ja koulutettu sekä päivittäiset rutiinit kunnossa.

VRK:n käytössä olevia seurantamenetelmiä

VRK:n johto seuraa tietoturvan toteutumista johdon kokouksien yhteydessä. Tietoturvapäällikkö raportoi kolme kertaa vuodessa tietoturvallisuuteen liittyvät tapahtumat. kahdeksankohtaisen jaottelun mukaisesti. Tietoturvan mittaamista tehdään sekä kvalitatiivisin että kvantitatiivisin mittarein. Johdolle raportoidaan mm. yksikkökohtaisesti tehtävät riskikartoitukset ja itsearvioinnit. Tietoturva-auditoinneista raportoidaan kaikki tehdyt havainnot. Riskikartoituksista puolestaan raportoidaan toimenpide-ehdotukset kaikkien havaittujen merkittävien riskitekijöiden suhteen.

Edellä kuvattujen menettelyjen lisäksi on käytössä joukko kvantitatiivisia (määrällisiä) mittareita, joita ovat mm.:

- luvattomien kirjautumisyritysten lukumäärä järjestelmiin
- palvelujen keskeytysten pituudet (esim. tietoliikenne, sähköposti) ja lukumäärät
- tietoturvasopimusten m äärä
- havaitut virukset
- varkauksien määrä
- pyydetyt luotettavuuslausunnot
- tietoturvapoikkeamat
- poistettujen käyttäjätunnusten määrä.
- tietoturvaryhmän kokousten lukumäärä.

Käytettyjä lähteitä

Robert S. Kaplan ja David P. Norton: The Balanced Scorecard, Translating Strategy Into Action. Harvard Business School Press, 1996.

Hallituksen esitys (56/2003) Eduskunnalle laiksi valtion talousarviosta annetun lain muuttamisesta.

Hallituksen tietoyhteiskuntaohjelma http://www.governmetn.fi/tiedosto/pdf/fi/41868.pdf

Kansallinen tietoturvastrategia http://www.mintc.fi/www.sivut/suomi/tele/tietoturvastrategia.pfd

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Valtionhallinnon tietoturvallisuuden johtoryhmä 7/2003. Valtiovarainministeriö.

Security Metrics Guide for Information Technology Systems. NIST Special Publication 800-55, July 2003 http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

Robert S. Kaplan ja David P. Norton: The Strategy-Focused Organization. Harvard Business School Press, 2001.

Seppo Määttä: Tasapainoinen menestysstrategia: Balanced Scorecardin tuolla puolen. Inforviestintä Oy, 2000.

Tuomas Lehmusmetsä: Tasapainoisen mittariston soveltuvuus tietoturvallisuuden mittaamiseksi. Toinen tietoturvallisuuden koulutusohjelma, tutkielmajulkaisu. Teknillinen korkeakoulu, koulutuskeskus Dipoli, 2003.

Parempaan tilivelvollisuuteen. Valtion tilinpäätösuudistuksen periaatteet. Työryhmämuistio 2/2003. Valtiovarainministeriö.

Tuomas Pöysti: Sisäinen tarkastus valtionhallinnossa ja tietoturvallisuuden hallinta. Pohjois-Suomen tuomarikoulu. Tietoturvallisuus ja laki, ajankohtaista asiaa tietoturvasta. Rovaniemi 2002.

TE-keskusten ohjaamisen ja päätöksenteon tietojärjestelmät JOTI. Kauppa- ja teollisuusministeriön kertomuksia ja selvityksiä 1/2000.

Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet, turvallisuuskulttuurin kehittäminen. OECD:n suositus. Suomenkielinen käännös: 2002, Valtiovarainministeriö.

Jorma Kajava: Tietoturvallisuuden hallinnan kriittiset onnistumistekijät. Hallinnon tutkimus vol. 22, 1/2003.

Tietoturvallisuuden hallintajärjestelmän arviointisuositus. Valtionhallinnon tietoturvallisuuden johtoryhmä 3/2003. Valtiovarainministeriö.

Tullilaitoksen itsearvioinnin työkirja. Tullihallitus, 2002.

Tulosohjauksen terävöittäminen. Työryhmämuistio 9/2003, Valtiovarainministeriö.

Työvoima- ja elinkeinokeskusten tulostavoitteet vuodelle 2003. Kauppa- ja teollisuusministeriön kertomuksia ja selvityksiä 2/2003.

Valtionhallinnon tietoturvallisuuskäsitteistö. Valtionhallinnon tietoturvallisuuden johtoryhmä 4/2003, Valtiovarainministeriö.

Valtion viranomaisen tietoturvallisuustyön yleisohje. Valtionhallinnon tietoturvallisuuden johtoryhmä 1/2001, Valtiovarainministeriö.

VMn tietoturvaohjeita ja –julkaisuja

- Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004
- Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006, VAHTI 1/2004
- Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
- Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, VAHTI 6/2003
- Käyttäjän tietoturvaohje, VAHTI 5/2003
- Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003
- Tietoturvallisuuden hallintajärjestelmän arviointi, VAHTI 3/2003
- Suositus turvallisesta etäkäyttöarkkitehtuurista, VAHTI 2/2003
- Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003
- Tunnistaminen valtionhallinnon verkkopalveluissa, VM 6/01/2003
- Arkaluonteisten kansainvälisten tietoaineistojen käsittelyperiaatteet, VAHTI 4/2002
- Valtion etätyön tietoturvallisuusohje, VAHTI 3/2002
- Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002
- Tietotekniikan turvallisuus ja toiminnan varmistaminen, PTS 1/2002 ja VM
- Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001
- Tietotekniikkahankintojen tietoturvallisuustarkistuslista, VAHTI 6/2001
- Sähköpostin ja lokitietojen käsittely, VAHTI 5/2001
- Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001
- Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
- Tietokoneviruksilta ja muilta haittaohjelmistoilta suojautumisen yleisohje, VAHTI 4/2000
- Tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000
- Valtion tietoaineistojen käsittelyn tietoturvaohje, VAHTI 2/2000
- Tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM, 5/01/2000
- Tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, VAHTI 2/1999
- Suositus toimitilaturvallisuudesta, VM 31.12.1998

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin: (09) 160 01
Telefaksi: (09) 160 33123
www.vm.fi

2/2004
TIETOTURVALLISUUS JA
TULOSOHJAUS

ISBN 951-804-432-5
ISSN 1455-2566