TEKNILLINEN KORKEAKOULU
Elektroniikan, tietoliikenteen ja automaation tiedekunta

Juha Kalander

Tietoturvallisuuden hallinta: palautejärjestelmän vaatimukset ja toteutustavat

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 5.12.2007

Työn valvoja	Professori Raimo Kantola, TKK
Työn ohjaaja	Diplomi-insinööri Kalevi Hyytiä, Pääesikunta

Tekijä: Juha Kalander

Työn nimi: Tietoturvallisuuden hallinta: palautejärjestelmän vaatimukset ja toteutustavat

Päivämäärä: 5. joulukuuta, 2007 **Sivumäärä:** 71+26

Osasto: Elektroniikan, tietoliikenteen ja automaation tiedekunta

Professuuri: S-38 Tietoliikenne- ja tietoverkkotekniikan laitos

Työn valvoja: prof. Raimo Kantola, Tietoliikennetekniikan professori

Työn ohjaaja: Kalevi Hyytiä, DI

Käsittelen tässä työssä tietoturvallisuuden hallintaa palautejärjestelmän avulla. Valtionhallinnossa tietoturvallisuuden hallinta perustuu normiohjaukseen, jota toteuttaa tietoturvallisuuden tietoturvatoiminnan hallintajärjestelmä. Ongelmana on saada esille hallinnan ja toiminnan tehokkuus ja vaikuttavuus.

Olen valinnut ongelma ratkaisuksi palautejärjestelmämallin. Valinnan peruste se, että prosessimuotoista toimintaa on ohjattava kuten prosessia ohjataan: tulosta mittaamalla ja vertaamalla annettuihin tavoitteisiin – siis takaisinkytkennällä. Esitän palautejärjestelmämallille vaatimuksia, jotka pohjautuvat kirjallisuustutkimukseen ja haastatteluihin, ja toteutustapoja. Palautejärjestelmän on tuotettava tilannekuva, joka on oikea-aikainen, perustuu merkitykselliseen tietoon ja on kohdennettu oikein.

Prosessimuotoisen toiminnan ohjaaminen kulminoituu mittaamiseen ja mittaustulosten analysointiin - metriikkaan. Palautejärjestelmän toteutustavoissa olen keskittynyt mittareiden ja metriikan määrittelyihin. Olen valinnut määrittelytavaksi Goal Question Metric -mallin, jota sovellan standardiin ISO/IEC 27001:2005. Toinen esittämäni toteutustapa koskee henkilöstön tietoturvakulttuurin mittaamista. Tietoturvallisuuden johtaminen on ihmisten johtamista ja johtamisen vaikuttavuus ilmenee tietoturvakulttuurina. Tietoturvakulttuuria on mitattava esimerkiksi henkilöstökyselyiden yhteydessä.

Avainsanat: Tietoturvallisuuden hallinta, palautejärjestelmä, mittaaminen

Author: Juha Kalander

Title: Security management: feedback system requirements and realization

Date: December 5, 2007 **Number of pages:** 71+26

Department: Faculty of Electronics, Communications and Automation

Professorship: S-38 Department of Communications and Networking

Supervisor: prof. Raimo Kantola, Professor of Communication Technology

Instructor: Kalevi Hyytiä, M.Sc (Tech.)

This thesis discusses information security management with a feedback system. The Finnish Goverment infomation security management system is based on the Finnish laws and directed with the standards. The basic problem is to show impact and effectiveness of the security management.

As a solution I have chosen the feedback model. The reason is that security management process should be controlled like any other process: with feedback system. This means measurement of the results of the security operations and comparing these results with the given goals from the security management system. I have stated demands for the feedback system based on the litterature study and interviews. The feedback system must provide meaningful information on time to the right target group.

The operations of feedback system is based on measurements and metrics. I propose to use the Goal Question Metric model for metrcis development. I have applied the model to the ISO/IEC 27001:2005 standard. The same model can be used for the development of metrics to evaluate the security awareness and culture of the organization. The security management is human resources management and the impact of management must be evaluated. The information security climate must be evaluated as part of the normal organizational climate measurements.

Keywords: Security management, feedback system, metrics

Esipuhe

Yli kymmenen vuoden työnteko ja opiskelu tietoturvan parissa on saavuttanut yhden huipentuman: diplomityöni on valmis.

Haluan kiittää Puolustusvoimia tämän diplomityön tekemisen mahdollistamisesta. Kiitos kuulee heille, jotka osallistuivat haastatteluihin ja erityisesti Kalevi Hyytiälle, joka antoi aiheen ja ohjasi työni valmiiksi. Lisäksi kiitos kaikille DiplomPro-hankkeen vetäjille TKK Dipolissa, te tarjositte hyvän ympäristön työskennellä.

Erityisesti haluan kiittää vaimoani ja lapsiani jaksamisesta ja tuesta tämän kymmenen vuoden aikana. Aikuisopiskelu ei onnistu ilman perheen tukea.

Tuusulassa, 5. joulukuuta, 2007

Juha Kalander

Sisällys

Lyhenteet

BSI	British Standards Institute, Iso-Britannian standardointi organisaatio
BSI	Bundesamt für Sicherheit in der Informationstechnik, Saksan tietoturvaviranomainen
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria, Kanadan valtion tietotekniikan tietoturvallisuuden arviointiperusteet
COBIT	Control Objectives for Information and related Technology, parhaiden käytänteiden runko tietoteknologialle
FIPS	Federal Information Processing Standards, Yhdysvaltojen hallinnon standardien kokoelma tietotekniikan käyttöä varten
GQM	Goal Question Metrics, metriikan määrittelytapa tavoitelähtöisesti
HVK	Huoltovarmuuskeskus
ISACA	Information Systems Audit and Control Association, tietojärjestelmien auditoijien ja tarkastajien yhteistyöjärjestö
ISECOM	Institute for Security and Open Methodologies, tietoturvatutkijoiden yhteistyöjärjestö
ISO/IEC	International Organization for Standardization/ International Electrotechnical Comission, kansainvälinen standardointiorganisaatio
ISM3	Information Security Management Maturity Model, tietoturvan hallinnan kypsyysmalli
ISMS	Information Security Management System, tietoturvallisuuden hallintajärjestelmä
ISSEA	International Systems Security Engineering Association, yhteistyöorganisaatio tietoturvan ohjauksen kehittämistä varten
ITIL	Information Technology Infrastructure Library, tietohallinnolle suunnattu menettelyohjeisto tietotekniikan hallintaan
ITSEC	Information Technology Security Evaluation Criteria, eurooppalainen tietotekniikan turvallisuuden arviointiperusteet
ISF	Information Security Forum, yritysten yhteistyöjärjestö parhaiden tietoturvakäytänteiden määrittelemiseksi
KPI	Key Performance Indicatiors, toiminnan avainmittarit
MDP	Markov Decision Process, Markovin päätöksentekoprosessi
MIS	Management Information System, tiedonhallintajärjestelmä

NIST	National Institute of Standards and Technology, Yhdysvaltojen standardointiorganisaatio
PDCA	Plan-Do-Check-Act, ISO/IEC 27001 toimintaprosessi
PTS	Puolustustaloudellinen suunnittelukunta
ROI	Return of Investment, pääoman tuottoaste investoinnille
ROSI	Return of Security Investment, pääoman tuottoaste tietoturvainvestoinnille
SEM	Security Event Management, tietoturvatapahtumien hallintajärjestelmä
SIEM	Security Information and Event Management, tietoturvatiedon ja -tapahtumien hallintajärjestelmä
SIM	Security Information Management, tietoturvatiedon hallintajärjestelmä
SLA	Service Level Agreement, palvelutasosopimus
SSAM	SSE-CMM Appraisal Method, kypsyystason arviointimenetelmä
SSE-CMM	Systems Security Engineering Capability Maturity Model (ISO 21827), toiminnan tietoturvallisuuden kypsyysmalli
TCSEC	Trusted Computer System Evaluation Criteria, Yhdysvaltojen hallinnon tietotekniikan turvallisuuden arviointiperusteet
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
VM	Valtiovarainministeriö

1 Johdanto

1.1 Alkusanat

Käsittelen tässä opinnäytteessä tietoturvallisuuden hallinnan palautejärjestelmän vaatimuksia ja toteutustapoja. Opinnäyte on tehty Puolustusvoimille.

Valtionhallinnossa on pitkät perinteet tietoturvallisuuden hallinnasta osana hyvää tiedonhallintatapaa. Valtionvarainministeriö (VM) on asettanut valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI), joka on lähes kolmenkymmenen vuoden ajan antanut tietoturvallisuuteen liittyviä ohjeita (VAHTI 1/2001).[1]

Tietoturvallisuustoimintaa ohjaa tietoturvallisuuden hallintajärjestelmä. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta vuodelta 1999 (VM 11.11.1999) kuvaa tietoturvallisuuden hallintajärjestelmän. Täydellisin esitys hallintajärjestelmästä on VAHTI-ohjeessa Tietoturvallisuuden hallintajärjestelmän arviointisuositus (VAHTI 3/2003). Hallintajärjestelmä yhdistää lainsäädännöstä, standardeista ja sopimuksista[2] tulevat vaatimukset (normiohjaus) yhdeksi kokonaisuudeksi.

1 VAHTI 1/2001 -dokumentissa on maininta yli 20 vuoden ajan. Voimassa oleva VAHTI-ohjeistus on Liittessä 1.

2 Suomessa valtiota koskevat merkittävät sopimukset viedään pääsääntöisesti lainsäädäntöön.

Palautejärjestelmälle on annettu perusteet VAHTI-ohjeessa 1/2001: ”Tietoturvallisuuden ylläpito edellyttää jatkuvaa tietoturvallisuuden seurantaa, sen perusteella ylimmälle johdolle tapahtuvaa raportointia sekä korjaavia toimenpiteitä.” Myös VAHTI 3/2003 korostaa samaa: ”Pelkkä tietoturvallisuussuunnittelu ja toimeenpano eivät riitä vaan selkeästi vastuutettu valvonta ja seuranta ovat oleellinen osa tietoturvallisuuden johtamista ja hallintaa.” Tarkemmin palautejärjestelmää ei ole suorasanaisesti tai ohjeistona määritelty. Tutkimusongelman voi määritellä seuraavasti: miten palautejärjestelmä on määriteltävä, mitä vaatimuksia sille voi asettaa ja mitä toteustapoja on. Tämän työn tavoitteena on antaa perustaa palautejärjestelmän määrittelylle ja toteutustavoille.

1.2 Työnkulku ja metodit

Metodeja on kaksi: kirjallisuustutkimus ja henkilöhaastattelut. Kirjallisuustutkimus jakautuu kahteen osaan: Työn aluksi luvussa 2 esitellään tietoturvallisuustoimintaan vaikuttava tärkein lainsäädäntö, tärkeimmät standardit ja suositukset eli normiohjaus. Luvussa 3 esitellään valtionhallinnon tietoturvallisuuden hallintajärjestelmä (VAHTI 1/2001 ja 3/2003 mukaisesti). Toinen osa kirjallisuustutkimuksesta sisältyy palautejärjestelmää käsittelevään lukuun (Luku 4), jossa on myös henkilöhaastatteluiden analyysi. Näiden perusteella esitetään palautejärjestelmän vaatimukset ja tarkastellaan mahdollisia toteutustapoja.

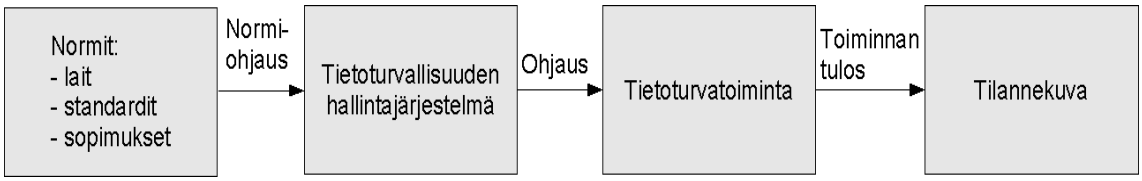
Lähdeviittauksia on käytetty seuraavasti: VAHTI-ohjeisiin ja muihin valtionhallinnon ohjeisiin viitataan järjestysnumerolla ja vuosiluvulla, kuten VAHTI 1/2001, PTS 1/2001. Työntekohetkellä voimassa oleva VAHTI-ohjeistus on Liitteessä 1 omana kokonaisuutena. Lakiviittaukset tehdään lain numerolla ja vuosiluvulla, kuten 621/1999. VAHTI-ohjeisiin vaikuttava lainsäädäntö on Liitteessä 2 omana kokonaisuutena. Muihin lähteisiin viitataan Harvard-standardin mukaisesti.

1.3 Rajaukset

Tämä työ ei ole laki- eikä standarditutkielma, mutta tärkeimmät kohdat niistä esitellään lyhyesti, jotta tietoturvallisuuden hallinnan palautejärjestelmän viitekehys olisi selvillä.

2 Normiohjaus

Tässä luvussa käsitellään lyhyesti valtionhallinnon tietoturvallisuustoimintaan vaikuttava normisto: lainsäädäntö ja standardit. Valtionhallinnossa on pyritty normiperustaiseen tietoturvallisuuden ohjaukseen: Lainsäädännöstä tulevat velvoitteet ja tietoturvatoiminnan perusteet. Standardit ja suositukset ovat välineitä hallinnan toteuttamiseen. Palautejärjestelmän vaatimuksia määriteltäessä ja toteutustapaa pohdittaessa on oleellista tietää, mistä siihen tulee vaatimuksia ja mihin sen vaikutuksen pitää ulottua. Tarkastelussa keskitytäänkin niihin kohtiin, jotka vaikuttavat palautejärjestelmän vaatimuksiin tai toteutustapoihin. Kuvassa 1 on esitetty normiohjauksen suhde valtionhallinnon tietoturvallisuuden hallintajärjestelmään ja tietoturvatoimintaan.



Kuva 1: Normiohjaus ja tietoturvallisuuden hallinta

2.1 Vaikuttava lainsäädäntö

Lainsäädäntö antaa tavoitetason tietoturvallisuuden toteuttamiselle. Palautejärjestelmää määriteltäessä ja toteutettaessa on tiedettävä vaikuttava lainsäädäntö ja sen antama tavoitetaso: näin tietoturvatoiminnan tulosta lainmukaisuuden osalta voi verrata annettuun tavoitetasoon. Tietoturvallisuuden hallintajärjestelmään vaikuttava lainsäädäntö[3] on runsasta: perustuslain säädöksistä aina kauppalakiin. Osa lainsäädännöstä sisältää suoraan tietoturvavallisuusvelvoitteita (kuten henkilötietolaki), osa vaikuttaa myös rajaavasti (kuten sähköisen viestinnän tietosuojalaki) ja osa välillisesti (sopimuslaki). Vaikuttavan lainsäädännön suhteita on kuvattu Kuvassa 2.

Kuva 2: Lainsäädännön suhteet

Lainsäädännön perusta on perusoikeuksissa, jotka on kuvattu perustuslaissa. Muu lainsäädäntö rajaa ja tarkentaa perustuslain säädöksiä. Valmiuslaki on poikkeusoloja varten ja siinä rajataan ja tarkennetaan osa lainsäädännöstä poikkeusoloihin sopivaksi.

Tärkein lainsäädäntö käsitellään aakkosjärjestyksessä. Rikoslaissa määritellään toimet, jos lakia rikotaan. Liitteessä 2 on lueteltu voimassa oleva lainsäädäntö, johon VAHTI-ohjeistus viittaa.

3 Lainsäädäntö kattaa kunkin käsiteltävän lain kohdalla kokonaisuuden laki, sen asetukset ja määräykset ja muut ohjeet.

2.1.1 Arkistolaki

Arkistolaki säätelee asiakirjojen laatimista, säilyttämistä ja käyttöä. Arkistolaki määrää esimerkiksi mitkä asiakirjat ovat säilytettävä (arkistoitava) pysyvästi. Keskeisiä käsitteitä ovat käytettävyys, eheys, luottamuksellisuus, tietosuoja ja tietoaineiston hävittäminen. Arkistolaitos ohjaa määräyksillään arkistolain toteutumista.

2.1.2 Henkilötietolaki

Henkilötietolaki säätää yksityisyyden suojan turvaamista koskevat menettelyt henkilötietoja käsiteltäessä. Keskeisiä käsitteitä ovat henkilötieto ja sen määrittely, henkilötietorekisteri ja sen syntyminen ja hyvä tiedonhallintatapa.

2.1.3 Laki kansainvälisistä tietoturvavelvoitteista

Laki säätelee esimerkiksi menettelyjä henkilön tai yhteisön luotettavuuden toteamiseksi kansainvälisissä yhteyksissä. Lisäksi laki määrittelee uudelleen tai tarkentaa julkisuuslaissa (621/1999) määriteltyjä tiedon käsittelytapoja kansainvälisen toiminnan mukaisiksi.

2.1.4 Laki sähköisestä asioinnista viranomaistoiminnassa

Laki määrittelee tarvittavat menettelyt sähköisen viestin käsittelyyn, kun viranomainen on järjestänyt sähköisen asioinnin mahdollisuuden. Keskeisiä käsitteitä ovat sähköinen viesti, määräajat, kirjaaminen, saavutettavuus, arkistointi.

2.1.5 Laki turvallisuusselvityksistä

Laki täydentää turvallisuusselvityksiin liittyen henkilön yksityisyyden suojaa ja henkilötietojen suojaa koskevia lakeja. Näin mahdollistetaan turvallisuusselvitysten tekeminen. Turvallisuusselvitys voidaan tehdä perusmuotoisena, laajana tai suppeana. Laissa määritellään missä tilanteissa erimuotoisia selvityksiä tehdään.

2.1.6 Laki valtion talousarviosta

Valtion hallinnon toimintaa ohjataan tulosohjausperusteisesti ja näin myös tietoturvatoimintaa. Lain keskeisiä käsitteitä ovat tiedon eheys ja luotettavuus, riskienhallinta ja sisäinen valvonta. Ohjaava viranomainen on Valtiokonttori.

2.1.7 Laki viranomaisen toiminnan julkisuudesta

Valtionhallinnon asiakirjat ovat pääsääntöisesti julkisia. Julkisuuslaki säätää perusteet pääsäännöstä poikkeamiseen määrittelemällä erityissuojattavat tietoaineistot. Erityissuojattavat tietoaineistot luokitellaan käsittely- (neljä luokkaa) tai turvallisuusluokkiin (neljä luokkaa). Asetetut luokat määrittelevät tietoaineiston käsittely- ja suojausvaatimukset ja suoja-ajan. Julkisuuslaki määrittelee hyvän tiedonhallintatavan valtionhallinnossa. Hyvä tiedonhallintatapa on hallittua, organisoitua ja ohjeistettua toimintaa, joka takaa halutun tietoturvatason syntymisen.

Lakiin liittyvä asetus tietoturvallisuudesta ja hyvästä tiedonhallintatavasta valtion-hallinnosta on uudistettavana.

2.1.8 Laki yksityisyyden suojasta työelämässä

Laki täsmentää rajanvetoa kansalaisen perusoikeuksien ja työntekijän oikeuksien välillä. Erityinen huomio on henkilötietojen käsittelyllä ja viestinnän suojalla suhteessa työnantajan velvollisuuteen toteuttaa ja valvoa tietoturvallisuutta. Valtionhallinnon henkilökunnan asemaa täsmentää vielä virkamieslaki.

2.1.9 Perustuslaki

Suomen perustuslain perusoikeussäännökset määrittelevät yksityiselämän suojan, sananvapauden ja julkisuuden. Perustuslakia tarkentavia lakeja ovat esimerkiksi henkilötietolaki, julkisuuslaki, laki yksityisyyden suojasta työelämässä ja sähköisen viestinnän tietosuojalaki.

2.1.10 Sähköisen viestinnän tietosuojalaki

Laki määrittelee sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan yleisissä viestintäverkoissa ja palveluissa. Keskeisiä käsitteitä ovat tunnistetieto, paikkatieto ja viestinnän tietoturva. Viestintävirasto on ohjaava viranomainen, joka täydentää lakia määräyksillään.

2.1.11 Valmiuslaki

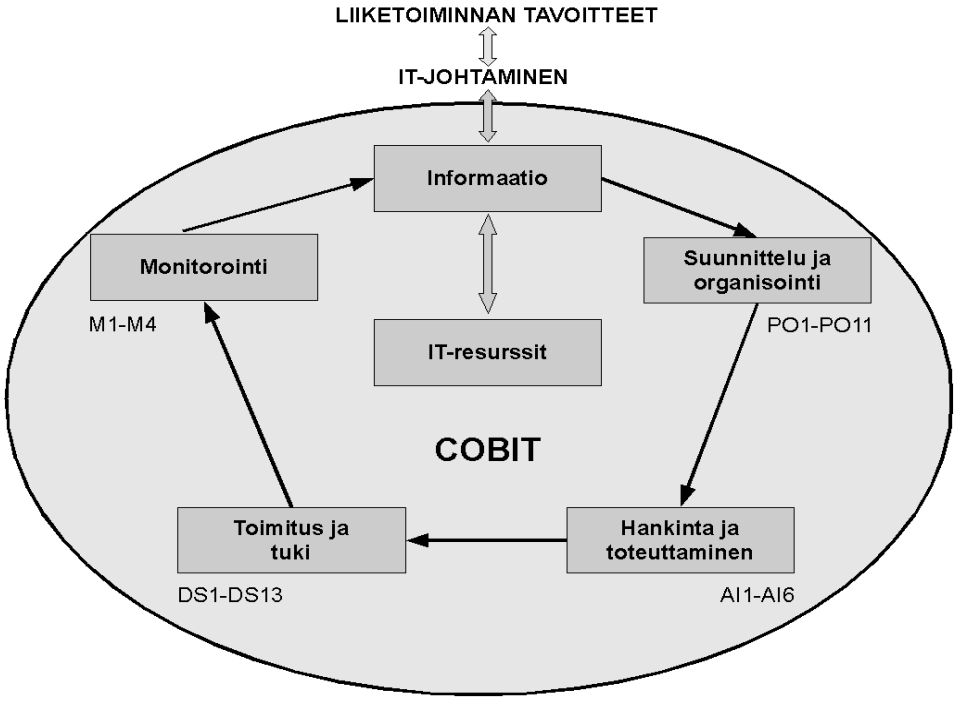
Laki määrittelee toimet poikkeusoloissa maan toiminnan ja perusoikeuksien turvaamiseksi. Keskeinen käsite on valmiussuunnitelma. Valtion viranomaisten on varauduttava poikkeusoloihin etukäteisvalmisteluin. Varautumista johtaa valtioneuvosto ja kukin ministeriö omalla hallinnonalallaan.

2.2 Standardeista ja suosituksista

Seuraavassa on lyhyet esittelyt tietoturvallisuuden hallintajärjestelmää käsittelevistä ja tietoturvatoimintaan vaikuttavista standardeista. Pääpaino palautejärjestelmään vaikuttavissa kohdissa.

2.2.1 COBIT

COBIT (Control Objectives for Information and related Technology) on laaja organisaation tietohallinnon, - tietotekniikan ja -järjestelmien hallintaan kehitetty valvontamalli. Kehittäjäorganisaatiot ovat ITGI (IT Governance Institute) ja ISACA (Information Systems Audit and Control Association). COBIT on liiketoimintalähtöinen malli, jossa on neljä hallinnollista aluetta (domains, lyhenteet PO, AI, DS ja M), jotka kattavat kaikkiaan 34 prosessia. COBIT sisältää menettelyn organisaation tietohallinnon ja -tekniikan toteuttamiseksi liiketoimintatavoitteisiin tukeutuen. Toteutumisen tasoa mitataan kypsyysmallilla, jonka selvittämiseksi on annettu mittaristo. Kuvassa 3 on havainnollistettu COBIT-prosessi.



Kuva 3: COBIT-prosessi

2.2.2 Common Criteria

Common Criteria (CC) on yhdistelmä kolmesta eri standardista: eurooppalainen ITSEC, kanadalainen CTCPEC ja yhdysvaltalainen TCSEC (niin sanottu Orange Book). ISO/IEC on muodostanut CC:n pohjalta standardit ISO/IEC 15408-1-3:2005, mutta alkuperäisen CC:n kehitys jatkuu ja sitä julkaistaan erillisinä suosituksina.[4]

CC määrittelee tavat, jolla 1) tietojärjestelmien käyttäjät määrittelevät tietoturva-tarpeensa ja -vaatimuksensa, 2) ohjelmistojen ja järjestelmien tekijät voivat toteuttaa tietoturvatoiminteet ja osoittaa tietoturvavaatimusten täyttyvän ja 3) testauksessa voidaan todistaa tietoturvavaatimusten täyttyvän. CC:n käyttö on suunniteltu niin, että vain hyväksytty testausorganisaatio voi arvioida järjestelmän tietoturvatason. Arviointi-menettely on kallis, mutta CC:n vaatimuslistoja voi hyödyntää omia järjestelmiä arvioitaessa. Taulukossa 1 on CC:n peruskäsitteet.

4 http://www.niap-ccevs.org/cc-scheme/cc_docs/

CC lyhenne	CC nimi	kommentti
TOE	Target Of Evaluation	arvioinnin kohde
PP	Protection Profile	käyttäjän vaatimukset tietoturvalle
SFR	Security Function Requirement	tuotteen yksittäinen tietoturvaominaisuus
ST	Security Target	TOEn tietoturvaominaisuudet
SAR	Security Assurance Requirement	kehitys- ja arviointivaiheen vaatimukset
EAL	Evaluation Assurance Level	tietoturvatasot (1-7)

Taulukko 1: Common Critera -käsitteet

2.2.3 ISO/IEC 27000 -sarja

ISO/IEC 27000 -sarja[5] on tietoturvallisuuden hallintaan suunnattu standardien kokoelma. Sarjan taustalla on British Standards Instituten BS 7799 -standardi, jonka ensimmäinen versio on vuodelta 1995.[6] Vuonna 1999 standardi jaettiin kahteen osaan[7]: Ensimmäisestä osasta muodostui ISO/IEC 17799 -standardi vuonna 2000 ja se uudelleen nimettiin standardiksi ISO/IEC 27002 vuonna 2005. Toisesta osasta muodostui ISO/IEC-standardi ISO/IEC 27001 vuonna 2005. Näyttää siltä, että standardin BS 7799 kolmas versio[8] otettaneen mukaan ISO/IEC-standardiin ISO/IEC 27005 vuonna 2009.

ISO/IEC 27001 määrittelee hallintajärjestelmälle vaatimukset ja ISO/IEC 27002 parhaat käytänteet (best practices) tietoturvallisuuden hallinnan toteuttamiseksi. Määrittelyissä on kuvattu hallintaprosesseja (clauses), kontrollivaatimuksia ja kontrolleja (control objectives and controls), mutta niiden toteuttamisen onnistumisen tasoa eli mittaamista ei ole kuvattu. Hallintaprosesseja on kaikkiaan 11. Niille on määritelty 39 kontrol-

5 http://www.27000.org/

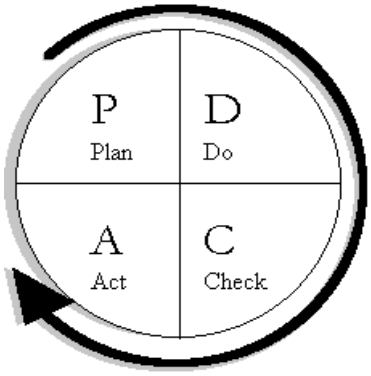
6 BS 7799:1995 Code of practice for information security management

7 BS 7799-1:1999 Code of practice for information security management ja BS 7799-2:1999 Information security management systems - Requirements

8 BS 7799-3:2006 Guidelines for information security risk management

litavoitetta. Tavoitteiden toteutumista seurataan yhteensä 131 kontrollilla. Huomionarvoista on se, että ISO/IEC 27001 ei määrittele riskienhallintaa (riskianalyysi) osaksi hallintajärjestelmää vaan hallintajärjestelmälle tavoitteet antavaksi toiminnaksi. Tästä syystä ISO/IEC 27002 ei aseta riskienhallinnalle tavoitteita ja kontrolleja.

Palautejärjestelmän kannalta olennaista on standardin ISO/IEC 27001 esittämä prosessimalli hallintajärjestelmän kehittämiseksi, toteuttamiseksi ja ylläpitämiseksi: Plan-Do-Check-Act[9] eli PDCA-malli (Kuva 4). Malli on yhteensopiva COBIT-prosessin kanssa.



Kuva 4: Plan-Do-Check-Act -prosessimalli

2.2.4 ISO/IEC 21827 SSE-CMM

Systems Security Engineering Capability Maturity Model (SSE-CMM)[10] on alunperin ISSEA:n (The International Systems Security Engineering Association) tekemä suositus tietoturvan kehittämiseksi ja ylläpitämiseksi. Suositus on otettu ISO/IEC standardiksi 21827, jonka uusin versio on vuodelta 2007.

SSE-CMM sisältää nimensä mukaisesti kypsyystasoajattelun tietoturvan kehittämisessä. Mallissa on tietoturvatoiminnalle 5 kypsyystasoa (on myös 0-taso, jossa tietoturvatoimia ei ole toteutettu). Kypsyystason selvittämiseksi ja toteuttamiseksi on kaikkiaan 22 prosessialuetta, joissa on yhteensä 129 peruskäytäntöä (base practises).

9 Esimerkiksi suunnittele-toteuta-tarkista-toimi: 1930-luvulla Walter Shewhartin kehittämä malli

10 http://www.sse-cmm.org/index.html

Pääjako on järjestelmien tietoturvaprosessit ja projekti- ja organisaatioprosessit. Malli siis huomioi sekä tuotekehityksen että organisaation toiminnan turvallisuuden. Mallissa yleisiä käytäntöjä (generic practices), jotka koskeva kaikkia prosessialueita. Yleiset käytännöt on ryhmitelty yleisiin ominaisuuksiin (12 common features), jotka jakautuvat eri kypsyystasoille.

Organisaation tietoturvatoiminnan kypsyystason arviointia varten on olemassa SSE-CMM Appraisal Method (SSAM). Arviointimenetelmä on tarkoitettu arviointiorganisaation toteutettavaksi, mutta sitä voi käyttää myös itsearviointiin.

SSE-CMM sisältää metriikan määrittelyprosessin, joka jakautuu prosessi- ja tietoturvametriikoiden määrittelyiksi. Mallissa toteutettu ominaisuuksien ja käytäntöjen jako johtaa siihen, että mittareita syntyy rajallinen määrä ja hyödyttävä monen prosessialueen tason selvittämistä.

2.2.5 NIST SP 800 -sarja

Vaikka NIST on yhdysvaltalainen organisaatio, sen tekemät dokumentit[11] on syytä ottaa huomioon tietoturvan toteuttamisessa ja toteutumisen todistamisessa. NIST:n tietoturvaan suunnattu SP 800 -sarjan (SP = Special Publications) dokumentit ovat, menettelyohjeita Yhdysvaltojen lainsäädännön mukaisten, kuten FIPS-vaatimusten, toteuttamiseksi. Tämän työn kannalta olennaisimmat NIST SP -dokumentit ovat NIST SP 800-26, SP 800-53 ja NIST 800-55. Niissä määritellään hallintaprosessit ja kontrollit FIPS-vaatimusten toteuttamiseksi. Peruskäsite on FIPS-vaatimuksissa määritelty käsite vaikutus (impact), joka on jaettu kolmeen vaikutusluokkaan: matala, keskitaso, korkea (low, medium, high). Vaikutusluokka kuvaa tietojärjestelmän kriittisyyttä tietoturvatapahtuman sattuessa.

NIST SP 800-26 sisältää auditointimallin, jolla tietoturvan toteutus ja taso selvitetään. Tietoturvan tasoja on 5 (vertaa SSE-CMM kypsyystasot). Dokumentissa on auditointi-lomake jokaiselle tietoturvatoiminnan osa-alueelle, jotka on määritelty dokumentissa NIST SP 800-53.

11 http://csrc.nist.gov/publications/

NIST SP 800-53 määrittelee tietoturvatoiminnan kolme pääluokkaa (hallinnallinen, toiminnallinen ja tekninen) ja niissä on kaikkiaan 17 tietoturvatoiminnan osa-aluetta, jolle on määritelty kontrolleja ja kontrollilaajennuksia, joita on toteutettava vaikutus-luokan mukaan. Esimerkiksi pääsynvalvonnalla (access control) on 20 kontrollia ja 19 laajennusta.

NIST SP 800-53A sisältää tietoturvakontrollien arviointiohjeen. Esimerkiksi edellä mainitun pääsynvalvonnan kontrolleille on määritelty kaikkiaan 152 tarkistuskohtaa.

NIST SP 800-55 määrittelee tietoturvametriikan käsitteen, metriikoiden kehitysprosessin ja mallimetriikoita 16 tietoturvan osa-alueelle. On syytä ottaa huomioon, että osa-alueita on määritelty kaikkiaan 17 ja osa eri nimillä kuin tässä dokumentissa. Olennainen piirre metriikan määrittelyissä on se, että metriikan täytyy muuttua kun tietoturvatoiminnan kypsyystaso muuttuu

2.2.6 Muita suosituksia

Information Security Management Maturity Model -konsortio[12] (ISM3 Consortium) on kehittänyt nimeään kantavan mallin tietoturvallisuuden hallinnan kehittämiseksi. Malli on yhteensopiva standardin ISO/IEC 27001 ja sen prosessimallin kanssa. ISM3 kuvaa 5 eri tasoista (verrattavissa SSE-CMM kypsyystasoihin) hallintajärjestelmän konfiguraatiota kaikkiaan 45 eri toiminnolla. Kaikki toiminnot on toteutettava ylimmän tason saavuttamiseksi ja tarkistusta varten on määritelty mittarit.

Information Security Forum[13] (ISF) on julkaisut oman standardinsa (The Standard of Good Practice for Information Security), jonka kehitys seuraa esimerkiksi COBIT- ja ISO/IEC 27002 -standardia. Nimensä mukaisesti standardi on käytännönläheinen ja antaa yksiselitteisiä ohjeita esimerkiksi tietoturvapolitiikan tekemiseksi tai verkko-palvelun suojaamiseksi.

12 http://www.ism3.com/

13 http://www.securityforum.org/

Suomessa merkittävän panoksen tietoturvallisuuden hallinnalle antavat Huoltovarmuuskeskus[14] (HVK) ja Puolustustaloudellinen suunnittelukunta (PTS), jonka sihteeristönä HVK toimii. Organisaatiot tekevät uhka-analyyseja huoltovarmuudella ja julkaisevat ohjeita valtionhallinnolle ja yrityksille uhkien hallitsemiseksi. HVK:n toiminta perustuu lakiin huoltovarmuuden turvaamisesta (1390/1992) ja sen tehtävä on huoltovarmuuden ylläpitämisen ja kehittämisen suunnittelu ja operatiivinen toiminta. HVK/PTS-julkaisuista mainittakoon esimerkiksi Tietotekniikan turvallisuus ja toiminnan varmistaminen (PTS 1/2002) ja Viestintäverkkojen ja viestintäpalveluiden varmistaminen (PTS 2/2005).

Saksan tietoturvaviranomainen Bundesamt für Sicherheit in der Informationstechnik (BSI) on tehnyt useita standardeja ja ohjeita[15] tietoturvallisuuden hallintaan ja toteuttamiseen. BSI Standard 100-1 Information Security Management Systems on yhteensopiva ISO/IEC 27001 standardin kanssa ja kattaa siis hallintajärjestelmän toteuttamisen. BSI Standard 100-2 IT-Grundschutz Methodology on puolestaan tietoturvatoiminnan toteuttamiseen suuntautunut ja siten lähellä ISO/IEC 27002 standardia. Kolmas BSI standardi (100-3) on riskianalyysin toteuttamista varten. Ohjeista mainittakoon IT Baseline Protection Manual, joka on kattava ohjeisto organisaation tietoturvan toteuttamiseksi.

2.2.7 Yhteenveto standardeista ja suosituksista

Vaikka standardit ja suositukset ovat syntyneet eri lähtökohdista (kontrollien -, prosessien -, riskien- tai tuotekehityksen hallinta), niissä on yhteisiä piirteitä. Prosessimalli on poikkeuksetta esillä ja prosessin ohjausmalli on yleensä unohdettu: vain COBIT sisältää selkeästi feedback-toiminteen. Terminologian erilaisuudesta huolimatta on kaikissa edellä käsitellyissä standardeissa ja suosituksissa tavoitteen asettaminen tärkeää: kaikille toimille pitää olla perustelu ja tavoite. Ilman tavoitteita mittaaminen on turhaa.

14 http://www.huoltovarmuus.fi/

15 http://www.bsi.bund.de/english/publications/index.htm

Standardeissa ja suosituksissa ovat esimerkiksi tietoturvatoiminnan osa-alueet jaoteltu eri lailla ja eri termein, mutta niiden voidaan todeta kattavan kaiken toiminnan (Broderick, 2005). Liitteessä 3 on yhteenvetotaulukko eräiden standardien ja suositusten tietoturvan ja tietoturvatoiminnan osa-alueista.

2.3 VAHTI-ohjeistus

Kuten alkulauseessa on todettu, valtionhallinnon tietoturvallisuustoimintaa ohjaa VAHTI-ohjeistus. Ohjeistuksessa on otettu huomioon lakien, standardien ja sopimusten asettamat vaatimukset tietoturvan toteuttamiseksi. VAHTI-ohjeistus kattaa turvallisuuden hallinnan (esimerkiksi VAHTI 3/3003), turvallisuustoiminnan (esimerkiksi VAHTI 1/2001) ja teknisen tietoturvan (esimerkiksi VAHTI 2/2001). Tässä luvussa käydään läpi tietoturvallisuuden hallinnan, kehityksen ja palautejärjestelmän kannalta olennaisin ohjeistus.

VAHTI-ohjeissa määritellään tietoturvatoiminta kahdeksaan osa-alueeseen, joita hallintajärjestelmällä ohjataan ja joiden tehokkuutta palautejärjestelmällä mitataan. Näitä ovat hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoaineistoturvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmisto-turvallisuus ja käyttöturvallisuus.

VAHTI 1/2001 Valtion viranomaisen tieturvallisuustyön yleisohje

VAHTI 1/2001 määrittelee valtionhallinnon tietoturvallisuuden hallintajärjestelmän, joka käsitellään erikseen seuraavassa luvussa. Muusta sisällöstä voi lyhyesti todeta: Valtiovarainministeriö ohjaa valtionhallinnon turvallisuutta. VAHTI koordinoi, kehittää, yhteensovittaa, ylläpitää tietoturvatavoitteita, toiminta- ja organisointilinjauksia, sekä määräyksiä, ohjeita ja suosituksia. Suunnittelu ja kehittäminen edellyttävät, että hallintaa ja seurantaa varten täytyy olla ajantasainen tietoturvasuunnitelma, jossa määritellään tietoturvatoiminnan tavoitetasot. Seurannan täytyy olla jatkuvaa ja aktiivista ja valvonnan kohdennettu siten, että toiminnan tehokkuus tulee esille.

Ministeriöillä on tietoturvallisuuden tulosohjausvastuu. Tietoturvatoiminnan ohjaus konkretisoituu tietoturvallisuuspolitiikassa ja -strategiassa. Tarkastuksen ja valvonnan on kohdistuttava tietoturvatoimenpiteiden ja tulosten saavutuksien todentamiseen.

Tämän ohjeen uudistamistyö on juuri meneillään.

VAHTI 3/2003 Tietoturvallisuuden hallintajärjestelmän arviointisuositus

VAHTI 3/2003 määrittelee ja tarkentaa valtionhallinnon tietoturvallisuuden hallinta-järjestelmää. Hallintajärjestelmän arvioinnin ja palautejärjestelmän kannalta on otettava huomioon seuraavaa: Tietoturvallisuuden kehittämiseksi on oltava jatkuvaluonteista arviointia. Jatkuvaluonteisen arvioinnin periaate sopii tulosohjausmalliin, jos tulosohjaus perustuu jatkuvaan auditointiin. Osa arvioinneista voi ja täytyy olla itsearviointeja. Arvioinnit on toteutettava niin, että arviointien taso saadaan henkilöriippumattomaksi. Auditointeihin perustuvaa arviointia voidaan täydentää mittareihin ja mittaamiseen tukeutuvalla jatkuvalla parantamisella ja vaikut-tavuusarvioinnilla.

Jotta palautejärjestelmällä olisi vaikutusta, johdon on määriteltävä mitä arviointitulosten seurauksena tapahtuu. Johdon on lisäksi järjestettävä organisaatiossaan riittävät valmiudet ja edellytykset onnistuneeseen arviointi- ja mittaamistoimintaan. Näitä ovat esimerkiksi resurssit ja valtuudet.

Arviointia ja mittaamista varten täyttyy olla mittareita seuraaville alueilla: laatu, tulosohjaus, tietoturvan taso, hallinnon taso. Standardien käyttö mitattavuuden edellytys. Standardien avulla saadaan myös tarvittaessa benchmark-vertailua organisaatioiden välillä.

Tietoturvallisuuden perustehtävä on käytettävyyden, eheyden ja luottamuksellisuuden takaaminen. Arviointi- ja mittausperusteet ovat siis perustehtävän onnistumisen toteaminen, jota ilmentää hallinnan ja tietoturvatoiminnan tehokkuus ja vaikuttavuus. Arvioinnilla ja mittaamisella halutaan seuraavaa tietoa: tavoitteiden saavuttamien,

tarkoituksenmukaisuus, velvoitteiden mukaisuus, taloudellisuus, vaikuttavuus, tehokkuus, omaisuuden turvaaminen.

VAHTI 7/2003 Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa

Organisaation johto vastaa tietoriskien hallinnasta, joka on päätöksentekotoimintaa, jonka tavoitteena on taata toiminnan jatkuvuus. Organisaation on tiedettävä toimintansa (tietonsa) vaikutus muihin organisaatioihin sekä oma riippuvuutensa muiden organisaatioiden toiminnasta (tiedosta).

Organisaation tapa käsitellä tietoa kuvaa sen kulttuuria ja tapaa toimia (kypsyystasoa). Organisaation kannalta on tärkeää, että tiedot 1) ovat oikein ja ajan tasalla, 2) ovat aina oikeiden henkilöiden saatavilla ja 3) eivät joudu vääriin käsiin.

Ohjeessa kuvataan riskien arviointi osana riskienhallintaa. Arviointiin liittyvät lainsäädännön vaatimukset, organisointi ja toteutustapa. Kun arvioinnissa on valittu toimenpiteet ja niiden mukainen toteutus tehty, seuranta ja palaute on järjestettävä toimien tehokkuuden selvittämiseksi ja kehittämisen toteuttamiseksi. Seuranta ja palaute edellyttävät mittaamista ja palautekanavan järjestämistä.

VAHTI 2/2004 Tietoturvallisuus ja tulosohjaus

Tietoturvallisuuden merkitys on kuvattu seuraavasti: ”Toiminnan häiriintyminen tai suoranainen lamaantuminen, tietovuodot ja erilaiset muut häiriötekijät vievät organisaation uskottavuutta ja johtavat vakaviin ongelmiin, jotka estävät tuloksellisen toiminnan.” Tietoturvallisuuden mittaaminen tulosohjauksen kannalta on turvallisuuskulttuurin mittaamista, johon kulttuuriin kuuluvat: turvallisuustietoisuus, vastuullisuus, vastatoimet, eettisyys ja demokratian tukeminen, riskien arviointi, turvallisuuden suunnittelu ja toimeenpano, turvallisuuden hallinta, uudelleen arviointi.

Riskienhallinta ja tietoturvallisuuden arviointi osana kehittämistä ja laadun parantamista toteuttavat tulosohjausmallia. Tähän liittyvän seurannan ja arvioinnin oltava systemaattista, jatkuvaa ja pysyvää toimintaa.

Ohjeessa on esitetty myös tuloskorttimallin (balanced scorecard) käyttöä tietoturvan tuloksellisuuden arviointiin. Esittelyssä on annettu myös palautejärjestelmän kannalta pätevät määrittelyt tiedolle: tiedon tulee olla relevanttia, olennaiseen keskittyvää, ristiriidatonta ja loogista ja analyysiin soveltuvaa.

Valtionvarainministeriö on määritellyt Tulosohjauskäsikirjassaan (VM 2/2005) tuloksellisuuden peruskriteerit seuraavasti: yhteiskunnallinen vaikuttavuus, toiminnallinen tehokkuus, tuotokset ja laadunhallinta ja henkisten voimavarojen hallinta. Tietoturvatoiminnalta edellytetään samoja ominaisuuksia.

VAHTI 6/2006 Tietoturvatavoitteiden asettaminen ja mittaaminen

Normisto antaa tietoturvatoiminnalle minimi- ja tavoitetasot, joiden toteutumista seurattava (mitattava). Tässä ohjeessa tavoitteiden asettaminen ja mittaaminen sidotaan tulosohjaukseen. Tavoitteita asetetaan useassa tasossa (ministeriö, virasto) ja usealle aikavälille (vuositaso, kehitysohjelmat). Tavoitteiden asettaminen tapahtuu tietoturvallisuuden hallintajärjestelmää kehitettäessä, joka järjestelmä normiohjauksen vaatimusten mukaisesti ohjaa tietoturvatoimintaa.

Hallintajärjestelmän kehityksen viitemalliksi on otettu kypsyysmalli (SSE-CMM), jonka kypsyystasoihin (1-5) tavoitteet ja niiden mittaaminen asettuvat.

Hallintajärjestelmälle määritellään haluttu kypsyystaso ja tason saavuttamiseksi kehityssuunnitelma. Saavutetun kypsyystason mittaaminen perustuu sekä laadulliseen (kvalitatiiviseen) että määrälliseen (kvantitatiiviseen) mittaamiseen. Edellistä edustavat auditoinnit ja jälkimmäistä teknisten järjestelmien tuottama tieto. Mittaustulokset kertovat operatiivisen toiminnan tason ja niistä saadaan tuki ohjauspäätöksille. Vertailu tehdään normatiiviseen käytäntöön.

Raportoinnissa organisaatioiden tarpeet määräävät sisällön, mutta tavoite on yhteinen: toiminnan parantaminen.

Ohjeessa esitetään seuraavat arviointi- ja mittausmenetelmät: itsearviointi, ulkoinen arviointi, benchmarking, laadullinen ja määrällinen mittaaminen. Mittaamisen on oltava prosessimuotoista eli jatkuvaa.

VAHTI 8/2006 Tietoturvallisuuden arviointi valtionhallinnossa

Kun VAHTI 3/2003 keskittyy hallintajärjestelmän arviointiin, niin tässä suosituksessa keskitytään tietoturvatoiminnan arviointiin. Suosituksessa esitetään arvioinnin pohjaksi sopivia standardeja (ITIL, ISO/IEC 27001, COBIT, SSE-CMM) sekä tietoturvatoimintaan vaikuttavan lainsäädäntö että VAHTI-ohjeistus Jokaisesta niistä saa arviointia auttavia tarkistuslistoja joko suoraan tai välillisesti. Esimerkkejä annetaan SSE-CMM- ja ITIL-pohjaisesta lähestymistavasta.

Tietoturvatoiminnan arviointi voidaan tehdä seuraavalla jaolla: tekninen tietoturvallisuus, tietoturvakulttuuri, johtamisjärjestelmä ja menettelytavat ja tietoturvapoikkeamat. Suosituksessa esitellään myös laaja arviointimalli perustuen laajennettuun tietoturvatoiminnan osa-aluejakoon. Perinteistä kahdeksaa osa-aluetta on laajennettu ulkoistamisella, etäkäytöllä, järjestelmäkehityksellä ja tietoturvapoikkeamien käsittelyllä sekä osto-palveluna hankituilla palveluilla. Tuloksena on laaja tarkistuskohteiden luettelo.

Yhteenvetona voi todeta, että VAHTI-ohjeistus siirtää normiohjauksen vaatimukset hallintajärjestelmän avulla tietoturvallisuustoiminnan ohjaukseksi. VAHTI-ohjeistus kuvaa hallintajärjestelmän toiminnan ja sen asettamat vaatimukset tietoturvan toteuttamiseksi eri organisaatiotasoilla. Hallintaa tuetaan valituilla standardeilla (ISO/IEC 27001, SSE-CMM) ja toteutumisen arvioimiseksi on koottu kattavat tarkistusluettelot.

3 Tietoturvallisuuden hallintajärjestelmä

Käsittelen tässä luvussa valtionhallinnon tietoturvallisuuden hallintajärjestelmän VAHTI 1/2001 ja VAHTI 3/2003 mukaisesti. Hallintajärjestelmä koostuu kymmenestä osasta, joiden kunkin osan lyhyessä esittelyssä tarkastellaan erityisesti palaute-järjestelmälle oleellisia kohtia.

3.1 Tietoturvallisuuspolitiikka ja toimintaperiaatteet

Organisaation ylin johto määrittelee tietoturvapolitiikalla tietoturvaperiaatteet ja toimintatavat. Tietoturvapolitiikka on myös tulosohjauksen väline ja siinä määritellään toimintalähtöiset tekniikasta riippumattomat vaatimukset esimerkiksi organisoinnille, vastuille, toteutustavoille, ohjeistukselle ja koulutukselle.

3.2 Tietoturvallisuusstrategia

Tietoturvallisuusstrategia on suunnitelma, jolla pyritään tavoiteltuun päämäärään. Tietoturvallisuusstrategissa täytyy ottaa huomioon tietohallintostrategian asettamat tavoitteet ja vaatimukset tietoturvatoiminnalle muuttuvassa toimintaympäristössä. Kyseiset strategiat ovat sidoksissa toisiinsa niin, että ne yleensä esitetään yhdessä. Koska tietohallintostrategia on yleensä liiketoimintatarpeiden ohjaamaa, tieto-turvallisuusstrategia tulee näin myös liiketoimintaohjaukseen.

3.3 Riskianalyysi

Riskianalyysi on tärkeä osa tietoturvariskien hallintaa. Riskienhallinnan ja riskianalyysin tehtävä on tunnistaa organisaation toimintaa kohdistuvat uhkat, uhkia vähentävät toimenpiteet ja jos uhka toteutuu, niin sen seuraukset. Riskienhallinnan menettelyistä sovitaan riskienhallintapolitiikassa, jossa määritellään esimerkiksi johdolle raportoitavat asiat. Riskianalyysiprosessi on jatkuvaa tietoturvatoimintaa muuttuvassa ympäristössä.

3.4 Tietoturvallisuussuunnitelma- ja ohjeet

Suunnitelmilla ohjataan tietoturvatoimintaa käytännössä ja ne tehdään kaikille organisaatiotasoille. Suunnitelmiin kuuluvat käytännön toimintaohjeet tietoturvan ylläpitämiseksi ja normaaliolojen järjestelmäkohtaiset toipumissuunnitelmat, jotka on testattu. Suunnitelmaan sisällytetään kaikki toimenpiteet, joilla tavanomainen toiminta ja sen tietoturva ylläpidetään (PTS 1/2002). Suunnitelmat tehdään kaikille tietoturvan kahdeksalle osa-alueelle.

3.5 Jatkuvuus- ja toipumissuunnitelma

Organisaatioiden on kyettävä toimimaan poikkeusoloissa. Sitä varten niillä täytyy olla jatkuvuus- ja toipumissuunnitelmat. Nämä suunnitelmat ohjeistavat valmiuslain (1080/1991) voimassaolon aikaista toimintaa. Jatkuvuussuunnitelma määrittelee keinot ja organisoinnin poikkeusolojen aikaiseen toimintaan. Toipumissuunnitelma määrittelee keinot toiminnan keskeytyksen minimoimiseksi ja palauttamiseksi normaaliksi. Olennaisia määriteltäviä asioita ovat keskeiset toiminnot ja järjestelmät, järjestelmien riippuvuudet, varajärjestelmät ja häiriöiden vaikutus. Suunnitelmia täytyy kehittää säännöllisesti.

3.6 Valmiussuunnitelma

Valmiussuunnitelmalla varaudutaan poikkeusolojen toimintaan. Suunnitelmassa huomioidaan esimerkiksi uhkakuvat, valtiovallan vaatimukset toiminnalle,

tietojenkäsittelyn merkitys. Suunnitelman tehtävä on sopeuttaa tietojenkäsittely kriisitilanteen sallimalle tasolle. Tämä tapahtuu halutun palvelun varmistamisella tai korvaamisella etukäteen sovitulla tavalla. Valmiussuunnitelman kattavuus riippuu organisaation tärkeysluokasta. Valtionhallinnossa luokittelun tekee VAHTI (PTS 1/2002).

3.7 Tietoturvallisuuden tulosohjaus

Valtionhallinnon periaatepäätöksen mukaisesti kaikkea toimintaa ohjataan tulosohjausmallin avulla, niin myös tietoturvatoimintaa. Kukin ministeriö vastaa oman hallinnonalansa tietoturvatoiminnan tulosohjauksesta. Tulosohjaus tapahtuu tietoturvallisuuspolitiikan ja -strategian avulla. Ministeriön vastuulla on tietoturvatoiminnan tulosten tarkastaminen ja valvominen. Jokainen organisaatiotaso on velvollinen huolehtimaan tietoturvallisuuden toteutumisesta omassa toiminnassaan.

Olennainen dokumentti on tulossopimus, jossa määritellään seurantavastuut ja raportointi ylimmälle johdolle. Tavoitteita asetettaessa on määritelty seurattavat mittarit.

3.8 Tietoturvallisuuden toteutustapa, organisointi ja vastuut

Tietoturvavastuut on vietävä organisaatio- ja henkilötasolle johtosääntöihin, työjärjestyksiin ja toimenkuviin ja samalla määritellään tarvittavat osaamisprofiilit. Turvallisuuden kehittäminen ja ylläpito on mahdollista vain, jos toiminnasta vastuussa olevat henkilöt tuntevat riskit ja riippuvuudet (PTS 1/2002). Organisoinnissa on huomioitava se, että vastuut eivät jää yhden henkilön varaan. Lisäksi on huolehdittavat siitä, että eri organisaatiot ja henkilöt tekevät yhteistyötä. Tietoturvavastuiden määrittelyissä olennainen osa on raportointivastuut. Vastuiden ja organisoinnin tulee seurata toiminnan muutoksia.

3.9 Vuosisuunnitelmat ja budjetit

Tulosohjaus edellyttää suunnitelmallisuutta. Tietoturvatoiminnan kustannukset (toimintamenot) on suunniteltava ja suunnitelmien on perustuttava toiminnan

tavoitteisiin. Suunnitelmat tehdään vuositasolla ja kirjataan budjettiin. Suunnitelmien toteutumista on seurattava.

3.10 Raportointi

Raportointivastuut määritellään esimerkiksi tietoturvan organisoinnissa ja tulossopimuksessa. Raportointi kattaa jokapäiväisen tietoturvatoiminnan ja toiminnan tuloksellisuuden. Jokapäiväisen toiminnan raportteja ovat esimerkiksi virustorjunnan, verkkohyökkäyksien tai käyttökatkoksien raportit. Toiminnan tuloksellisuuden raportit kuvaavat tietoturvan tilannekuvaa. Raportoinnissa on otettava huomioon eri organisaatioiden ja organisaatiotasojen tarpeet.

3.11 Yhteenveto hallintajärjestelmästä

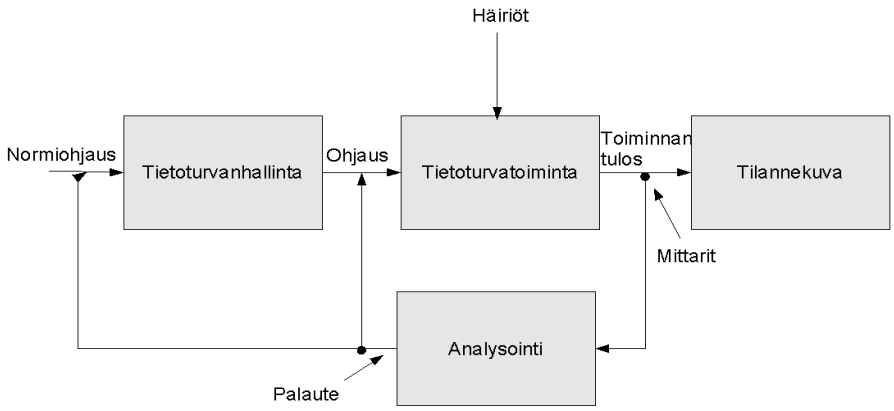
Valtionhallinnon tietoturvallisuuden hallintajärjestelmä on toimiva kokonaisuus, joka kattavasti määrittelee tietoturvatoiminnan perusteet ja tavoitteet. Kokonaisuuden perusteella on määriteltävissä palautejärjestelmän kannalta olennaiset asiat: tietoturva-toiminnan tehokkuus verrattuna hallinnollisiin menettelyihin ja hallinnollisten toimien vaikuttavuus organisaatioiden tietoturvatietämyksen kehitykseen.

4 Tietoturvallisuuden hallinta: palautejärjestelmä

Käsittelen tässä luvussa tietoturvallisuuden hallinnan palautejärjestelmän viitemallin, vaatimuksia ja toteutustapoja. Aluksi esittelen siis takaisinkytkentään perustuvan viitemallin. Vaatimuksia varten on ensiksi kirjallisuustutkimus ja toiseksi henkilöhaastatteluiden analysointi, joiden perusteella esitän vaatimuksia palautejärjestelmälle. Lopuksi esitän toteutustapoja palautejärjestelmälle.

4.1 Palautejärjestelmän viitemalli

Tietoturvallisuuden perustehtävä on tiedon käytettävyyden, eheyden ja luottamuksellisuuden takaaminen. Tietoturvatoiminnan tuloksellisuus on käytettävyyden, eheyden ja luottamuksellisuuden toteutumisen aste. Tietoturvallisuuden hallinnan tuloksellisuuden mittari on tietoturvatoiminnan tehokkuuden ja vaikuttavuuden toteutumisen aste valtionhallinnossa. Tietoturvallisuuden hallinta ja tietoturvatoiminta ovat määritelty prosessimallien mukaan (kuten ISO/IEC 27001 PDCA). Koska tietoturvallisuuden palautejärjestelmän on tuotettava tietoa tietoturvaprosessista hallintaprosessiin, niin käytän viitemallina takaisinkytkentämallia. Prosessinohjauksessa takaisinkytkentä siirtää toiminnan mittaustietoa toiminannan ohjaukseen. Palautejärjestelmämalli on keino siirtää tietoturvatoiminnan tuloksesta tietoa toiminnan ohjaukseen, tietoturvallisuuden hallintajärjestelmään. Palautejärjestelmän viitemalli (palautejärjestelmämalli) on esitetty seuraavassa kuvassa (Kuva 5, vertaa Kuva 1):



Kuva 5: Palautejärjestelmämalli

Palautejärjestelmä on siis laajempi kuin raportointijärjestelmä, joka on osa palautejärjestelmää. Palautejärjestelmän idea on prosessin analysointi ja prosessin toimintaan vaikuttaminen. Olennaista on halutun tietoturvatason määrittely, toiminnan mittaaminen ja vertailu haluttuun tasoon[16] ja ohjaavat toimenpiteet. Tietoturvatasojen määrittelyssä olennainen osa on mitattavien kohtien löytäminen, mittareiden valinta ja palautekanavan suunnittelu.

Organisaation tai yrityksen toiminnoista ei tule prosesseja lisäämällä sana prosessi toiminnon perään. Prosessille on olennaista halutun tason (tavoitteen) määrittely, mittaaminen ja ohjaaminen (feedback). Jos toimintoa ei mitata eikä tuloksia analysoida, ei toiminta voi ohjata eikä se ole prosessi. Tämä mittaaminen, tulosten analysointi ja ohjaus analysoinnin perusteella muodostaa palautejärjestelmän, jonka avulla tiedetään missä tietoturvan osalta ollaan ja mihin ollaan menossa. Lord Kelvin (William Thomson) on puheessaan vuonna 1883 todennut: ”When you can measure what you are speaking about and express it in numbers, you know something about it.”[17]

16 Vertailu voidaan tehdä myös eri organisaatioiden välillä (benchmarking).

17 Institute of Civil Enginees -luento: http://www.todayinsci.com/K/Kelvin_Lord/Kelvin_Lord.htm

Kuten edellä olleiden VAHTI-ohjeiden ja hallintajärjestelmän käsittelyssä on todettu, palautejärjestelmälle on tarve. Kehittäminen, seuranta, valvonta ja ylläpito edellyttävät perusteita ja ne syntyvät palautejärjestelmän määrittelyistä. Määrittelyissä kuvataan 1) mittaamisen tavoitteet, 2) mitattavat kohteet ja mittarit, jotka osoittavat tavoitteiden toteutumista, ja 3) mittaustulosten analyysit (metriikat), jotka osoittavat ohjaustarpeen tavoitteisiin pääsemiseksi.

Palautejärjestelmän perustehtävä on esittää todisteet organisaation tietoturvan tasosta ja toiminnan luotettavuudesta – tilannekuvan muodostaminen. Tilannekuva kertoo esimerkiksi riskien toteutumisen, uhkien kehittymisen, toimintaprosessien vaikutukset ja niiden häiriöt ja uusien järjestelmien, menettelyiden ja ohjeiden vaikutukset.

Organisaation on osoitettava olevansa sen luottamuksen arvoinen, joka sille on tietoturvapolitiikassa asetettu ja jota lait ja muut vaatimukset edellyttävät. Jeffrey Williams ja George Jelen (1998) ovat määritelleet varmuuden seuraavasti: ”Assurance is a measure of confidence in the accuracy of a risk or security measurement.” Tietoturvatavoitteiden asettajilla täytyy olla luottamus tietoturvamekanismien oikeellisuuteen ja vaikuttavuuteen ja varmuus tavoitteiden hallinnan toimivuudesta (Kajava & Savola, 2005).

Käsiteanalyysia: Tässä opinnäytteessä palautejärjestelmän käsittely kulminoituu mittaamiseen ja mittaustulosten analysointiin. Englanninkielisessä kirjallisuudessa käytetään termejä metrics ja measurement. Esimerkiksi Kovacich (1997) on määritellyt käsitteet seuraavasti: ”Metric is standard of measurement using quantitative, statistical and/or mathematical analyses. Security metrics: application of quantitative, statistical and/or mathematical analyses to measuring infosec functional trends and workload.” Metriikka on mittaamisen standardi. Tietoturvametriikalla etsitään toiminnallisia kehityssuuntia ja työmääriä.

Suomen kielessä metriikka tarkoittaa mittajärjestelmää, ja yleensä käsitettä käytetään runomittojen yhteydessä. Matematiikassa metriikka on etäisyysfunktio.[18] Tässä työssä käsitteellä metriikka tarkoitetaan niitä tapoja, jolla kerättyä (mitattua) dataa käsitellään

18 http://fi.wikipedia.org/wiki/Metriikka_(matematiikka)

tilannekuvan luomiseksi. Kysymyksessä on siis datan muokkaaminen, yhdistely ja analysointi eri mallien ja välineiden avulla. Mittaaminen on auditointia, monitorointia, valvontaa, seurantaa, lokien käsittelyä: termi tässä työssä kattaa kaikki käsitteet, joita eri standardeissa ja suosituksissa edellytetään tietoturvatoiminnan tehokkuuden selvittämiseksi. Palautejärjestelmä on metriikkajärjestelmä, joka tuottaa datasta tilannekuvan.

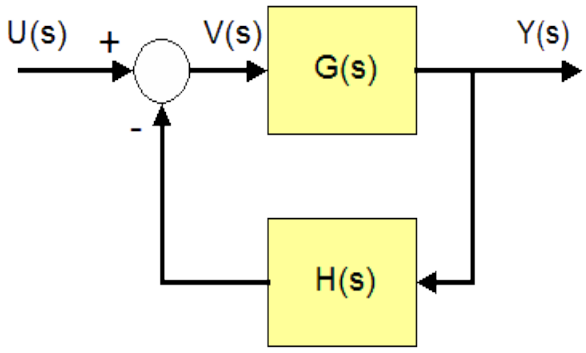
Kirjallisuudessa käsitteitä mittaaminen ja metriikka käytetään käsitteellisesti sekaisin: metriikka sisältää mittaamisen ja mittaaminen sisältää analysoinnin.

4.2 Palautejärjestelmistä yleisesti

Tässä jaksossa käsittelen lyhyesti palautejärjestelmämalleja, jotka ovat lähtökohtana tämän työn palautejärjestelmämallille. Nämä mallit ovat prosessi- ja sähkötekniikassa (säätötekniikan feedback-järjestelmät) ja johtamisessa (henkilöstötutkimukset) käytettyjä malleja. Takaisinkytkentä (feedback) tarkoittaa järjestelmässä vaikutuksen kohdistumista ohjausjärjestelmän kautta takaisin alkuperäiseen vaikutuksen lähteeseen.

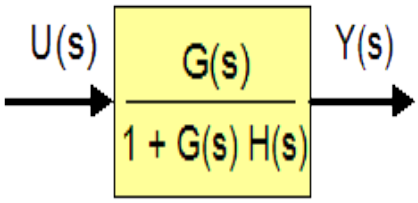
Palautejärjestelmä säätötekniikassa:

Säätötekniikassa takaisinkytkennän perusmalli (ilman häiriötekijöitä) on Kuvassa 6.



Kuva 6: Takaisinkytkennän perusmalli

Kuvan 6 symbolit: U(s) on heräte, Y(s) on vaste, G(s) ja H(s) ovat siirtofunktioita Laplace-muunnettuina.[19] V(s) on apumuuttuja, joka yleensä sievennetään pois Kuvan 7 mukaisesti, jolloin saadaan esille järjestelmän vaste sisään tulevalle syötteelle.



Kuva 7: Muunnettu takaisinkytkentä

Siirtofunktio kuvaa järjestelmän ulostulon ja sisäänmenon suhdetta. Palaute-järjestelmämallin käsitteillä palautejärjestelmän siirtofunktio kuvaa toiminnan tuloksen (tilannekuvan) suhdetta normiohjaukseen.

Palautejärjestelmän peruselementit ovat tavoitetaso, mittaaminen, ohjaus, siirtofunktio ja vasteaika. Järjestelmän toiminnan ja palautejärjestelmän kannalta vasteaika on tärkeä käsite. Tietoturvallisuuden hallinnan ja tietoturvatoiminnan reagointikyky eli vasteaika muuttuvassa toimintaympäristössä on tehokkuuden ja vaikuttavuuden mittari.

Palautejärjestelmämallissa takaisinkytkentä tarkoittaa, että palautejärjestelmä kuvaa tietoturvatoiminnalle asetettujen vaatimusten suhdetta toiminnan tuloksiin, jotka ilmenevät tilannekuvana.

Palautejärjestelmä johtamisvälineenä:

Tietoturvallisuuden hallintajärjestelmä on johtamisjärjestelmä. Yrityksissä käytetään palautejärjestelmiä osana johtamisjärjestelmää. Yleisin tällainen palautejärjestelmä lienee henkilöstökyselyt. Kyselyä suunniteltaessa on oleellista löytää avainmittaristo. Englanninkielisessä kirjallisuudessa käytetään käsitettä KPI eli Key Performance Indicators, jonka voi kääntää termillä tuottavuusmittarit. Tuottavuusmittarit ovat

19 Dynaamisen järjestelmän aikariippuvat differentiaaliyhtälöt muutetaan aikariippumattomiksi laskennan helpottamiseksi. Tuloksena kerto- ja jakolaskuja.

olennainen osa johtamisjärjestelmien (MIS) määrittelyjä (Caldelli & Parmigiani, 2004). Johtamisvälineenä henkilöstökyselyt ovat olleet joko mittaus alaisten näkemyksestä esimiehistä tai päin vastoin. Mitataan siis joko johdon ja johtamisen tai työtekijöiden ja työnteon prosessien tehokkuutta. Nykyään yleisesti käytetty palautemalli on 360 asteen palaute (Gray et al., 2007). Mallin idea on se, että henkilö saa palautteen useasta eri organisaatio tasolta: alaisilta, esimiehiltä ja kollegoilta. Mitataan siis kokonais-valtaisemmin toiminnan ja prosessien tehokkuutta ja saadaan kehityskohteita selville.

4.3 Kirjallisuustutkimus

Kirjallisuuskatsauksessa olen keskittynyt tietoturvallisuuden hallintaan, sen kehittämiseen, ohjaukseen ja mittaamiseen sekä standardeja käsittelevään materiaaliin. Tietoturvallisuuden hallintaa ja tietoturvatoimintaa käsittelevässä kirjallisuudessa ei juuri käsitellä ohjausta palautejärjestelmämallin (feedback-malli) mukaisesti. Jatkuva kehitys, mittaaminen, prosessimalli, seuranta, valvonta ja ylläpito ovat kyllä termeinä esillä, mutta selkeää kokonaisvaltaista esitystä tietoturvaprosessin ohjausmallista ei ole.

Hallintajärjestelmistä ja -malleista:

Tietoturvallisuuden hallinta on tiedonhallintaa ja turvallisuustiedon hallintaa. Teknisen tietoturvallisuustiedon hallintaan on kehitetty järjestelmiä, jotka keräävät dataa eri järjestelmistä, yleensä lokitietoja, ja analysoivat sitä erilaisin menetelmin, kuten korrelaatioilla. Järjestelmistä käytetään yleisesti lyhennettä SIM[20], SEM[21] tai SIEM[22] riippuen kehittäjästä (Hellman, 2006). Tekniset järjestelmät tuottavat dataa eri muodoissa, joten SIM-järjestelmien täytyy sovittaa data organisaation haluamaan muotoon. Useat järjestelmät kuitenkin jäävät SIM-järjestelmiltä saavuttamatta, kuten henkilöstöhallinnon järjestelmät, vaikka niistä saatava tieto on tärkeää tietoturvallisuuden hallinnan kannalta (Jaquith, 2007).

20 Security Information Management

21 Security Event Management

22 Security Information and Event Management

Tietoturvallisuuden tietoa ovat tietoturvallisuuden kriteerit ja evaluaatiot, riskien kriteerit ja arviot, riskianalyysin tulokset, auditoinnin ja mittausten tulokset ja tietoturvamonitorointien tulokset (Mäkinen, 2006). Nämä tiedot pitäisi olla palautejärjestelmän käytettävissä ja mielellään yhdestä tietojärjestelmästä saatavilla.
Turvallisuustiedon hallinnassa voidaan erottaa kaksi prosessia (Mäkinen, 2006): turvallisuustietoa luova prosessi ja tätä tietoa hallitseva prosessi. Tietoa luova prosessi määrittelee tavoitteet ja keinot, ja tietoa hallitseva prosessi määrittelee palautteen niistä johdon käsiteltäväksi. Tietoa tuottava prosessi on tietoturvatoimintaa ja tietoa hallitseva prosessi on palautejärjestelmä. Johdon kannalta on tärkeää saada tilannekuva ja ohjaavien toimien vaikutus tilannekuvan kehityksessä.

Tietoturvatoiminnan ympäristö on muuttuvaa ja sisältää paljon epävarmuuksia. Jos toimintaympäristö joutuu hyökkäyksen tai muun häiriön kohteeksi, sen on selviydyttävä siitä. Selviytymistä varten organisaatioilla on lakien ja vaatimusten mukaisesti valmius- ja toipumissuunnitelmat. Palautejärjestelmän kannalta selviytymistä voi käsitellä systeemiteoriassa käytetyn käsitteen informaation palaute (information feedback) avulla (Kreidl & Frazier, 2004). Kreidl ja Frazier esittelevät mallia automaattisen puolustusjärjestelmän avulla, joka on yhden tietojärjestelmän ominaisuus, mutta se on ajateltavissa koko tietoturvatoiminnan ja -hallinnan palautejärjestelmän mallina. Selviytymisen kannalta palautejärjestelmän täytyy käsitellä tietoturvatietoa tuottavilta järjestelmiltä tulevaa dataa, arvioida sen merkitystä aikaisempien havaintojen ja vasteiden perusteella ja päättää uusista vasteista. Päätöksen teko perustuu sen hetkiseen havaintoon ja aikaisempaan tilannekuvaan.

Tilannekuva on tietoturvan tila tietyllä ajanhetkellä ja tilamuutoksen tarve määritellään järjestelmämallin avulla. Järjestelmämalli on tilakonemalli, jota voidaan ohjata Markov-päätöksentekoprosessilla (Kreidl & Frazier, 2004). Tietoturvatapahtuma on järjestelmän kannalta virhe, joka muuttaa tilaa. Tilakonetta ohjataan aktiivisilla tai passiivisilla kontrolleilla: aktiivinen kontrolli vaikuttaa tilaan ja passiivinen kontrolli siihen miten tilaa tarkkaillaan. Päätöksentekoa ohjaa kustannus- ja palkkiotekijä. Oikea päätös palkitaan ja väärä päätös johtaa ylimääräisiin kustannuksiin. On tärkeä huomata, että väärään positiiviseen tietoon perustuva päätös johtaa lisäkustannuksiin ja väärään negatiiviseen tietoon perustava päätös johtaa riskin kasvuun ja sitä kautta

lisäkustannuksiin (Kreidl & Frazier, 2004). Markov-prosessin hyödyntäminen mahdollistaa matemaattisten todennäköisyyslaskentaan perustuvien mallien (kuten Markovin ketjut) hyödyntämisen tietoturvatapahtumien hallinnassa (Sallhammar et el, 2006). Perusteluna on se, että riskiarviot perustuvat todennäköisyyksiin. Tietoturvatapahtumien hallintaa varten pitää muodostaa pitkän aikavälin normimalli tapahtumista. Reaaliaikatapahtumia verrataan normimalliin poikkeamien havaitsemiseksi (Ye et al., 2004).

Johtamisesta ja ohjauksesta:

Juha Miettisen mukaan tietoturvajohtamisprosessin peruselementit ovat: riskien tunnistaminen, suojausten määrittely, suunnittelu ja toteutus, suojaustason valvonta ja suojausten kehittäminen (Miettinen, 1999).

Suojaustason valvonta on mittaamista ja liittyy palautejärjestelmään. Vain mittaamalla ja tulosten analysoinnilla voidaan suojauksia kehittää. Valvonnan osalta on päätettävä mitä valvotaan eli mitataan ja päätösprosessi alkaa jo riskien tunnistamisessa. Tehtävänä on löytää ne prosessimittarit, jotka kertovat johtamisen tuloksellisuuden ja vaikuttavuuden. Kysymys on siitä miten prosessia mitataan. Ratkaisumalleja tietoturvaprosessien mittaamiseen tarjoavat eri standardit ja suositukset, kuten SSE-CMM.

Tietoturvajohtamisen välineet Miettinen (1999) on määritellyt seuraavasti: Toiminta-ajatus, jota ohjaavat visiot ja arvot, jotka määrittelevät strategian ja politiikat. Toiminta-ajatus muunnetaan strategiaa toteuttavaksi toiminnan suunnitteluksi, joka konkretisoituu päivittäisen toiminnan johtamisena.

Tietoturvallisuuden johtaminen on ihmisten johtamista. Organisaation johto vastaa siitä millainen työ- ja turvallisuusilmapiiri organisaatiossa on. Turvallisuusilmapiirin kannalta on tärkeää, että organisaation johto ilmaisee oman turvallisuusasenteensa ja perusväline tähän on tietoturvapolitiikka. Johdon asenne vaikuttaa merkittävästi yksittäisen työntekijän asenteeseen, mikä puolestaan näkyy koko organisaation asenteena. Toisaalta organisaation käyttäytyminen vaikuttaa yksittäisen työntekijän

asenteeseen (adaptiivinen vaikutus, Chan et al., 2005). Erityisesti kriisi- tai muutos-tilanteissa asenteiden muutosta on seurattava.

Kehittämisestä:

Tietoturva- ja toimintaprosessien kehittäminen teknisessä ja nopeasti muuttuvassa maailmassa vaatii organisaatiolta paljon. Standardeista saa apua hallintajärjestelmiin ja toimintaan (esimerkiksi ISO/IEC 27000 -sarja) ja toiminnan kehittämisessä kypsyys-malli (SSE-CMM) ohjaa organisaatiota hyvin. Ongelma on vaatimusten jalkauttaminen organisaation toimintaan ja kulttuuriin. Organisaation tietoturvakulttuuria ja -asennetta ohjataan koulutuksella. Koulutusohjelmaa kehitettäessä on otettava huomioon kohdeyleisö ja tavoitteet. Oleellinen osa ohjelmaa on palautteen kerääminen ja tulosten mittaaminen (Siponen, 2000).

Koulutusohjelman tekeminen on oppimisjärjestelmän ja -ympäristön rakentamista, jossa on tärkeää valita käytettävät menetelmät ja mallit (NIST SP 800-16). Koulutusohjelma voidaan yhdistää organisaation tietoturvan kehittämisohjelmaan. Jos kehittämisohjelma perustuu kypsyystasomalliin, niin tietoturvaosaamiselle on esitetty vastaava malli (Thomson & von Solms, 2006). Koulutuksen kautta henkilö siirtyy tasolta seuraavalle (kaikkiaan 5 tasoa) tavoitteena tietoturvamyönteisen asenteen syntyminen, joka näkyy koko organisaatiossa.

Mittaamisesta ja metriikasta:

Metriikan käytön perusidea tietoturvallisuuden hallinnan osana on: mittaaminen, analysointi ja tilannekuvan muodostus. Valittu metriikka ei ole vain toiminnan mittaamista, epätyydyttävien tulosten ja syiden etsimistä ja kehityskohteiden osoittamista varten. Se on myös jatkuvaa politiikan kehitystä, politiikan muutosten toteuttamista ja tavoitteiden ja keinojen sääntelyä varten. Tämä tarkoittaa siis takaisinkytkentää eli palautejärjestelmää. Tilannekuvaan kuuluu sekä toiminta-ympäristön, toiminnan että hallinnollisen turvallisuuden tila. Tietoturvaprosessien tuloksellisuus selviää määrittelemällä metriikka avainmittareilla (KPI). Metriikan tavoitteena on saada numerotietoa numeroista. (Jaquith, 2007).

Suomessa tehdyn kyselytutkimuksen (Sademies, 2004) ja siitä tehtyjen analyysien perusteella metriikalle voidaan esittää seuraavia vaatimuksia: tietoturvatasosta on saatava todistus, lokien käsittelyyn on saatava lisää älykkyyttä, salakuuntelu on havaittava, auditoinnin on saatava tukea, liiketoimintavaatimusten täyttyminen tietoturvavaatimuksissa on ilmettävä, liiketoimintayksiöiden tietoturvatoimia on mitattava ja liiketoiminnan on saatava tukea suojaustason määrittelylle (Sademies & Savola, 2004; Kajava & Savola, 2005).

Tietoturvataso kertoo tietoturvatoimien tehokkuuden ja vaikuttavuuden. Käsitteenä tietoturvataso on suhteellinen: mihin ja mitä verrataan (Jaquith, 2007). Vertailun perusteena voi olla tietoturvainvestointien suuruus saman kokoisissa organisaatioissa tai tietoturvatapahtumien määrä suhteessa henkilöstön määrään. Oleellista on vertailukelpoisen tiedon saaminen ja siinä lokien käsittely on avainasemassa. Tietoturvadataa syntyy paljon ja datan tulkintaan tarvitaan sekä apuvälineitä, kuten hallintaohjelmistot (SIM), ja hyvin määritelty metriikka (Hellman, 2006; Jaquith, 2007). Hellman korostaa, että tietoturvanhallinta on myös tietoturvatiedonhallintaa.

Organisaation johdon kannalta ja tulosohjausmallin mukaisesti mittaamisen tuloksena on tietoturvainvestointien ja -organisaation perustelu (Chapin & Akridge, 2005).

Tietoturvallisuuden hallinnan ja metriikan uranuurtaja on George F. Jelen. Hän on esittänyt metriikalle seuraavat vaatimukset (Payne, 2006; Revenel, 2006): tarkkaan määritelty, mitattavissa oleva, saavutettavissa oleva, toistettavissa oleva ja aikariippuva. Näihin vaatimuksiin (SMART[23]) vastataan metriikkaprojektilla. Projektille voidaan asettaa seuraavat lähtökohdat (Kovacich, 1997): miksi tietoja pitää kerätä, mitä tarkkaan määriteltyjä tietoja kerätään, miten tietoja kerätään, milloin tietoja kerätään, kuka kerää tiedot ja missä prosessin vaiheessa tietoja kerätään.

Näiden lähtökohtien perusteella käynnistettävän metriikkaprojektin vaiheet voivat olla seuraavat (Nichols & Sudbury, 2006): tavoitteiden määrittely, tarvittavien tietojen määrittely (kysymykset), metriikan kehittäminen (vastaukset), raporttien ja

23 Specific, Measurable, Attainable, Repeatable, Time-dependent

raportointiaikataulun määrittely, metriikan käyttöönotto (mittaamisen käynnistäminen), tarkastuspisteiden ja -kohteiden määrittely ja metriikan jatkokehityksen määrittely.

Tärkeä ominaisuus metriikalle on läpinäkyvyys: mistä esitetty tulos on saatu. Mittaustietoja esiteltäessä kohderyhmän on luotettava sekä käytettyyn dataan että käytettyihin mittareihin, joten niiden on oltava ymmärrettäviä koko organisaatiossa (Jaquith, 2007).

Mittareiden valinnalle pitää olla perusteet. Victor Basili on kehittänyt ohjelmistokehityksen laadun seurantaa varten Goal Question Metrics -mallin (Basili et al., 1994).[24] Itse asiassa edellä esitetty metriikkaprojektin vaiheet sisältävät GQM-mallin sitä mainitsematta. Mallin lähtökohtana on tavoitteen (goal) asettaminen mittaamiselle. Tavoitteen saavuttamista tarkennetaan kysymyksillä (question) ja vastauksia kysymyksiin etsitään oikeilla mittareilla (metrics). Menetelmän tarkoitus on saada selville kattava metriikka, jolla pystytään seuraamaan ohjelmistojen laatua useasta eri näkökulmasta. Tämä on mahdollista, koska menetelmässä etsitään mittareita, jotka vastaavat useampaan kysymykseen ja siten kertovat useamman tavoitteen toteutumisen Mallia selvitetään enemmän (Luku 4.5) yhtenä osa palautejärjestelmän toteutustapaa.

Mistä GQM-malliin saadaan tavoitteita? Tietoturvastandardit on kehitytetty erityisesti auditointia varten (Jaquith, 2007) eikä niissä ole huomioitu toiminnan sisältöä (Siponen, 2006). Standardeista saadaan kuitenkin esille tarvittavat tavoitteet GQM-mallin käyttöä varten. Esimerkiksi standardeista SSE-CMM[25] mittaa organisaation kykyä tuottaa turvallisuutta (tuotteita, palveluita, toimintoja). Mistä tietää tuloksen, jos toteuttaa standardin vaatimukset? Ratkaisu on oikean metriikan määrittely prosesseille ja turvallisuudelle.

SSE-CMM-standardissa oleva käytänteiden jako (tietoturva- ja organisaation peruskäytänteet) voidaan muuttaa metriikkajaoksi: prosessi- ja turvametriikka (Kormos, 1999). Prosessimetriikka todistaa määrällisillä tai laadullisilla mittareilla (myös on/off-

24 Alkuperäinen esitys on vuodelta 1984 (Basili, V. & Weiss, D.M.: A Methodology for Collecting Valid Software Engineering Data)

25 Kypsyystasotesti verkossa: http://ivs.cs.uni-magdeburg.de/sw-eng/us/java/CMM/cmm_test.shtml

mittarilla), että tietty taso on saavutettu. Turvametrikkaa on mitattava ominaisuus tietoturvaprosessissa, joka on todiste tehokkuudesta (vaikutuksesta). Metriikoille tavoitteet ja tarvittavat kysymykset saadaan SSE-CMM-standardin lukujen 5 ja 6 sisällöstä.

Mittaaminen ja metriikka ovat viime aikoina nousseet vahvasti esille. Suuri osa tietoturvauhkista ja hyökkäyksistä kohdistuu nykyään tietojärjestelmiin, siis ohjelmiin (SANS, 2007). Tietojärjestelmä koostuu useista ohjelmakomponenteista ja alijärjestelmistä ja sellaisen hallinta mittareilla ja mittaamisella on vaikeaa – eräiden mielestä jopa mahdotonta (Bellovin, 2006). Bellovin pitää tietoturvametriikkaa tulevaisuuden Khimairana[26] (Kuva 8) – kauhukuvana.

Kuva 8: Khimaira

Riskienhallinnasta:

Riskienhallinta on yleensä riskien tunnistamista, mutta ei näiden arvottamista. Mikä on tiedon arvo yksittäisissä kohteissa (työasemat, palvelimet) ja mikä on niiden yhteisarvo? Miten tieto liikkuu organisaatiossa, entä ulos ja sisään? Pelkkien riskien määrittelyn lisäksi pitää määritellä riskien suhde tiedon arvoon. Mikä on tietoturvatapahtuman suhde tiedon arvoon? (Jaquith, 2007)

Riskianalyysin vaikeus: riskejä laskettaessa on mahdollista tehdä liikaa arvailuja ja arvotuksia (subjektiivisuus). Useat epävarmuustekijät saattavat johtaa oletuksiin, joiden

26 Kreikkalaisessa mytologiassa hirviö, jolla leijonan pää, vuohen ruumis ja käärmeen pyrstö.

perusteella tehdään vääriä investointeja (liikaa, liian vähän). Miten saadaan esille kustannusvastaavuus? (Stewart, 2004)

Andrew Stewart (2004) on esittänyt myös riskien kompensaatioteorian: Kun organisaatiossa suojaavia keinoja lisätään, niin jossain tehdään toimia, jotka mitätöivät ne. Syntyy väärä luottamus tietoturvatoimien tehokkuuteen. Tämän estämiseksi tarvitaan tietoturvatoiminnan institutialisointi eli ottaminen osaksi ydintoimintaa. Edellytyksenä on toimintaympäristön muovaaminen sellaiseksi, jossa käyttäjät osallistuvat tietoturvaprosessiin. Organisaation pitää kehittää pysyvä tietoturvakulttuuri.

Riskianalyysi on työlästä ja saattaa johtaa ylimitoitettuihin tai väärin kohdennettuihin tietoturvatoimintoihin. Tuloksena on resurssien tuhlaus ja väärä turvallisuuden tunne. (Jelen, 1995). Jelen on esittänyt mallin, jossa riskianalyysin lähtökohta on organisaation missio – tehtävä. Riskianalyysin pohjaksi täytyy selvittää tehtävän toteuttamiseksi tarvittavat kriittiset tiedot ja järjestelmät. Tarvitaan vastaus kysymykseen, mikä tieto vihollisen käsissä antaa viholliselle edun (esimerkiksi kaupallisen). Kun vastaukset edellisiin on saatu, riskianalyysissä voidaan keskittyä olennaiseen.

Taksonomioista:

Tietoturvatoiminnan ja sen synnyttämän tilannekuvan ymmärtämisen perustana on se, että organisaatiossa yhteinen kieli. Yhteisen kielen on katettava mittaaminen, analysointi ja raportointi. Lisäksi on eduksi, että käytetty kieli on ymmärretty toimialalla ja mittaukset tehty yhtenäisesti. Esimerkiksi Savola (2007) on esittänyt luokittelua tietoturvan metriikalle. Yhtenäisen esitystavan synnyttämiseksi myös mitattavat kohteet täytyy ymmärtää yhteisellä kielellä. Tietoturva-alueella on esitetty erilaisia luokitteluja (ontologiat ja taksonomiat) esimerkiksi tietoturvauhkille, -tapahtumille (Landwehr, 1993; Aslam, 1996; Abbas et al., 2005). Käytännön esimerkki yrityksestä yhtenäistää tietoturvauhkien ja tapahtumien esittämistä on Mitren ylläpitämä CVE-hakemisto.[27] Yhteinen kieli auttaa myös organisaatioiden välisessä tiedon-vaihdossa ja yhteistyössä.

27 http://cve.mitre.org – Common Vulnerabilities and Exposures

Kuten aikaisemmin on todettu, tietoturvallisuuden hallinnasta iso osa ihmisten johtamista. Johtamisen tuloksena organisaation syntyy tietoturvakulttuuri, joka voidaan ilmaista kypsyystasolla. Henkilöstön tietoturvakulttuurin ja -tietoisuuden kehittämiseksi ja ymmärtämiseksi on esitetty ontologia (Siponen & Kajava., 1998).

Varmuudesta:

Peruskysymykset ovat (Jelen & Williams, 1998):

1) Kuinka turvassa olen?
2) Kuinka varma olen edellisen kysymyksen vastaukseen?

Aikaisemmin on jo mainittu, että Jelen on määritellyt varmuuden luottamuksen mitaksi. Kun organisaation johdolle esitetään tietoturvan tilannekuva, niin samalla kerrotaan hallinnollisten toimien suhteesta tietoturvatoiminnan tulokseen (palautejärjestelmä-mallin siirtofunktio). Samalla on todistettava myös tilannekuvan varmuus.

Riskien ja turvallisuuden arviointi sisältää aina epävarmuutta. Toistuvilla mittauksilla epävarmuuden määrä selviää. Mitä suurempi varmuus tarvitaan, sitä useammin täytyy mitata. Samoin, mitä isompi riskiarvio riskianalyysissä on tehty, sitä useammin täytyy mitata.

Bruce Schneier (2007) on määritellyt varmuuden luottamusta rakentavaksi toiminnaksi. Tietoturvapolitiikan täytyy vastata organisaation tarpeita ja sen täytyy olla yhtenäinen koko organisaatiossa. Tietoturvapolitiikka toteuttavien toimintoja täytyy olla riittävästi. Toimintojen täytyy oikein käyttöönotettuja, jotta ne toteuttavat asetetut tavoitteet ja vain ne.

Audun Jøsang on käsitellyt paljon luottamusta. Hän on esittänyt sille subjektiiviseen logiikkaan perustuvan metriikan (Jøsang, 2001). Lisäksi hän on käsitellyt luottamuksen hallintaa (Jøsang et al., 2005). Subjektiivinen logiikka mahdollistaa varmuuden esittämisen laskennallisesti todennäköisyyksiin perustuen ja siten kuvaa hyvin luottamuksen astetta ja siihen liittyvää epävarmuutta. Subjektiivisessa logiikassa todennäköisyydet perustuvat henkilöiden uskoon ja epäuskoon (belief/unbelief) esitetyn

väitteen (esimerkiksi väite ”olemme turvassa”) luotettavuudesta. Luottamuksen hallinnan kannalta oleellisia käsitteitä ovat luotettavuus (reliability) ja päätös (decision). Luotettavuus kuvaa sitä todennäköisyyttä, jolla henkilö toimii odotetulla tavalla. Päätös kuvaa puolestaan henkilön toimintaa tietyssä tilanteessa luotettavuuden tasosta riippumatta. Esimerkiksi henkilö voi tietyssä tilanteessa lähettää aineistoa salaamatta epäluotettavaa tiedonsiirtoväylää pitkin, kun hän katsoo, että tilanne vaatii sitä vaikka tuloksena voi olla tiedon paljastuminen. Tietoturvallisuuden johtamisen kannalta mahdollisuus varmuuden esittämisestä ihmisten toiminnasta luotettavasti numeerisesti antaa kuvan johtamisen vaikuttavuudesta. Numeerisen mallin todennäköisyyksien suuruudet mahdollistavat myös poikkeustilanteiden hallinnan, kun tiedetään mihin ihmisten toiminnassa pitää keskittyä.

4.4 Haastatteluiden analysointi

Koska opinnäytteeni käsittelee palautejärjestelmän vaatimuksia, niin osana vaatimusmäärittelyjen tekemistä haastattelin kohdeorganisaation henkilöitä. Haastatteluihin osallistui kaikkiaan 8 tietoturvallisuustoiminnassa mukana olevaa henkilöä seuraavista Puolustusvoimien organisaatioista: Johtamisjärjestelmäkeskus, Maanpuolustuskorkeakoulu, Materiaalilaitos ja Pääesikunnan osastot: Asiakirjahallinto, Johtamisjärjestelmäosasto, Operatiivinen osasto ja Tutkinta. Kysymykset jakautuivat varsinaisen palautejärjestelmän ja mittaamisen kesken. Käsitellyt kysymykset olivat:

1. Mikä tietoturvallisuuden palautejärjestelmä teidän mielestänne on?
2. Miten tietoturvallisuuden palautejärjestelmän pitäisi mielestänne toimia?
3. Mitä tietoa palautejärjestelmästä tarvitaan laatu- ja tulosohjaukseen?
4. Millaisia tietoturvamittareita toiminnalle pitäisi olla, mitä pitäisi mitata?
5. Mikä pitäisi olla automatisoinnin aste mittaamisessa?

Kysymykset oli jaettu kirjallisina etukäteen sisältäen saatteen.[28] Kirjallisessa versiossa on enemmän kysymyksiä, mutta päädyimme lopullisena toteutuksena haastattelu-

28 Liittessä 4 on alkuperäinen kirjallinen kysely, joka vastaajien pyynnöstä muutettiin suoraksi haastatteluksi, jossa keskitytään vain tulevaisuuden toiveisiin.

muotoon, jossa käsitellään vain tulevaisuuden toiveita ja vaatimuksia, nykytilaa ei käsitelty. Näin taattiin opinnäytteeni säilyminen julkisena.

Haastattelu tehtiin noin tunnin kestäneenä henkilökohtaisena haastatteluna. Haastattelun aluksi esittelin haastattelun lähtökohdat kyselyn kirjallisen version saatteen mukaisesti. Haastattelussa käytiin kysymykset läpi yksi kerrallaan, mutta pääsääntöisesti keskustelussa kuitenkin palautejärjestelmää ja mittaamista koskevia huomioita oli ja käsiteltiin yhtäaikaa. Jako kysymyskohtaisiin vastauksiin on siis osittain minun.

Kysymys 1: Mikä tietoturvallisuuden palautejärjestelmä teidän mielestänne on?

Kysymyksen tarkoitus oli selvittää haastateltavien näkemys palautejärjestelmästä yleisellä tasolla, pohjautuen haastattelun alustuksessa esiteltyihin lähtökohtiin. Perusajatukseni on, että palautejärjestelmä sisältää aina vaikuttavan (ohjaavan) ominaisuuden järjestelmään (tässä hallintajärjestelmään ja toimintaan), josta palautetta kerätään (feedback-malli). Lähtökohtana on tietoturvastandardeissa esitetty vaatimus, että standardeissa vaadittuja kontrolleja on seurattava ja kehitettävä: seuraaminen edellyttää mittaamista ja kehittäminen on siitä syntyvän palautteen vaikutusta.

> Avainkäsitteitä, joita haastattelussa tuli esille, olivat: johtaminen, tekninen taso, hallinnallinen taso, henkilöstötaso, auditoinnit, prosessituki, riskienhallinta.

Haastattelussa kävi ilmi, että vaikka tietoturvallisuuden hallintaa ja tietoturvatoimintaa ei ole toteutettu esitellyn palautejärjestelmämallin mukaisesti, niin erilaisia palautejärjestelmiä on olemassa. Nämä palautejärjestelmät toteutuvat osana kutakin toimivaa organisaatiota, kuten asiakirjahallinto, mutta suoraa feedback-mallin mukaista ohjausvaikutusta toimintaan niissä ei ole. Kyse on lähinnä siitä, että pääsääntöisesti palautejärjestelmämallia ja -toimintaa ei ole formaalisti määritelty ja dokumentoitu. Toimiva palautejärjestelmä on auditointeihin perustuva toiminnan tarkastelu ja siitä syntyvä hallinnan ja toiminnan ohjaus. Pelkästään auditointeihin perustuva tietoturvatoiminnan kehitys on kuitenkin hidas tapa ohjata toimintaa nopeastikin muuttuvassa tietoturvaympäristössä.

Tietoturvallisuuden hallintajärjestelmä on osa johtamisjärjestelmää. Kun tietoturva toimintaa johdetaan ja ohjataan hallintajärjestelmällä, palautejärjestelmän täytyy olla osa johtamisen tukijärjestelmiä.

Olennaiseksi koettiin se, että palautejärjestelmä on osa sekä teknistä- että hallinnallista toimintaa. Erityisesti henkilöstön kytkeminen palautejärjestelmään koettiin tärkeäksi: käyttäjiltä palautteen saaminen on tärkeää muissakin kuin ongelmatilanteissa. Palautejärjestelmä nähtiin myös osana riskienhallintaa, joka järjestelmä tuottaa eri prosessien toimintaa tukevaa tietoa.

Kysymys 2: Miten tietoturvallisuuden palautejärjestelmän pitäisi mielestänne toimia?

Kysymyksen tarkoitus oli selvittää haastateltavien näkemys siitä, miten palautejärjestelmän pitäisi toimia, kun yhteinen ymmärrys siitä mitä palautejärjestelmällä tässä opinnäytteessä tarkoitetaan ja mihin sillä pyritään.

> Avainkäsitteitä, joita haastattelussa tuli esille, olivat: johtaminen, päätöksenteko, tilannekuva, automatisointi, poikkeamat, luottamus, vaikuttavuus, trendit, organisaatiotasot.

Kysymyksen 1 käsittelyssä sivuttiin jo palautejärjestelmän toimintaa: sen pitää olla järjestelmä, joka tukee eri tietoturvaprosessien toimintaa ja kehitystä eri organisaatiotasoilla. Erityisesti korostuivat riskienhallinta ja vaikuttavuus. Riskienhallinnan osalta tarvitaan tietoa, joka auttaisi riskianalyysia tuottamalla uusia riskiparametreja ja kuvaamalla olemassa olevien riskiparametrien toimivuuden. Myös tieto siitä onko riskien ottaminen kasvanut on tärkeää. Vaikuttavuudella tarkoitetaan sekä toiminnan että vastatoimien vaikuttavuutta (tuloksellisuutta), samalla se ilmaisee tietoturvallisuuden hallinnan tehokkuutta. Tietoturvatoiminnan vaikuttavuus näkyy siinä, että se on mahdollistanut uusien toimintojen käyttöönoton. Esimerkkinä operatiivisen järjestelmän käyttö harjoituksissa kenttäolosuhteissa. Toiminnan vaikuttavuus on siis lisännyt luottamusta.

Eri organisaatiotasoja kiinnostaa tietoturvan tilannekuva. Palautejärjestelmän pitää tuottaa samasta datasta eri tasoisia tilannekuvia: ylin johto on kiinnostunut tilannekuvasta koko valtakunnan tasolla, verkon turvallisuudesta vastaavat ovat kiinnostuneet tietoturvasta esimerkiksi verkon käytettävyyden osalta ja asiakirjahallinto kadonneiden asiakirjojen osalta. Tilannekuvan muodostuksessa oleellista on myös trendien havaitseminen: palautejärjestelmän avulla pitää saada tietoa siitä, mihin suuntaan pitkällä aikajaksolla tietoturva on kehittynyt ja tarvittaessa osoittaa korjaavia toimenpiteitä (liittyy edellä mainittuun riskianalyysin tekoon).

Päätöksenteon tueksi tarvitaan myös oikein kohdennettua tietoa. Erityisesti operatiivisessa toiminnassa tarvitaan automaattisesti kerättyä ajantasaista tietoa akuutin tietoturvauhkan ratkaisemiseksi. Lisäksi palautejärjestelmästä on saatava tietoa sekä tehtyjen että suunniteltujen tietoturvainvestointien ja -toimien tueksi.

Organisaation johto tarvitsee tietoa siitä, miten annetut tietoturvatavoitteet ovat toteutuneet. Tämä kertoo sen, miten hyvin johtaminen on turvattu.

Kysymys 3: Mitä tietoa palautejärjestelmästä tarvitaan laatu- ja tulosohjaukseen?

Kysymyksen tarkoitus oli selvittää haastateltavien näkemys palautejärjestelmästä suhteessa laatu- ja tulosohjaukseen. Valtionhallinnon toiminnan kehityksessä on käytössä tulosohjausmalli ja laatu kytkeytyy osaksi tulosohjausta. Tietoturva ja sen toteutuminen on osa organisaation laatua ja olisi aivan perusteltua ottaa tietoturva-auditointi osaksi laatuauditointia.

> Avainkäsitteitä, joita haastattelussa tuli esille, olivat: laatujohtaminen, investointiperusteet, uudet toiminnat, vaikuttavuus, tehokkuus, tietoturvakulttuuri.

Kuten missä tahansa organisaatiossa investoinnit ja henkilöstötarve on perusteltava. Tietoturvatoiminnan ongelma on, että tuotantolaitoksiin verrattavaa investoidun pääoman tuottoaste (ROI tai ROSI) on vaikea laskea: paperikoneelle sen voi tehdä, mutta mikä on palomuurin tuotos. Palautejärjestelmästä on saatava tietoa, joka kertoo,

että tietoturvatoiminta on mahdollistanut uusien toimintojen käyttöönottoja ja miten erilaisten tietoturvapoikkeamien määrälle on tapahtunut. Tietoturvapoikkeamien määrä erityisesti siltä osin, joka kertoo organisaation tietoturvakulttuurin kehityksen.

Turvallinen toiminta on laadukasta toimintaa. Tietoturvallisuuden johtaminen on osaltaan laatujohtamista, joten tietoturvatoiminnan tuloksellisuuden mittaamisesta pitää saada metriikan avulla tietoa myös laatujärjestelmään.

Kysymys 4: Millaisia tietoturvamittareita toiminnalle pitäisi olla, mitä pitäisi mitata?

Kysymyksen tarkoitus oli selvittää millaisia mittareita haastateltavien mielestä pitää olla. Tässä kohdassa käsiteltiin konkreettisia mittareita, vaikka edellisissä haastattelun kohdissa sivuttiin useastikin mittareita. Tässä mittarilla tarkoitetaan eri lähteistä kerätystä datasta tehtyjä analyysin (metriikan) kautta saatuja tuloksia.

> Avainkäsitteitä, joita haastattelussa tuli esille, olivat: johtamisen turvallisuus, tehokkuus, vaikuttavuus, kohdentaminen, oikea-aikaisuus, läpinäkyvyys, henkilöstö, normistonmukaisuus, hyvä tiedonhallintatapa.

Mittareiden täytyy olla tarkoituksenmukaisia, jolloin ne kertovat asetettujen tavoitteiden (kuten riskianalyysi, tulosohjaus, budjetointi) toteutumisista. Tarvittavat mittarit kertovat tietoturvatoiminnan tehokkuudesta ja toimenpiteiden vaikuttavuudesta. Mittareiden täytyy olla myös kohdennettu siten, että ne oikea-aikaisesti kertovat halutulle kohderyhmälle tietoturvan osa-alueiden tilan: aina yksittäisestä kohteesta (esimerkiksi virusturva) isoon kokonaisuuteen (esimerkiksi riskienhallinnan kokonaistila). Mittarit ja mittaaminen on toteutettava siten, että niiden merkitys on eri organisaatiolle sama (yhteinen kieli). Mittareiden toimivuutta on myös seurattava, koska muuttuvassa ympäristössä mittareiden ei voi olettaa pysyvän vakoina.

Myös henkilöstöä pitää mitata: sekä toimintaa ja toimia että asennetta ja sitoutumista. Henkilöstön palaute tietoturvatoiminnasta on tärkeää ja heillä pitäisi olla helposti käytettävissä oleva tapa raportoida tietoturvasta ja siihen liittyvistä tapahtumista.

Kiinnostavaa tietoa on esimerkiksi tietojen kalastelun (social engineering) kohteeksi joutuminen.

Tietoturvan ja tietoturvatoiminnan tilan lisäksi mittaamisen ja mittareiden pitää tukea tietoturvapoikkeamien selvityksestä. Tarve on jäljitettävyystiedosta aina tekniseen todisteiden keräämiseen.

Organisaation johdon ja erityisesti operatiivisen johdon täytyy tietää miten hyvin johtaminen on turvattu. Erityisen tärkeää on kriittisen tiedon käytettävyys tietoverkoissa reaaliajassa.

Lait edellyttävät hyvän tiedonhallintatavan noudattamista. Miten toteutuu tarkoituksenmukaisuus esimerkiksi työntekijän osalta, onko oikeat ja sopivat välineet käytössä? Entä kansalaisten osalta, ovat normiston mukaisesti rekisteriselosteet saatavilla?

Kysymys 5: Mikä pitäisi olla automatisoinnin aste mittaamisessa?

Kysymyksen tarkoitus oli selvittää haastateltavien näkemys mittaamisen automatisoinnin tarpeesta. Kysymyksen taustalla on se tosi asia, että toiminnallista tietoa tuottavia järjestelmiä on paljon ja niistä saatava tieto kiinnostaa useita organisaatiota.

Avainkäsitteitä, joita haastattelussa tuli esille, olivat: tehokkuus, oikea-aikaisuus.

Mittaaminen ei ole itse tarkoitus vaan sen avulla saatu tieto on tärkeää. Näin olleen mittaamisen ei pidä kuormittaa organisaatioita: miten enemmän dataa ja mitä tiheämmin mitataan sitä automaattisempaa pitää olla.

Lopputulema:

Palautejärjestelmän kaltainen toiminta koetaan tärkeäksi ja käytännössä sellaista toimintaa onkin, mutta ei yhtenäisesti määriteltynä. Palautejärjestelmän kannalta on

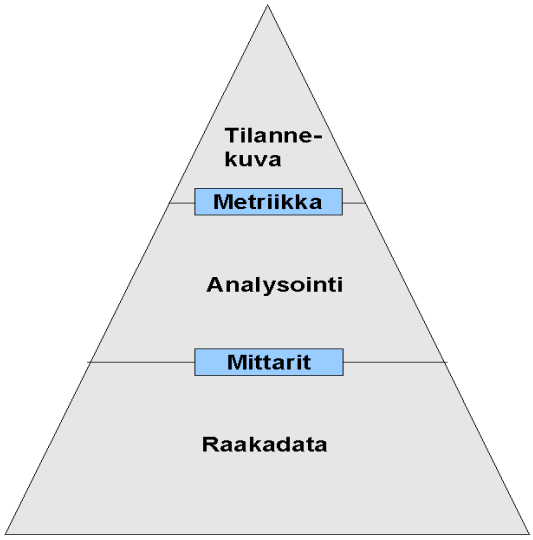
oleellista, että siihen saadaan tietoa teknisten järjestelmien lisäksi henkilöstöltä. Tietoturvastandardit edellyttävät, että riskianalyysien pohjalta valittujen kontrollien toimintaa ja tehokkuutta seurataan (mitataan) ja että niitä kehitetään, mutta niissä ei kerrota mitä mittaamisella tarkoitetaan. Palautejärjestelmämalli yhdistettynä järjestelmälliseen mittareiden määrittelyyn on keino selvittää kontrollien tehokkuus ja saada niiden kehittämiseen ohjaavaa tietoa. Palautejärjestelmään tietoa tuottavien mittareiden täytyy olla tarkoituksen mukaisia, joten niiden suunnittelun täytyy olla sidoksissa riskienhallintaan ja riskianalyysin.

Johtamisen kannalta palautejärjestelmän täytyy tuottaa sellaista tietoa, joka tukee sekä johtamistoimintaa (turvallinen ympäristö) ja päätöksentekoa että johtamisen kehittämistä, tässä siis hallintajärjestelmän kehittämistä ja asetettujen tavoitteiden uudelleen arviointia.

4.5 Palautejärjestelmän vaatimukset

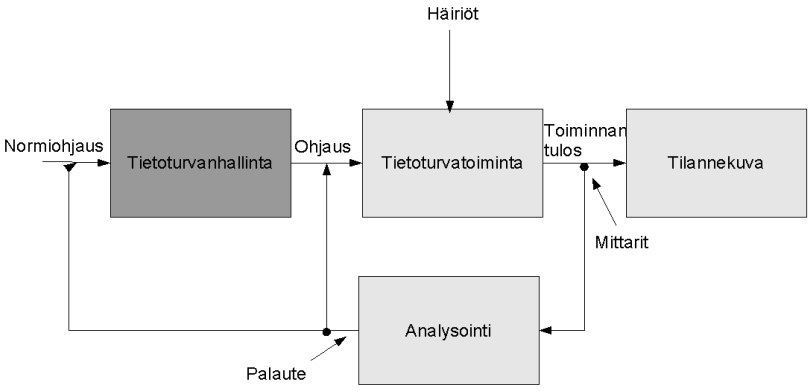
Palautejärjestelmä kytkeytyy tietoturvallisuuden hallintajärjestelmään. Tässä työssä vaatimusmäärittelyjen rakenne tulee Luvussa 3 esitellyn hallintajärjestelmän rakenteesta, ylimmän tason jakona hallinnallinen osa ja toiminnallinen (operatiivinen) osa. Kuten Luvussa 2.3 on todettu tietoturvatoiminta jaetaan kahdeksaan osa-alueeseen. On syytä huomata, että ISO/IEC 27001:2005 sisältää 11 osa-aluetta ja ne ovat standardien käytön mukana tulossa Suomeenkin.

Palautejärjestelmän täytyy tuottaa organisaation johdolle tilannekuva sekä tarkasteluhetken tietoturvasta (snap shot) että tietoturvan kehityssuunnasta (trend analysis). Lisäksi organisaation eri osilla ja tasoille pitää saada niiden tarvitsemat tilannekuvat. Tämän kaiken on synnyttävä samasta kerätystä datasta. Palaute-järjestelmän vaatimukset konkretisoituvat pitkälti mittaamisen (mittarit) ja tiedon analysointiin (metriikka), jotka kohdentuvat tietoturvatoimintaan. Kuvassa 9 on tilannekuvan muodostamista palautejärjestelmän käsitteiden kautta.



Kuva 9: Palautejärjestelmän tiedonkolmio

4.5.1 Vaatimuksia hallintajärjestelmän kannalta



Kuva 10: Palautejärjestelmämallin käsiteltävä osuus: hallinta

Tietoturvallisuuspolitiikka ja toimintaperiaatteet

Palautejärjestelmän on tuotettava tietoa siitä, että organisaation toiminta- tai liiketoimintatavoitteiden (mission) asettamat vaatimukset ovat kirjattu politiikkaan, ja että toiminnan muutokset näkyvät tarvittaessa politiikan muutoksena. Tärkeää tietoa ovat esimerkiksi ohjeistuksen eheys kautta organisaation ja henkilöstön koulutuksen tuloksellisuus.

Tietoturvallisuusstrategia

Palautejärjestelmän täytyy saada tietoa tietohallinnon strategiasta ja pystyttävä tuottamaan tietoa strategian toteutumisesta tietoturvan näkökulmasta tai tietoturvan kannalta strategiassa olevista vaaroista.

Riskianalyysi

Palautejärjestelmän kehitys on osa riskienhallintaa. Riskianalyysissa saadaan palautejärjestelmälle tietoa siitä, mitä on seurattava ja mitattava, ja miten tuloksia raportoidaan ja kenelle. Riskienhallinta ja riskianalyysiprosessi ovat jatkuvaa toiminta ja ne tuottavat palautejärjestelmälle uusia vaatimuksia prosessin aikana. Palautejärjestelmän vasteaika muutoksiin on oltava lyhyt. Palautejärjestelmän toiminnan määrittely täytyy sitoa riskienhallintaprosessiin ja tietoturvatavoitteiden asettamiseen. Aina riskianalyysia tehtäessä täytyy päättää, mikä on analysoitavan kohteen tavoite tietoturvan toteutuksessa (vaikutus) ja miten vaikutusta mitataan. Samoin on päätettävä, mitä mittareita kohteelle asetetaan (metriikka) ja miten mittaustulokset ohjaavat toimintaa.

Tietoturvallisuussuunnitelma ja -ohjeet

Palautejärjestelmän on tuotettava tietoa siitä, että suunnitelmat ja ohjeet vastaavat tietoturvapolitiikan asettamia vaatimuksia. Suunnitelmat ja ohjeet määrittävät tietoturvatoiminnan, joten palautejärjestelmän on muutettava toiminnan tulos ilmaisuksi suunnitelmien ja ohjeiden tehokkuudesta.

Jatkuvuus- ja toipumissuunnitelma

Riskianalyysin perusteella organisaatiolla on oltava tiedossa toiminnan kannalta kriittiset järjestelmät ja tiedot. Palautejärjestelmän on erityisesti seurattava niitä ja niissä tapahtuvia muutoksia. Tärkeää on myös siirtää tieto muuttuneesta toimintaympäristöstä suunnitelmiin ja erityisesti kolmansien osapuolien (ulkoistukset) vaikutus on huomioitava.

Valmiussuunnitelma

Organisaation on tiedettävä tärkeysluokkansa ja sen mukaisesti toteutettava varautuminen. Yleensä varautuminen tehdään varmistuksilla ja korvaavien järjestelmien ylläpidolla sovitulla tavalla. Palautejärjestelmän on tiedettävä varmistusten taso ja toimintakyky. Suunnitelman mukaiset testaukset on tehtävä niin, että niistä saadaan palautejärjestelmälle toimintatason vaatimukset.

Tietoturvallisuuden tulosohjaus

Tulosohjauksella mitataan tietoturvatoiminnan tehokkuutta ja tietoturvallisuuden hallinnan vaikuttavuutta suhteessa organisaatioon ja investointeihin. Palautejärjestelmän täytyy yhdistää tietoturvallisuuspolitiikassa ja -strategiassa asetetut tavoitteet ja tulossopimuksessa määritellyt mittarit tehokkuuden ja vaikuttavuuden ilmaisuksi. Palautejärjestelmän avulla on saatava perustelut organisaatiolle ja investoinneille.

Tietoturvallisuuden toteutustapa, organisointi ja vastuut

Toteutustavan ja organisoinnin täytyy vastata tietoturvapolitiikan vaatimuksia. Erityisesti vastuiden osalta palautejärjestelmän on pystyttävä ilmaisemaan, että toteutus on haluttu: vastuuta ei vain yhden henkilön varaan ja vastuuhenkilöiden osaaminen on tietoturvatoiminnan edellyttämällä tasolla.

Vuosisuunnitelmat ja budjetit

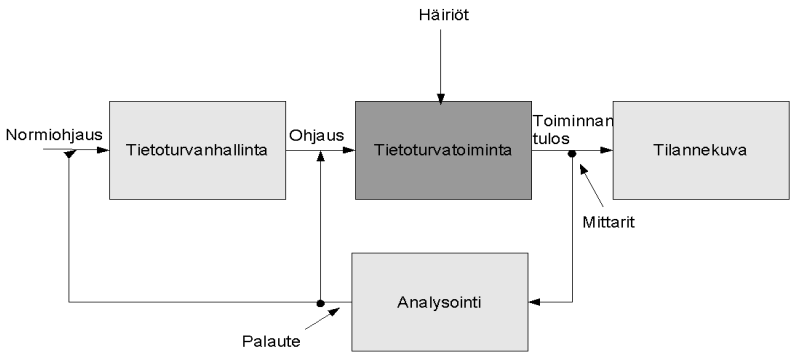
Suunniteltujen kustannusten on vastattava toiminnan tavoitteita. Palautejärjestelmästä on saatava tietoja, joka osoittaa toiminnan tehokkuuden ja vaikuttavuuden kustannustehokkuuden tai perustelut poikkeamiin suunnitelmista ja budjetista.

Raportointi

Raportointi perustuu määriteltyihin raportointivastuisiin: kuka raportoi, mitä ja kenelle raportoidaan. Raportointi on palautejärjestelmän oleellinen osa. Sen lisäksi, että palautejärjestelmästä saadaan metriikkaan perustuvaa analysoitua tietoa toiminnan ohjausta varten, on sen kautta samasta datasta saatava eri organisaatioiden ja organisaatiotasojen tarvitsemia raportteja. Palautejärjestelmän on myös huolehdittava siitä, että raportointiin tarvittava tieto on käytettävissä, ja että raportointi tapahtuu sovitun aikataulun mukaisesti.

Yhteenvetona voidaan palautejärjestelmästä hallintajärjestelmän kannalta todeta, että useat vaatimukset ovat yhteisiä eri hallintajärjestelmän osille (esimerkiksi tulosohjaus ja budjetointi), joten sama analysoitu tieto vastaa useampaan kysymykseen. Tarpeiden perusteella voi todeta vielä, että palautejärjestelmän täytyy saada tietoa tavalla tai toisella muista tietojärjestelmistä: ei vain teknistä tietoa tuottavista järjestelmistä, mutta esimerkiksi myös henkilöstö- ja taloushallinnon järjestelmistä. Tiedon saanti voi perustua teknisiin ratkaisuihin tai auditointeihin. Valtaosa palautejärjestelmän tarvitsemasta tiedosta hallintajärjestelmää varten tulee tietoturvatoiminnan mittaamisesta. Palautejärjestelmän on myös pystyttävä tuottamaan tieto tarvittaessa myös muihin järjestelmiin.

4.5.2 Vaatimuksia tietoturvatoiminnan kannalta



Kuva 11: Palautejärjestelmämallin käsiteltävä osuus: toiminta

Hallinnollinen tietoturvallisuus

Tietoturvapolitiikka on johdon ilmaisu tietoturvatoiminnan tarpeellisuudesta ja tietoturva-asenteesta ja hallinnollisen tietoturvan perusta. Käytännössä edellä läpikäydyn hallintajärjestelmän tarvitsema tieto palautejärjestelmästä ja siitä kerättävä tieto palautejärjestelmälle koskee hallinnollista tietoturvallisuutta. Erityisesti palautejärjestelmän pitää pystyä ilmentämään tietoturvaosaamisen ja -ymmärtämisen taso (sekä johdon että henkilöstön osalta), ja että toiminta on lakien ja suositusten mukaista. Kun seuraavat seitsemän tietoturvatoiminnan osa-aluetta on liitetty palautejärjestelmän piiriin, niin hallinnollisen tietoturvallisuuden ja tietoturvapolitiikan tehokkuus on mitattavissa ja ilmaistavissa.

Henkilöstöturvallisuus

Henkilöstö on avainasemassa tietoturvan toteuttamisessa. Henkilöstöturvallisuuden tehtävä on henkilöstö aiheutuvien riskien hallinta. Keinot henkilöstöturvallisuuteen ovat riskianalyysit, avainhenkilöstön määrittelyt, varahenkilöjärjestelyt, työsuhteen

elinkaaren hallinta ja tietenkin koulutus. Henkilöstöturvallisuuden toteutuminen kertoo organisaation tietoturvakulttuurin tason ja hyvän tiedonhallintavan toteutumisen.

Henkilöstöturvallisuuden tärkeimpiä prosesseja on käyttöoikeuksienhallinta, jonka tavoitteena on sekä tiedon suojaamisen että tiedon saatavuuden takaaminen. Se on sidoksissa järjestelmien, tietojen ja työtehtävien luokitteluun. Palautejärjestelmän kannalta tämä tarkoittaa sitä, että järjestelmän on tunnistettava luokitukset. Palautejärjestelmän on pystyttävä seuraamaan käyttöoikeuksien käyttöä ja muutoksia koko työsuhteen elinkaaren ajan: oikeuksien perustamisesta niin poistamiseen.

Palautejärjestelmän kautta on selvittävä organisaatiossa käytettyjen toimien taso ja tehokkuus: onko turvaselvitykset tehty, miten organisaatiossa tapahtuvat muutokset on huomioitu esimerkiksi varahenkilöjärjestelyissä, onko koulutuksella ollut vaikutusta turvallisuuden kehittymiseen, ovatko käyttöoikeudet ajan tasalla. Henkilöstö-turvallisuuden hallinnalle tärkeää tietoa on myös henkilöstöön kohdistunut tietojen kalastelu (social engineering), sen raportointiin on oltava menettelyt.

Fyysinen turvallisuus

Toiminnan turvallisuuden takaaminen alkaa fyysisestä turvallisuudesta. Siihen liittyvät toimi- ja laitetilojen ja järjestelmien luokittelu ja suojaus, kulkuoikeuksien hallinta, tietoliikenne- ja sähköverkon suojaus ja varmistus. Erityistä huomioita on kiinnitettävä organisaation ulkopuolisten henkilöiden (huoltomiehet ja muut vastaavat) hallintaan. Palautejärjestelmän on tiedettävä suojattavat kohteet ja niiden tasot ja pystyttävä liittämään kulku- ja käyttöoikeudet ja oikeuksien valvontatiedot niihin. Myös eri suunnitelmien ja niihin liittyvien harjoitusten pito ja niistä saatu tieto on oleellista palautejärjestelmälle.

Tietoaineistoturvallisuus

Valtionhallinnossa tietoaineistoturvallisuuden tarpeet määrittelevät pitkälti julkisuuslaki (621/1999) ja arkistolaki (831/1994). Toiminnan edellytyksenä on aineistojen luokittelu ja sen mukaisten toimintaohjeiden ja menettelyiden käyttö. Menettelyihin kuuluvat

salassapitosopimukset, salauskäytännöt, tiedon käsittely ja talletustavat ja käyttöoikeuksien hallinta oleellisena osana. Palautejärjestelmän pitää tietää luokittelut ja luokitteluihin liittyvät käsittelyvaatimukset. Sen lisäksi palautejärjestelmän pitää pystyä seuraamaan aineistoa ja sen liikkumista organisaatiossa (tai organisaatiosta ulos) koko sen elinkaaren ajan, aineiston syntymisestä sen arkistointiin tai hävittämiseen asti. Sama koskee eri tietovälineitä: järjestelmän pitää tietää millä tietovälineellä liikutetaan ja säilytetään. Tietoaineistoturvallisuudesta huolehtiminen toteuttaa tiedon käytettävyyden, eheyden ja luottamuksellisuuden vaatimukset.

Tietoliikenneturvallisuus

Organisaatioiden toiminta on nykyään riippuvaista tietoverkoista. Tietoverkkojen ja tietoliikenteen turvallisuuden on vastattava organisaatioiden turvallisuustarpeita, jotka tulee huomioida verkon rakentamisessa ja käytössä. Turvallisuustarpeita toteuttavat esimerkiksi varajärjestelyt (kahdennukset, varareitit), tietoturvaratkaisut (palomuurit, salaustekniikat), valvontajärjestelmät ja henkilöstön osaaminen.

Palautejärjestelmän kannalta tietoliikenne ja sen järjestelmät ovat teknisen datan (lokitietoa paljon) tuottajia, josta pitää erilaisin analyysein ja suodatuksin tuottaa järkevää tietoa tilannekuvan muodostamiseksi. Palautejärjestelmän on myös tiedettävä esimerkiksi kuinka pitkän tietoliikennekatkon organisaation toiminta kestää, mikä henkilöstön koulutuksen ja osaamisen taso, miten ulkoiset toimijat (eri palvelujen tarjoajat) vaikuttavat toimintaan ja muutokset ja niiden vaikutusten hallinta.

Laitteistoturvallisuus

Jos organisaatioiden toiminta on riippuvaista tietoliikenteestä, niin on se sitä myös tietojärjestelmistä: valtaosa tiedosta tuotetaan, käsitellään ja säilytetään tietojärjestelmissä. Fyysisten järjestelmien (palvelimien, työasemien ja tietoliikennelaitteiden) on toteutettava asetetut tietoturvavaatimukset. Laitteistot on luokiteltava ja kirjattava, niille on oltava vararatkaisut ja ne on sijoitettava luokittelun mukaisiin tiloihin. Erityistä huomioita on kiinnitettävä laitteiden etäkäyttötarpeisiin ja ulkoistettuihin laitteistoihin. Palautejärjestelmän on tiedettävä mistä laitteistoista eri

toiminnot ovat riippuvia ja mikä on toiminnon katkon vaikutus organisaation toimintaan. Merkittäviä tietoja ovat sallitut katkosajat (huollot) ja sopimuksiin kuuluvat vasteajat (SLA:t).

Ohjelmistoturvallisuus

Laitteistot eivät toimi ilman ohjelmistoja. Tietoteknisessä maailmassa ohjelmistot ovat tietoturvallisuuden kannalta iso riskitekijä. Valtaosa verkkojen kautta tapahtuvista hyökkäyksistä kohdistuu ohjelmistovirheiden ja puutteiden hyödyntämiseen (SANS, 2007). Ohjelmistot täytyy testata ja luokitella ennen käyttöönottoa ja niissä on oltava riittävät turvamekanismit (salaus, vahva käyttäjätunnistus) tarvittavan suojaustason toteuttamiseksi. Palautejärjestelmän on tiedettävä käytetyt ohjelmistot, niihin tulevien korjausten määrä ja toteutusajat. Kriittisten järjestelmien ohjelmistovikojen korjausten vasteajat on määriteltävä.

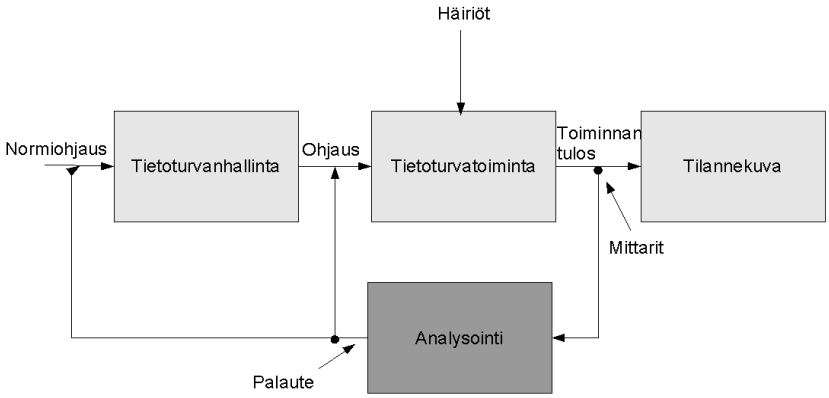
Kuten edellisessä kohdassa järjestelmien riippuvuussuhteet ovat tärkeä tietää, jotta esimerkiksi ylläpitojen vaatimat katkokset voidaan suunnitella ja asettaa niille sallitut toteutusajat. Kuten tietoliikennejärjestelmät, ohjelmistot ja niiden valvonta tuottaa paljon dataa (lokitietoa), jonka on oltavat palautejärjestelmän käytettävissä ja jonka käsittelylle on tehtävä säännöt. Erityisesti on huomattava, että osaa datasta on käsiteltävä yksityisyyden suojaa koskevien lakien mukaisesti.

Käyttöturvallisuus

Ohjelmien ja järjestelmien käytön on oltava turvallista. Käyttöoikeuksien on oltava määritelty niin, että käyttäjä ei toimillaan saa vahinkoa aikaiseksi, mutta hänellä on kaikki tarvitsemansa tieto ja järjestelmät käytettävissään. Erityisesti kriittisten järjestelmien ja tietojen osalta huolto- ja ylläpitomenettelyjen, suojausten, varmistusten, seurannan ja käyttöoikeuksien on oltava palautejärjestelmän tiedossa. Haittaohjelmien ja roskapostin torjunta ja leviämisen estäminen ovat osa käyttöturvallisuutta. Toiminnasta syntyvän datan on oltava palautejärjestelmän käytettävissä ja kuten edellä yksityisyyden suoja on otettava huomioon.

Yhteenvetona voidaan todeta, että tietoturvatoiminnasta palautejärjestelmälle kerättävä tieto ja siitä analysoinnin kautta syntyvät ohjaustarpeet on luettavissa VAHTI-ohjeesta 8/2006 ja erityisesti sen liitteestä 2. Kaikkiin ylläoleviin osa-alueisiin kuuluu asianmukaisen koulutuksen ja dokumentoinnin toteuttaminen.

4.5.3 Vaatimuksia mittaamiselle ja metriikalle



Kuva 12: Palautejärjestelmämallin käsiteltävä osuus: analysointi

Palautejärjestelmä ei saa tietoa ilman mittaamista eikä se pysty tuottamaan tilannekuvan tarvitsemaa tietoa ilman metriikkaa. Palautejärjestelmä koostuu olemassa olevasta jatkuvasta toiminnasta, jolle on asetettu lähtötaso ja tavoitteet, toiminnan mittaamisesta ja analysoinnista ja määrämuotoisesta tavasta ohjata toimintaa analysoinnin tulosten perusteella. Mittaus ja analysointi voivat olla automatisoituja kuten myös ohjaus (tietoturvan tekniset alijärjestelmät, kuten palomuuri).

Metriikan pitää perustua asetettuihin tavoitteisiin. Toisin sanoen palautejärjestelmän, joka metriikkaa hyödyntäen muodostaa eri tietoturvan osa-alueista ja kokonaisuudesta tilannekuvan, toiminnan täytyy perustua asetettuihin tavoitteisiin.

Aikaisemmin on todettu, että metriikka on numeroita numeroista. Tärkeitä tietoja on kuvattava aikana, rahana, työmäärinä tai järkevillä suhdeluvuilla. Esimerkiksi vasteajat kertovat paljon tietoturvatoiminnan tehokkuudesta.

Organisaation kypsyystason kasvaessa seurattavien toimintojen määrä kasvaa, joten myös mitattavan tiedon määrä kasvaa (SSE-CMM, NIST SP 800-26): automatisoinnin tarve kasvaa. Kun mittaamisen määrä kasvaa, tarvitaan myös enemmän metriikkaa analysointiin. Mitä enemmän tietoa kerätään ja analysoidaan sen edullisemmaksi mittaaminen ja analysointi täytyy tehdä.

Metriikkaa täytyy myös hallita ja kehittää järjestelmällisesti. Paras paikka metriikan kehittämiselle on riskianalyysin yhteyteen määritelty metriikkaprosessi. Metriikan tueksi riskienhallinnassa täytyy tehdä riskien määrällinen luokittelu ja arvottaminen ja sen perusteella tehty kiireellisyysluokitus (Jaquith, 2007).

Mittaaminen täytyy määritellä mitattavan kohteen mukaan: kriittisiä kohteita täytyy mitata useammin kuin muita kohteita. Kun merkitys ja/tai mittaustiheys on suuri, niin mittaamiseen voi käyttää vähän aikaa ja vähän optioita. Kun merkitys on pieni ja/tai mittaustiheys on pieni, niin käytettävää aikaa on paljon ja optioita voi olla paljon. (Jaquith, 2007)

Analysointitekniikoiden pitää tukea haluttujen tulosten esittämistä (toteutumia). Tekniikoita ovat esim. keskiarvo, mediaani, hajonta, ryhmittelyt, aikasarjat, korrelaatiot (Jaquith, 2007). Raporttien esitystavan oltava siinä standardimuodossa, jonka organisaatio on sopinut. Tärkeää on läpinäkyvyys, tieto siitä mistä tulos on saatu, ja yhteinen kieli. Tulosten esittämisen lisäksi on siis tärkeää, että aina voidaan jäljittää mistä tulos on saatu: tiedon jäljitettävyys. Voidaan esittää vaatimus, että raportointivaiheessa täytyy alkuperäisen datan olla käytettävissä (NIST SP 800-55).

Mittareiden vaatimukset: luotettavia, soveltuvia, yksiselitteisiä, helppolukuisia, oikea-aikaisia, olennaisuus (mitataan oikeita asioita). Mittareita täytyy olla sekä laadulliset että määrällisiä. Laadulliset mittarit ovat pääsääntöisesti auditointisuuntautuneita, määrällisten mittareiden pitää olla automatisoituja ja numeerisia. Uhkien mittaaminen

on hankalaa: sen lisäksi, että mitataan tietoturvatapahtumia ja -kontrolleja, joita käytetään, täytyy mitata myös miksi jotain tapahtuu ja myös miksi ei. (Jaquith, 2007)

4.6 Palautejärjestelmän toteutustavat

Palautejärjestelmän toteuttamisen osat ovat määrittelyt, toiminta ja tekniset järjestelmät. Palautejärjestelmän toiminnan kannalta on tärkeää oikean ja tarkoituksenmukaisen tiedon saanti ja analysointi. Tietoa saadaan mittaamalla haluttuja kohteita ja sovitun metriikan mukaisesti sitä analysoimalla.

Minä keskityn tässä työssä määrittelyihin ja toimintakulttuuriin. Määrittelyjen osalta pääpaino on metriikan ja mittaamisen määrittelyissä, joiden määrittelyjen perusteella palautejärjestelmä saa ja käsittelee (analysoi) dataa tiedon (tilannekuvan) muodostamiseksi. Palautejärjestelmän toiminta kulminoituu mittaamiseen ja mittaustulosten analysointiin. Tutkin Goal Question Metrics -menetelmän käyttöä tietoturvametriikan määrittelyssä.

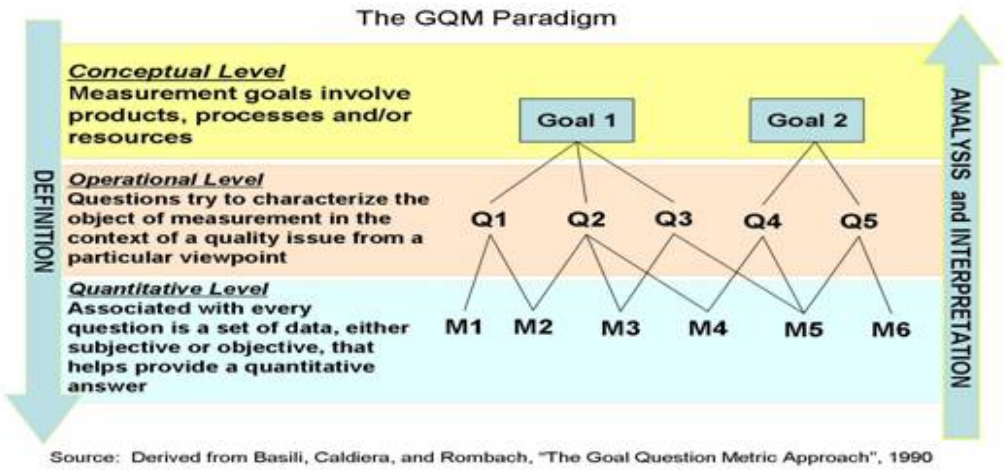
Toiminnan osalta keskityn organisaation toimintakulttuurin mittaamiseen ja erityisesti käyttäjien tietoturvailmapiirin selvittämiseen. Toimintakulttuurin taso ilmaisee hyvän tiedonhallintatavan toteutumisen ja halutun kypsyystason saavuttamisen. Tutkin itsearviointien ja auditoinnin käyttämistä tietoturvailmapiirin mittaamisessa. Käsittelemättä jäävät tekniset järjestelmät ovat tietoturvatoimintaan liittyvää tietoa (dataa) tuottavia järjestelmiä, kuten palomuuri, virustorjunta tai kulunvalvontajärjestelmä, ja tietoturvatiedon käsittelyyn tarkoitettuja järjestelmiä (SEM/SIM/SEIM).

4.6.1 Määrittelyt ja mittaaminen

Kirjallisuustutkimuksen ja palautejärjestelmän vaatimusmäärittelyjen mukaan tietoturvan mittaaminen edellyttää tavoiteasetannasta lähtöisin olevia oikein kohdennettuja mittareita. Ongelmana on eri standardien (SSE-CMM, ISO/IEC, Cobit, CC) vaatimusmäärittelyiden (objectives, controls, domains) muuttaminen mitattaviksi kohteiksi ja metriikaksi. Luvussa 4.2 lyhyesti esitelty GQM-malli on kehitetty

tavoitteista lähtevään mittaamiseen (Basili et al., 1994). Vaikka malli on alunperin suunniteltu ohjelmistosuunnittelun apuvälineeksi, niin on sitä kehitetty edelleen (Berander & Jönsson, 2006,). Mallin perusidea toimii kaikissa kehitystä mittaavissa kohteissa.

Mallissa lähdetään kolmitasoisesta määrittelystä (Kuva 13): käsitteellinen taso (Conceptual level, Goal), toiminnallinen taso (Operational level, Question) ja määrällinen taso (Quantitative level, Metric). Kuvasta 13 havaitaan, että määrittely tehdään ylhäältä-alas -menetelmällä ja mittausten analysointi alhaalta-ylös -menetelmällä.



Kuva 13: GQM-malli

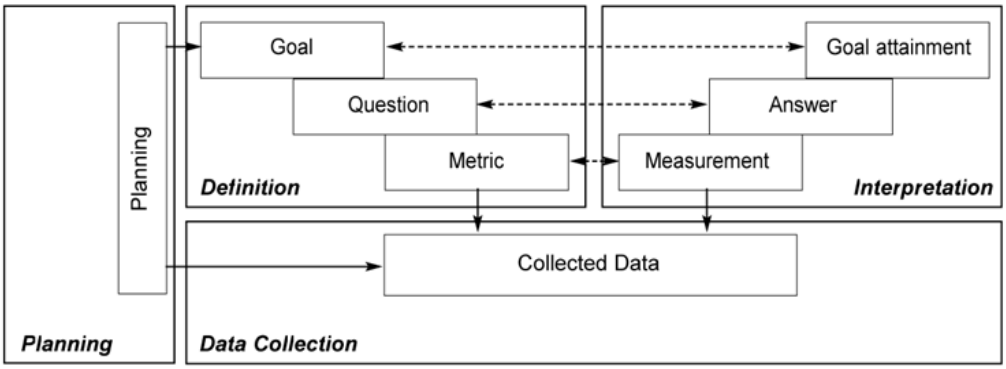
GQM-mallin mukainen tietoturvatoiminnan analysointi toteutetaan projektina. Projektin aikana toimii kehitysprosesseja, joita on kaikkiaan neljä:

1. Suunnitteluvaihe (planning), jossa mittausprojekti perustetaan ja sille tukiryhmä, kehitettävä (mitattava) kohde valitaan ja määritellään ja tehdään projektisuunnitelma. Olennainen osa suunnittelua on koulutus.
2. Määrittelyvaihe (definition), jossa mittausprojekti määritellään: tavoitteet, kysymykset ja metriikka, jotka dokumentoidaan. (Tämä vaihe on varsinainen

GQM-malli.) Samalla määritellään suunnitelmat tulkintavaihetta ja palautteen antoa varten.

3. Datankeruuvaihe (data collection), jossa varsinainen data kerätään. Vaiheeseen kuluu datankeruun testaus, metriikan perustietokannan luominen ja analysoinnin määrittely.
4. Tulkintavaihe (interpretation), jossa kerätty data analysoidaan kohdassa 2 sovitulla metriikalla ja tuloksena on vastauksia asetettuihin kysymyksiin, jotka vastaukset kertovat onko asetetut tavoitteet saavutettu. Tämä on myös palautevaihe.

Kuvassa 14 on esitetty GQM-mallin mukaisen metriikkaprojektin toteutusprosessit ja niiden väliset suhteet.



Kuva 14: GQM-mallin mukainen metriikkaprojektin toteutusprosessit

GQM-projekti on syytä perustaa samalla kuin metriikkaprojekti (Nichols & Sudbury, 2006) käynnistetään. GQM-projektin tavoitteet ovat samat kuin metriikkaprojektin (tietoturvallisuuden todistaminen) ja vaatii johdon tuen. Organisaation johto asettaa tavoitteet organisaation toiminnalle ja tietoturvavaatimuksille, joten heidän osuutensa projektin toteutukseen ensi arvoista.

GQM-mallissa datan keruun pitää perustua dokumentoituun tarpeeseen ja käytäntöön ja tarve muutetaan kysymyksiksi. GQM-prosessiin on otettava mukaan henkilöt, joiden näkökulmasta mittausta tarkastellaan. Heiltä saadaan tarvittavaa dataa ja he ovat sen analysoinnin ja tulkinnan asiantuntijoita (Differding, 1996).

Organisaatiossa on paljon mittaustietoa tuottavia järjestelmiä, joista dataa kerätään (mitataan). Yleensä mittaustulos on kuva järjestelmästä tiettynä ajanhetkenä. Jos mittaustuloksia ei analysoida laajemman kokonaiskuvan saamiseksi ja asetettujen tavoitteiden toteutumisen selvittämiseksi, mittaamiseen käytetyt resurssit ovat tuhlausta (van Solingen et al., 1999). Asian voi todeta myös niin, että jos dataa syntyy paljon, on väärin hyödyntää sitä vain kertaluontoisesti eikä tehdä siitä pitkäjänteisempää aikaulottuvuuteen sidottua analyysia.

Jos dataa tuottavia järjestelmiä on paljon, voi yhden tavoitteen toteutumisen selvittämistä varten kertyä kymmeniä tai satoja mittareita organisaation koosta ja tavoitteista riippuen. GQM-projektin toteutuksessa datan keruu on osoittautunut kaikkien kalleimmaksi (Fuggetta et al., 1998), joten GQM-prosessin automatisointi on tärkeää. Automatisointi onnistuu, jos toistuvasti suoritettavat osuudet suunnitellaan niin, että ne ovat aina toistettavissa samoilla mittareilla ja työkalua[29] käyttäen. (Lavazza, 2000, Aversano et al., 2004b)

GQM-malli on toimiva, kun haetaan toiminnalle avainmittareita (KPI). GQM-malli toimii periaatteessa kuten Occamin partaveitsi[30] valittaessa mitattavia kohteita. GQM-malli mahdollistaa mittareiden määrää minimoivat määrittelyt, mutta sitä ei alkuperäisessä huomioida. Pelkona on ollut, että kehitetään enemmän mittareita, kuin ehditään kerätä ja analysoida.

GQM-projektiin on ehdotettu vaiheistus tarkistuspisteineen mittareiden määrän rajaamiseksi (Berander & Jönsson, 2006). Tarkastuspisteissä etukäteen sovittu organisaatio käy läpi ehdotetut mittarit, luokittelee ja priorisoi ne. Tämän perusteella valitaan vain organisaation kannalta oleelliset mittarit (KPI). Menettelyyn kuuluu vielä valitun mittariston (metriikan) esittely koko organisaatiolle.

Huomioon otettavaa on se, että GQM on analyyttinen malli. Siinä ei ole huomioitu esimerkiksi liiketoiminnan tarpeita, mutta mallia on kehitetty myös liiketoiminnan

29 Esimerkkityökalu: http://fc-md.umd.edu/gqm/

30 Occam's Razor: Wilhelm Ockhamilaisen esittämä periaate, jonka mukaan paljoutta ei tule asettaa edelle turhaan.

mittaamiseen (Aversano et al., 2004a). Tähän tarpeeseen voidaan hyödyntää myös tuloskorttimallia, johon GQM-mallilla saadut tulokset liitetään (Buglione & Abran, 2000). GQM -projektin määrittelyvaihe (vaihe 2) on siis varsinainen GQM-malli ja yleensä se on kaavakepohjainen.

Liitteessä 5 on luettelo metriikasta GQM-mallilla tehtynä. Kohteena on standardin ISO/IEC 27001:2005 esittämät kontrollit (Annex A). Kullekin tietoturvan 11 osa-alueelle annetuista kontrolleista on valittu pari tarkastelun kohteeksi. Metriikan määrittelyssä on käytetty GQM-mallin mukaista kehityslomake (Basili et al., 1994). Kaavakkeen idea on dokumentaation syntyminen, mikä on standardien vaatimusten mukaista.. Kuten edellä on todettu, mallia on kehitetty edelleen ja tavoitelähtöisen metriikan määrittelyyn on useita eri kehityslomakkeita.

4.6.2 Toiminnan mittaaminen ja henkilöstöpalaute

Standardit ja suositukset eivät huomioi ihmisten käyttäytymistä (sisäiset tekijät). Ihmisen mieltä ja aikeita ei voi monitoroida (Yulin, 2006). Työntekijä on edelleen tietoturvariskeistä suurin vaikka tietämyksen myötä uhka on pienentynyt (Tucci, 2007). Silti yhä enemmän hyökkäykset kohdistuvat suoraan ihmisen käyttäytymistapoihin: tiedonkalastelu ja verkkohuijaukset[31] lisääntyvät koko ajan (SANS, 2006). Tietoturvatoiminnan yksi perustehtävä on kuitenkin ihmisten ohjaaminen oikeaan tietoturvakulttuuriin, jossa tietoturvan peruselementit toteutuvat. Peruselementit ovat käytettävyys, eheys ja luottamuksellisuus. Ohjaaminen on pitkälti tiedon hallintaa ja uuden tiedon synnyttämistä. Ohjaaminen tapahtuu myös ohjeistuksilla, teknisillä apu- ja pakkokeinoilla ja seurannalla. Toiminnan mittaamisen tarkoitus ei ole kuitenkaan ihmisten mittaaminen vaan prosessien mittaaminen.

Jotta henkilöstö saadaan sitoutettua haluttuun tietoturvakulttuuriin, niin henkilöstön palaute tietoturvatoiminnasta on tärkeää. Näin henkilöstö kokee olevansa osa tieturvatoimintaa ja tietoturvaa ohjaavat organisaatiot saavat tarvittavaa tietoa tietoturvakäyttäytymisen tilasta. Henkilöstön palautetta voidaan käsitellä myös tietoa

31 Englanninkielisiä termejä ovat social engineering, phishing. spear-phishing.

tuottavan organisaation näkökulmasta: palautteen avulla organisaation täytyy tuottaa itselleen uutta tietoa.

Tietoturvatoiminnan ja -ilmapiiriin tarkastelu henkilöstön kannalta jakautuu kahteen osaa: varsinainen tietoturvaorganisaatio ja muu henkilöstö. Esitän seuraavaa mallia: Henkilöstön asennetta tietoturvaan ja näkemystä tietoturvailmapiiristä kartoitetaan osana laatuauditointia tai vuosittaisia henkilöstön ilmapiiritutkimuksia. Tietoturva-organisaation näkemys tietoturvan tilasta ja tietoturvailmapiiristä tarvitaan useammin. Edellisten kartoitusten lisäksi heidän tulisi tehdä esimerkiksi neljännesvuosittain itsearviointi. Ihannetilanteessa jatkuvan auditoinnin periaate saisi olla käytössä.

Kun organisaatiossa on käytössä kypsyystasomalliin (SSE-CMM) perustuva tietoturvan kehitysohjelma, henkilöstön tietoturva-asennetta on myös käsiteltävä kypsyysmallin mukaisesti (Siponen, 2000; Thomson et al., 2006). Kuten kirjallisuuskatsauksessa on todettu, niin turvallisuusilmapiiri voidaan yhdistää tavoitteiden mukaiseen käyttäytymiseen (Chan et al., 2005). Samassa tutkimuksessa selvitetty sekä henkilöstön vaikutusta ilmapiiriin että ilmapiirin vaikusta henkilöstöön. Tuloksena oli, että ilmapiirin syntyyn eniten vaikuttavat työtoverit, ja sitä kautta heidän merkityksensä tietoturvakäyttäytymiseen on suuri.

Ilmapiiritutkimuksessa on tärkeää saada selville esimiesorganisaation näkemys alaisistaan ja päinvastoin sekä kollegiaalinen näkemys työyhteisön ilmapiiristä. Tällaisia näkemyksiä tarjoaa 360 asteen palaute -malli, jota yleisesti henkilöstöhallinnot käyttävät. Sen vaiheet ovat: tavoitteiden määrittely (miksi), palautteen keräämismallin määrittely (sähköposti, www-sivut), arviointimallin suunnittelu (määrällinen, laadullinen), kyselyn toteuttaminen, vastausten kerääminen ja analysointi, tulosten jakaminen ja kehityssuunnitelman teko (Levine, 2003).

Yllä olevat vaiheet ovat yhtenevät edellä esitetyn GQM-mallin toteutusvaiheiden kanssa. Onkin luontevaa, että kyselyn tavoitteet saadaan organisaation asettamien tietoturvatavoitteista ja kysymykset kehitetään GQM-projektin yhteydessä. Oleellista kyselyissä on pitkän aikavälin verrannollisen tiedon saaminen, mutta jos organisaation

tavoitteet muuttuvat, kysymystenkin täytyy muuttua. Siksikin on luontevaa, että kyselyn kysymykset muodostetaan GQM-projektin yhteydessä.

Tietoturvaorganisaatio on jokapäiväisessä toiminnassaan yhteydessä muuhun organisaatioon ja sen toiminnan tuloksiin. Siksi on sekä järkevää että tärkeää kartoittaa erikseen heidän näkemystään organisaation tietoturvatilasta ja tietoturvaorganisaation omasta ilmapiiristä. Edellä esitetyn kaltaiset kyselyt muodostuvat usein toistettuina liian raskaiksi sekä tekijöille että vastaajille, joten tarvitaan kevyempi menetelmä.

Itsearviointi on nopea ja tehokas tapa ilmaista näkemys sekä omasta että muiden toiminnasta ja organisaation ilmapiiristä.[32] Jos tietoturvaorganisaatio pitää säännöllisiä tilannekatsauksia tai vastaavia, niin itsearvioinnin voi tehdä samassa yhteydessä ryhmätyönä – ryhmäarviointina.

Esimerkiksi Peter Bitterli (2005) on esittänyt mallin ISO/IEC 17799:2000 (ISO/IEC 27002:2005) kontrollien itsearvioinnille. Itsearvioinnin perusta on kypsyysmalli, joka pohjautuu COBITin kypsyysmallille (yhteensopiva siis SSE-CMM:lle). Kypsyysmallin tasot ovat: ei olemassa (0), epävirallinen (1), toistettavissa oleva (2), käyttöönotettu (3) ja optimoitu (4) (Bitterli, 2005).

Bitterli (2005) on esittänyt kontrollien itsearvioinnin tekoa työryhmässä osana riskianalyysia. Sijoitus on hyvä, koska riskianalyysin osana pitäisi olla myös GQM-prosessin, jossa tarvittavat arvioitavat kohteet ja kysymykset voidaan määritellä. Tärkeää on, että pelkkien kontrollien lisäksi on arvioitava toimintaa ilmapiirin kannalta. Itsearvioinnin pohjana voi pitää myös standardia NIST SP 800-26. On huomattava, että itsearviot antavat aina subjektiivisen näkemyksen asioiden tilasta, joten ne kuvaavat hyvin organisaation ilmapiiriä.

Tietoturvakulttuurin muodostamiseksi organisaatiossa oleva hiljainen tieto (tacit knowledge) on saatava osaksi käsitteellistä ulkoista tietoa (explicit knowledge), joka voidaan muuntaa halutuksi kulttuurilliseksi tiedoksi (cultural knowledge). Kulttuurisen

32 Kahden lapsen isänä olen havainnut, että nykyään itsearviointia opetellaan ja tehdään jo alakoulusta alkaen ja käytännössä vastaukset ovat aina rehellisiä.

tiedon on vaikeasti hallittavissa ja sen katsotaan sisältävän paljon hiljaista tietoa. Hiljainen tieto on kokemukseen perustuvaa, organisaation kannalta piilo-osaamista: sitä on vaikea välittää ja viestiä. Hiljaisen tiedon määrä ja sen siirtyminen ulkoiseksi tiedoksi on hyvä mittari työilmapiiristä: tietoa ei luovuteta ahdistettuina eikä pakottamalla. Ongelmana on, että hiljaista tietoa on vaikea mitata. (Nonaka, 1994) Mittaamiseksi on kehitettyjä malleja, kuten kolmiomalli (Richards & Busch, 2000). Siinä hiljaista tietoa haetaan psykologilla testeillä, osallistuvalla havainnoinnilla ja käsiteanalyysilla, johon data kerätään kyselyllä. Nonaka (1994) on todennut, että hiljaisen tiedon esille saamisessa esimiestyö on avainasemassa.

Yhteenvetona voi todeta, että organisaation tietoturvallisuuden hallinnan kannalta on tärkeää saada tieto toimivan organisaation tietoturvailmapiiristä ja erityisen tärkeää se on tietoturvaorganisaatiolta.

5 Pohdinta ja johtopäätökset

Olen käsittelyt tässä työssä tietoturvallisuuden hallintaa valtionhallinnon näkökulmasta. Käsittelyn lähtökohdaksi annettiin palautejärjestelmä hallinnan välineenä. Koska valtionhallinnossa tietoturvatoimintaa ohjaava hallintajärjestelmä perustuu prosessi-ajatteluun standardien (kuten SSE-CMM ja ISO/IEC 27001) mukaisesti, niin valitsin lähtökohdaksi prosessiohjauksen takaisinkytkentämallin. Mallin perusteella tein palautejärjestelmämallin, joka on koko käsittelyn lähtökohta. Tavoitteena oli saada palautejärjestelmälle vaatimuksia ja esittää toteutustapoja.

Vaatimuksia varten tein kirjallisuustutkimuksen ja henkilöhaastattelut Puolustusvoimien organisaatiossa. Kirjallisuustutkimuksella kartoitin asiantuntijoiden näkemyksiä tietoturvallisuuden hallinnasta prosessinäkökulmasta. Tietoturvatoiminnan ja sen hallinnan prosessimuotoa korostettiin, mutta yleisesti ei ollut havaittavissa näkemyksiä siitä, miten prosessia ohjataan. Kirjallisuustutkimuksen perusteella löytyi kuitenkin yhteistä näkemystä siitä, mitä tietoturvallisuuden hallinta vaatii: standardien mukaisuutta, yhteistä kieltä ja jatkuva seurantaa ja kehittämistä. Lisäksi korostui mittaamisen ja mittareiden tärkeys ja ne ovat perusedellytys seurannalle ja kehittämiselle.

Haastattelut antoivat tärkeää tietoa siitä, mitä tietoturvasta vastaavat henkilöt haluavat tietoturvallisuuden hallinnalta ja palautejärjestelmältä. Haastatteluissa korostuivat seuraavat asiat: oikea-aikaisen toimintaa ja päätöksentekoa tukevan tiedon saanti,

organisaatiokohtaisten näkemysten ottaminen huomioon, toiminnan vaikuttavuuden näkyminen ja henkilöstöltä saatavan palautteen tärkeys.

Palautejärjestelmän toteutustavoiksi valitsin mittareiden ja metriikan määrittelyt ja henkilöstöpalautteen keräämisen. Mittareiden ja metriikan määrittelymenetelmäksi valitsin Goal Question Metric -mallin (GQM-malli), joka on ohjelmistokehitykseen suunniteltu menetelmä ohjelmien analysoimiseksi. Koska malli lähtee tavoitteiden asettamisesta ja sen mukaisesta metriikan kehittämisestä, se soveltuu hyvin tietoturvamittareiden kehittämiseen. Tietoturvatoiminta ja tietoturvallisuuden hallinta lähtee aina organisaation tavoitteista. Metriikan kehitys tapahtuu prosessimuotoisesti ja GQM-prosessin järkevä sijoituspaikka on riskianalyysiprosessissa. Olen soveltanut GQM-mallia tietoturvametriikan kehittämiseksi standardin ISO/IEC 27001 asettamille tietoturvatavoitteille.

Henkilöstöpalautteen keräämisen lähtökohdaksi otin tietoturvakulttuuriin esiintuomisen. Tietoturvallisuuden hallinta on ihmisten johtamista ja johtamisen tulosta voidaan ilmentää toiminnan kypsyystasoilla SSE-CMM-standartin mukaisesti. Kypsyystason on ilmettävä tietoturvakulttuurina ja hyvänä tiedonhallintatapana. Valituista menetelmistä 360 asteen palaute -malli kuvaa sekä johtamisen että henkilöstön tietoturvakulttuuria. Tietoturvakulttuurin arviointi on tehtävä säännöllisesti ja voi tehdä vuotuisissa henkilöstökyselyissä tai laatuauditoinnin yhteydessä. Olennaista on, että arvioinneissa on erikseen kysymyksiä tietoturvatoiminnasta. Toinen valittu menetelmä, itsearvioinnit, kuvaa puolestaan henkilöstön tietoturvailmapiiriä. Itsearviointeja on tehtävä organisaation tarpeiden mukaisesti. Yhteisenä tuloksena edellisistä saadaan hallinnollisten menettelyjen tehokkuus ja vaikuttavuus organisaatioiden toiminnassa. Arviointikysymysten tekemiseen sopii edellä mainittu GQM-malli ja tekopaikaksi riskianalyysi.

Työni lopputulos on, että prosessimuotoista toimintaa täytyy ohjata prosessimallien mukaisesti ja tämä ohjaustapa on takaisinkytkentä. Käyttämäni palautejärjestelmämalli on takaisinkytkentä tietoturvatoiminnan tuloksesta tietoturvallisuuden hallintaa ja se kertoo toiminnan tuloksesta suhteessa normiohjaukseen. Palautejärjestelmän ydin on toiminnan mittaaminen ja tulosten analysointi tarkoituksenmukaisella metriikalla.

Palautejärjestelmän on tuotettava oikea-aikaisesti merkityksellistä ja luotettavaa tietoa sitä tarvitseville henkilöille ja organisaatioille. Näin ollen palautejärjestelmän määrittelyissä tärkeimmät vaiheet ovat mitattavien kohteiden ja mittaustulosten analysointitapojen, metriikan, valinta. Valittu GQM-mallia on hyödynnettävissä sekä metriikan muodostukseen että arviointikysymysten tekoon samassa riskianalyysin liitetyssä GQM-prosessissa.

Lopuksi on syytä todeta, että esitetty palautejärjestelmämalli ei ratkaise kaikkia tietoturvaongelmia. Järjestelmä toimii vain siinä ympäristössä, jossa se pystyy keräämään tietoa ja esittämään tiedon analysoinnin tulokset. Organisaatiota vastaan kohdentuva toiminta, joka tapahtuu organisaation ulkopuolelle, ei tuota mittaustuloksia organisaatiolle. Esimerkiksi vakoilu on yleensä toimintaa, jota pyritään tekemään huomaamattomasti ja organisaation ulkopuolella, jos mahdollista. Toisin sanoen tietoturvaa ei voi jättää vain yhden järjestelmän ja menettelyn varaan.

6 Lähdeluettelo

Abbas, A. & El Saddik, A. & Miri, A. 2005. A State of the Art Security Taxonomy of Internet Security: Threats and Countermeasures. GESTS International Transactions on Computer Science and Engineering. Vol 19:1. S. 27-36. ISSN 1738-6438.

Aslam, T. & Krsul, I. & Spafford, E. H. 1996. Use of a Taxonomy of Security Faults. Teoksessa: Proceedings of the 19th NIST-NCSC National Information Systems Security Conference. Baltimore, USA. 22.-25.10.1996. NIST-NCSC. S. 551-560.

Aversano, L. & Bodhuin, T. & Canfora, G. & Tortorella, M. 2004a. A Framework for Measuring Business Processes Based on GQM. Teoksessa: Proseedings of the 37th Hawaii International Conference on System Sciences, Vol 1. Hawaii, USA. 5.-8.1.2004. Washington, DC, USA. IEEE Computer Society. S. 10012.1. ISBN 0-7695-2056-1.

Aversano, L. & Bodhuin, T. & Canfora, G. & Tortorella, M. 2004b. WebEv - A Collaborative Environment for Supporting Measurement Frameworks. Teoksessa: Proceedings of the 37th Hawaii International Conference on System Sciences, Vol 1. Hawaii, USA. 5.-8.1.2004. Washington, DC, USA. IEEE Computer Society. HICSS. S. 10012.1. ISBN 0-7695-2056-1.

Basili, V. R. & Caldiera, G. & Rombach, H. D. 1994. The goal question metric approach. Encyclopedia of Software Engineering, 2.ed. pp. 528-532, John Wiley & Sons, Inc. ISBN 1-54004-8.

Bellovin, S. 2006. On the Brittlenes of Software and the Infeasiblity of Security Metrics. IEEE Security and Privacy. IEEE Computer Society. S. 96. ISSN 1540-7993.

Berander, P. & Jönsson, P. 2006. A Goal Question Metric Based Approach for Efficient Measurement Framework Definition. Teoksessa: Proceeding of 5th ACM-IEEE International Symposium of Empirical Software Engineering (ISESE'06). Rio de Janeiro, Brazil. 21.-22.9.2006. IEEE Press. S. 316-325. ISBN 1-59593-218-6.

Bitterli, P. 2005. Using Control Self-assessment for Risk Management. ISACA Workshop 22.6.2005. Oslo, Norway.

Broderick, J. Stuart. 2005. ISMS, security standards and security regulations. Teoksessa: Information Security Technical Report 11. S. 26-31. ISSN 1363-4127.

Buglione, L. & Abran, A. 2000. Balanced Scorecards and GQM: What are the Differences?. Teoksessa: Proceedings of FESMA/AEMES Software Measurement Conference 2000. Madrid, Spain. 18.-20.10.2000. ISBN 84-688-7161-3.

Caldelli, A. & Parmigiani, M. L. 2004. Management Information System - A Tool for Corporate Sustainability. Journal of Business Ethics. Vol 55:2. S. 159-171.ISSN 0167-4544 (painettu). ISSN 1573-0697 (sähköinen).

Chan, M. & Woon, I. & Kankanhalli, A. 2005. Perceptions of information security at the workplace: linking information security climate to compliant behavior. Journal of Information Privacy and Security. Vol 1:3. S. 18-41. ISSN 1553-6548.

Chapin, D. A. & Akridge, S. 2005. How can security be measured? Information Systems Control Journal. Vol 2. Information Systems Audit and Control Association. ISSN 1526-7407.

Differding, C. & Hoisl, B. & Lott, C. M. 1996. Technology Package for the Goal Question Metric Paradigm. Internal Report 281/96. Department of Computer Science, University of Kaiserslautern, Germany.

Fuggetta, A. & Lavazza, L. & Morasca, S. et al. 1998. Applaying GQM in an Industrial Software Factory. ACM Transactions on Software Engineering and Methodology. Vol. 7:4. S. 411-448. ISSN 1049-331X.

Gray, Á. & Lewis, A. & Fletcher, C. et al. 2003. 360 degree feedback: Best practice guidelines. http://www.psychtesting.org.uk [Online]. 2003. Saatavissa: http://www.psychtesting.org.uk/the-ptc/guidelinesandinformation.cfm. [Viitattu 11.10.2007].

Hellman, G. 2006. From logs to logic: best practices for security information management. EDPACS- The EDP Audit Control, and Security Newsletter. Vol. 33:12. ISSN 0736-6981.

Jaquith, A. 2007. Security metrics. USA, Addison-Wesley. 333 s. ISBN 978-0-321-34998-9.

Jelen, G. F. 1995. A new risk management paradigm for INFOSEC assessments and evaluations. 1995. Teoksessa: Proceedings of the 11th Annual Computer Security Applications Conference.. Los Alamitos, CA, USA: IEEE Computer Society. S. 216-267.

Jelen, G. F. & Jeffrey R. W. 1998. A Practical Approach to Measuring Assurance. Teoksessa: Proceeding of the 14 th Annual Computer Security Applications Conference. Los Alamitos, CA: IEEE Computer Society. S. 333-343.

Jøsang, A. 2001. A Logic for Uncertain Probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. Vol. 9:3. ISSN 0218-4885.

Jøsang, A. & Keser, C. & Dimitrakos, T. 2005. Can We Manager Trust? Teoksessa:

Proceedings of the 3rd International Conference on Trust Management. Paris, France. 23.-26.5.2005. Lectures Notes on Computer Science Vol 3447. ISBN 978-3-540-26042-4.

Kajava, J. & Savola, R. 2005. Towards better information security management by understanding security metrics and measuring processess. EUNIS 2005 - Leadership and Strategy in a Cyber-Infrastructure World. The University of Manchester, UK. 20.-24.6.2005. EUNIS, Paris, France.

Kormos, C. & Givans, N. & Gallagher, L. A. & Bartol, N. 1999. Using security metrics to assess risk management capabilities. Teoksessa: Proceedings of the 22th National Information Systems Security Conference. USA, Arlington. 18-21.10.1999. National Institute of Standards and Technology and National Computer Security Center of the National Security Agency.

Kovacich, G. 1997. Information Systems Security Metrics Management. Computers and Security. VOL 16:7. S. 610-618. ISSN 0167-4048.

Kreidl, O. P. & Frazier, T. M. 2004. Feedback Control Applied to Survivability: a Host-based Autonomic Defense System. IEEE Transactions on Reliability. Vol. 53:1. S. 148-166. ISSN 0018-9529.

Landwehr, C. E. & Bull, A. R. & McDermott, J. P. & Choi, W. S. 1994. A Taxonomy of Computer Program Security Flaws, with Examples. ACM Computing Surveys. Vol. 26:3. S. 211-254. ISSN 0360-0300.

Lavazza, L. 2000. Providing Automated Support for the GQM Measurement Process. IEEE Software. Vol. 17:3. S. 56- 62. ISSN 0740-7459.

Levine, M. 2003. 360 Assessments – Where Do I Start?. http://www.surveyconnect.com. [Online]. 2003. Saatavilla: http://www.surveyconnect.com/surveyconnect_resources.cfm. [Viitattu 10.10.2007]

Miettinen, J. E. 1999. Tietoturvallisuuden johtaminen - näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari. 318 s. ISBN 952-14-0229-6.

Mäkinen, H. 2006. For development of ISMS standards. http://www.yhteiskunnantieto.fi. [Online]. 7.4.2006. Saatavilla: http://www.yhteiskunnantieto.fi/whitepapers.php. [Viitattu 7.9.2007].

Nichols, E. A. & Sudbury, A. 2006. Implementing security metrics initiatives. EDPACS - the EDP Audit Control, and Security Newsletter. Vol. 34:6. S. 10-20. ISSN 0736-6981.
Nonaka, I. 1994. A Dynamic Theory of Organizational Knowledge Creation. Organization Science. Vol. 5:1. S. 14-37. ISSN 1047-7039.

Payne, S. C. 2006. A Guide to Security Metrics. http//www.sans.org. [Online]. 26.6.2006. Saatavilla: http://www.sans.org/reading_room/top25.php. [Viitattu 17.8.2007].

PTS 1/2002. Anon. 2002. Tietotekniikan turvallisuus ja toiminnan varmistaminen. Helsinki: Puolustustaloudellinen suunnittelukunta, Tietojärjestelmäjaosto. 91 s. ISBN 951-53-2406-8.

Ravenel, J. P. 2006. Effective Operational Security Metrics. EDPACS - the EDP Audit Control, and Security Newsletter. Vol. 33:12. S. 10-19. ISSN 0736-6981.

Richards, D & Busch, P. 2000. Measuring, Formalising and Modelling Tacit Knowledge. International Congress on Intelligent Systems and Applications (ISA2000). 12.15.12.2000. Sydney, Australia. International ICSC Congress.

Sademies, A.2004. Process approach to information security metrics in Finnish industry and state institutions. VTT Publications 544. S. 88. ISBN 951-38-6407-3. (pdf url http://www.vtt.fi/inf/pdf/publications/2004/P544.pdf)

Sademies, A. & Savola, R. 2004. Measuring the Information Security Level – a Survey of Practice in Finland. Teoksessa: Proceedings of the 5th Annual International Systems

Security Engineering Association (ISSEA) Conference. Arlington, Virginia. 13-15.10.2004. 10 S.

Sallhammar, K. & Helvik, B. E. & Knapskog, S. J. 2006. Towards a stochastic model for integrated security and dependability evaluation. Teoksessa: Proceedings of the First International Conference on Availability, Reliability and Security. Vienna, Austria. 20.-22.4.2006. IEEE Computer Society. Los Alamitos, CA, USA. S. 156-165. ISBN 0-7695-2567-9.

SANS. 2007. SANS Top-20 Internet Security Attack Targets. http://www.sans.org/top20. [Online]. 15.10.2006. Saatavissa: http://www.sans.org/top20/#h2. [Viitattu 17.9.2007]

Savola, Reijo. 2007. Towards a Security Metrics Taxonomy for the Information and Communications Technology Industry. Teoksessa: Proceedings of International Conference on Software Engineering Advances (ICSEA 2007). Cap Esterel, France. 25.-31.7.2007. S. 60-66. ISBN 0-7695-2937-2.

Schneier, B. 2007. Assurance. Schneier on Security. A blog covering security and security technology http://www.schneier.com/blog. [Online]. 9.8.2007. [Viitattu 21.10.2007]. Saatavissa: http://www.schneier.com/blog/archives/2007/08/assurance.html

Siponen, M. 2000. A Conceptual Foundation for Organizational Information Security Awareness. Information Management and Security. Vol 8:1. S. 31-41. ISSN 0968-5227.

Siponen, M. 2006. Communications of the ACM. Vol. 49:8. S. 97-100. ISSN 0001-0782.

Siponen, M. T. & Kajava, J. 1998. Ontology of Organizational IT Security Awareness - From Theoretical Foundations to Practical Framework.. Teoksessa: 7th Workshop on Enabling Technologies (WETICE'98), Infrastructure for Collaborative Enterprises. 17-19.6.1998. Palo Alto, USA. S. 327-333. ISBN 0-8186-8751-7.

van Solingen, R . & Berghout, E. 1999. The Goal Question Metric Method: A Practical Guide for Quality Improvement of Software Development. Berkshire, England: McGraw-Hill Publishing Company. 216 s. ISBN 007-709553-7.

Stewart, A. 2004. On risk: perception and direction. Computers and Security. Vol 23:5. S. 362-370. ISSN 0167-4048.

Thomson, K-L. & von Solms, R. 2006. Towards an Information Security Competence Maturity Model. Computer Fraud & Security. Vol.2006:5. S. 11-15. ISSN 1361-3723

Tucci, Linda (ed). 2007. Fewer Security Breaches Blamed on Human Error. http://searchcio.techtarget.com. [Online]. 19.9.2007]. [Viitattu 21.10.2007]. Saatavissa: http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci1273058,00.html

VM 2/2005. Salminen, M (toim). 2005. Tulosohjauksen käsikirja. Helsinki: Valtiovarainministeriö. 125 s. ISBN 951-804-531-3.

Williams, Jeffrey R. & Jelen, George F. 1998. A Framework for Reasoning about Assurance. Arca Systems Inc. Document Number ATR 97043.

Ye, N. & Zhang, Y. & Borror, C. M. 2004. Robustness of the Markov-Chain model for cyber-attack detection. IEEE Transactions on Reliability. Vol 53:1. S. 116-123. ISSN 0018-9529.

Yulin, Dai & Shiying, Li & Li, Luo. 2006. Information Relevance Management Model – A New Strategy in Information Security Management in the Outsourcing Industry. Teoksessa: Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science. 10.-12.7.2006. Honolulu, Hawaii, USA. IEEE Computer Society. Los Alamitos, CA, USA. S. 433-438. ISBN 0-7695-2613-6.

Liitteet

Liite 1: Voimassa oleva VAHTI-ohjeistus (28.8.2007)

Ohjeistus on luettavissa Valtiovarainministeriön www-sivuilta: VAHTI-ohjeistus.[33]

VAHTI 2/2000	Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje
VAHTI 3/2000	Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI x/2000	Julkisuuslain mukaisen tietojärjestelmäselosteen laadintasuositus
VAHTI x/2000	Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje
VAHTI 1/2001	Valtion viranomaisen tieturvallisuustyön yleisohje
VAHTI 2/2001	Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 3/2001	Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 6/2001	Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista
VAHTI 1/2002	Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 3/2002	Valtionhallinnon etätyön tietoturvallisuusohje
VAHTI 4/2002	Arkaluontoiset kansainväliset tietoaineistot - käsittelyperiaatteet
VAHTI 1/2003	Valtion tietohallinnon internet-turvallisuusohje
VAHTI 2/2003	Turvallinen etäkäyttö turvattomista verkoista
VAHTI 3/2003	Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 4/2003	Valtionhallinnon tietoturvakäsitteistö
VAHTI 7/2003	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 1/2004	Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006
VAHTI 2/2004	Tietoturvallisuus ja tulosohjaus
VAHTI 3/2004	Haittaohjelmilta suojautumisen yleisohje

33 http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp

VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 5/2004	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 1/2005	Information Security and Management by Results
VAHTI 2/2005	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 3/2005	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2006	Electronic-mail handling instruction for state goverment
VAHTI 5/2006	Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 6/2006	Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 7/2006	Muutos ja tietoturvallisuus – alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 8/2006	Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 9/2006	Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 10/2006	Henkilöstön tietoturvaohje
VAHTI 11/2006	Tietoturvakouluttajan opas
VAHTI 12/2006	Tunnistaminen julkishallinnon verkkopalveluissa

Liite 2: VAHTI-ohjeissa viitattu voimassa oleva lainsäädäntö

Luetteloon on päivitetty ajantasainen lainsäädäntö[34]. Voimassa olevan lainsäädännön tekstin saa www-palveluista Edilex[35] tai Finlex.[36]

Arkistolaki 831/1994
Asetus puolustustaloudellisesta suunnittelukunnasta 239/1960
Asetus Suomen ja Länsi-Euroopan unionin välisen turvallisuussopimuksen. voimaansaattamisesta ja sen eräiden määräysten hyväksymisestä ja sen soveltamisesta annetun lain voimaantulosta 42/1998
Asetus valtion talousarviosta 1243/1992
Asetus viranomaisen toiminnan julkisuudesta 1030/1999
Hallintolaki 434/2003
Henkilökorttilaki 829/1999
Henkilötietolaki 523/1999
Kauppalaki 355/1987
Kuntalaki 365/1995
Laki huoltovarmuuden turvaamisesta 1390/1992
Laki julkisen hallinnon yhteispalvelusta 223/2007
Laki julkisesta työvoimapalvelusta 1295/2002
Laki julkisista hankinnoista 348/2007
Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004
Laki puolustustaloudellisesta suunnittelukunnasta 238/1960
Laki Suomen ja Länsi-Euroopan unionin välisen turvallisuussopimuksen eräiden määräysten hyväksymisestä ja sen soveltamisesta 282/1998
Laki sähköisestä asioinnista viranomaistoiminnassa 13/2003
Laki turvallisuusselvityksistä 177/2002
Laki valtion talousarviosta 423/1988
Laki varallisuusoikeudellisista oikeustoimista 228/1929

34 VAHTI-ohjeissa viitattujen, mutta muuttuneiden lakien, uusinta versiota käytetään (Työsopimuslaki 320/1970 -> 55/2001) eikä kumottuja lakeja ole listattu.

35 http://edilex.fi/saadokset/lainsaadanto/, vaatii rekisteröitymisen, ilmainen TKK:n verkosta.

36 http://www.finlex.fi/fi/laki/ajantasa/

Laki viranomaisen toiminnan julkisuudesta 621/1999
Perustuslaki 731/1999 10§ ja 11§
Rikoslaki 39/1889
Sähköisen viestinnän tietosuojalaki 516/2004
Tekijänoikeuslaki 404/1961
Työsopimuslaki 55/2001
Vahingonkorvauslaki 412/1974
Valmiuslaki 1080/1991
Valtion virkamieslaki 750/1994
Valtioneuvoston ohjesääntö 262/2003
Väestötietolaki 507/1993

Liite 3: Standardien ja suositusten tietoturvan osa-alueet -taulukko.

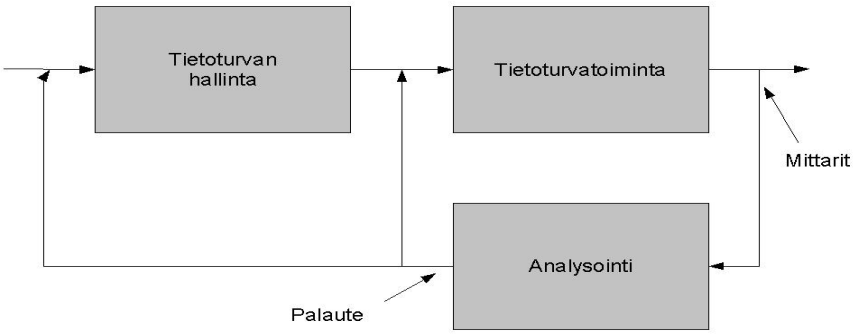
PTS/VAHTI	COBIT	ISO/IEC 27001/27002	NIST SP 800-53	ISO/IEC 21827
Hallinnollinen tietoturvallisuus	Planning and organization	Security policy	Access control	Administer security controls
Henkilöstöturvallisuus	Acquisition and implementation	Organization of information security	Awareness and training	Assess impact
Fyysinen turvallisuus	Delivery and support	Asset management	Audit and accountability	Assess security risk
Tietoaineistoturvallisuus	Monitoring	Human resources security	Certification, accreditation and security assessments	Assess threat
Tietoliikenneturvallisuus		Physical and environmental security	Configuration management	Assess vulnerability
Laitteistoturvallisuus		Communications and operations management	Contingency planning	Build assurance argument
Ohjelmistoturvallisuus		Access control	Identification and authentication	Coordinate security
Käyttöturvallisuus		Information systems acquisition, development and maintenance	Incidence responce	Monitor security posture
		Information security incident management	Maintenance	Provide security input
		Business continuity management	Media protection	Specify security needs
		Compliance	Physical and environmental protection	Verify and validate security
			Planning	Ensure quality
			Personnel security	Manage configuration
			Risk assessment	Manage project risk
			System and services acquisition	Monitor and control technical effort
			System and communication protection	Plan technical effort
			System and information integrity	Define organization's systems engineering process
				Improve organization's systems engineering process
				Manage product line evolution
				Manage systems engineering support environment
				Provide ongoing skills and knowledge
				Coordinate with suppliers

Liite 4: Alkuperäinen kysely

Arvon vastaaja,

Tämä kysely liittyy diplomityöhöni aiheesta Tietoturvan hallinta: palautejärjestelmän vaatimukset ja toteutustavat. Teen diplomityöni tietoturvallisuuspäällikkö Kalevi Hyytiän ohjauksessa. Teknisen korkeakoulun puolelta valvojana on prof. Raimo Kantola Sähköosastolta.

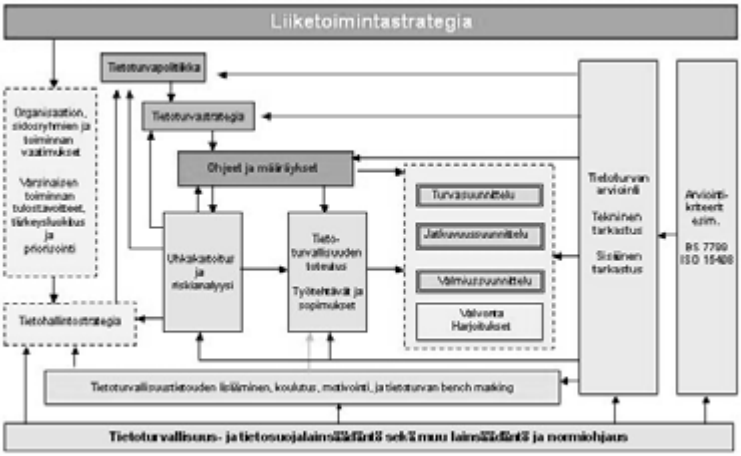
Diplomityöni käsittelee tietoturvatoiminnasta syntyvän datan keräämistä ja käsittelemistä siten, että niistä saadaan ajantasaista ja tarpeellista tietoa tietoturvaprosessien ja -toiminnan ohjaamiseen ja kehittämiseen, siis tietoturvallisuuden hallintajärjestelmän kehittämiseen (Kuva 1). Tietoturvatoiminnan lisäksi ohjaavaa tietoa syntyy muuttuvasta toimintaympäristöstä. Työssäni käytetään toiminnasta nimeä palautejärjestelmä.



Kuva 1: Palautejärjestelmän periaate

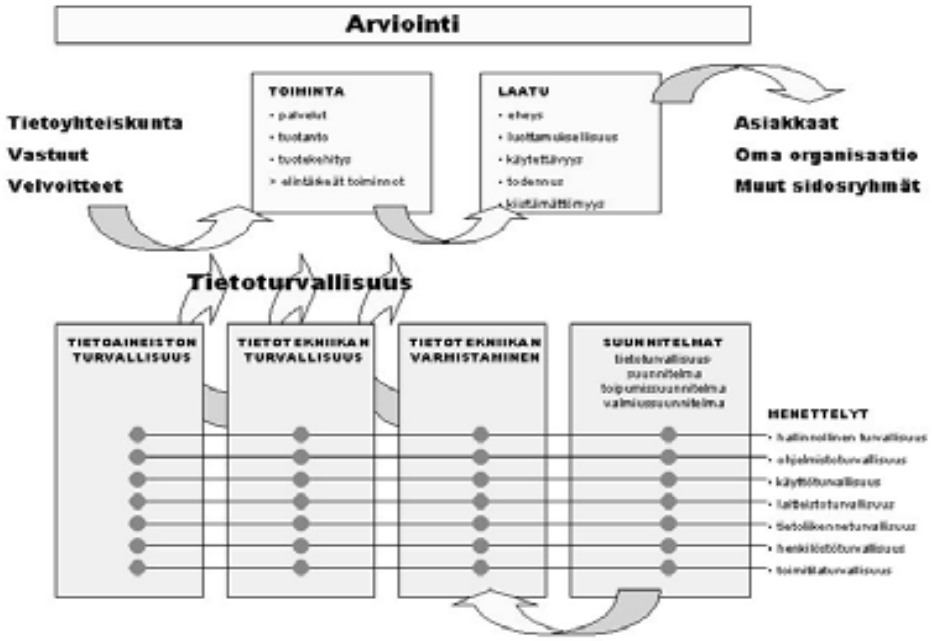
Palautejärjestelmä on osa raportointijärjestelmää, joka tuottaa eri tasoista tietoa samasta datasta mahdollisimman automatisoidusti. Avainsanoja ovat mittaaminen, analysointi ja kokonaiskuvan muodostaminen. Myös aikaulottuvuus on tärkeä: sekä reaaliaikaisuus että pitkän aikavälin muutosten havaitseminen samasta datasta on oltava mahdollista.

Valtionhallinnon tietoturvallisuuden hallintajärjestelmä, joka määrittelee aktiivisen tietoturvatoiminnan viitekehyksen, on määritelty esimerkiksi dokumentissa Vahti 3/2003 (http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/02_tietoturva ohjeet_ja_maaraykset/index.jsp). Hallintajärjestelmän muodostamista ohjaavat lainsäädäntö, sopimusten tuomat velvoitteet ja standardit Kuvan 2 mukaisesti.



Kuva 2: Tietoturvallisuuden hallintajärjestelmä Vahti 3/2003 mukaisesti

Hallintajärjestelmä määrittelee ne tarpeet, jotka konkretisoituvat jokapäiväiseksi tietoturvatoiminnaksi (menettelyt Kuvan 3 mukaan), kuten kulunvalvonta, käyttöoikeuksien hallinta, palomuurien säännöstö, tietoliikenteen valvonta jne. Tämä toiminta tuottaa tavalla tai toisella dataa palautejärjestelmän käsiteltäväksi. Datan muoto riippuu mittaustavasta: hallinnollisia toimia mitataan eri lailla kuin esimerkiksi virustorjuntajärjestelmää.



Kuva 3: Tietoturvallisuuden ja laadun arviointi Vahti 3/2003 mukaisesti

Kyselyn viitekehys on tietoturva, tietoturvan hallinta, operatiivinen tietoturvatoiminta. Tietoturvallisuuden hallintajärjestelmä esiintyy myös nimillä tietoturvallisuuden johtamisjärjestelmä ja tietoturvallisuuden hallinta- ja johtamisjärjestelmä.

Toivon saavani runsaasti mielipiteitänne palautejärjestelmästä. Koska diplomityöni tulee olemaan julkinen, niin toivon, että vastaukset ovat julkaistavissa anonyymisti työni liitteenä. Jos jotain kohtaa tai tietoa ei haluta julkaistavan, niin laitattehan asiasta huomautuksen vastauksiinne.

Ystävällisesti,
Juha Kalander

e. juha@kalander.fi
g. 050-5224918

Kysymykset koskien palautejärjestelmää:

(Kysymykset ovat yleisellä tasolla ja niillä on tarkoitus kartoittaa näkemyksiä palautejärjestelmästä. Mikä se on, mitä se voisi olla? Vastauksissa toivon näkemyksiä Kuvan 1 periaatteen pohjalta)

1. Mikä tietoturvallisuuden palautejärjestelmä teidän mielestänne on?

2. Miten palautejärjestelmän toimii omassa organisaatiossanne?

3. Miten palautejärjestelmä saa tietoa toiminnastanne: automaattisesti, manuaalisesti?

4. Miten palautejärjestelmästä saatua tietoa käsitellään?

5. Miten tietoturvallisuuden palautejärjestelmän pitäisi mielestänne toimia?

6. Mitä tietoa palautejärjestelmästä tarvitaan laatu- ja tulosohjaukseen?

Kysymykset koskien mittaamista:
(Tietoturvan hallinnan kahdeksan osa-aluetta ovat hallinnon , henkilöstö-, fyysinen , tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus (menettelyt Kuvan 3 mukaisesti). Hallinnan ohjaamalla tietoturvatoiminnalla taataan tietojen eheys, luottamuksellisuus ja käytettävyys. Tietoturvatoimintaa mitataan. Vastauksissa voi hyödyntää dokumenttia Tietoturvallisuuden arviointi valtionhallinnossa, Vahti 8/2006 (http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/02_tietoturva ohjeet_ja_maaraykset/index.jsp), jonka dokumentin liitteessä 6 kuvattu mainittujen kahdeksan osa-alueen tarkistuslista. Tehokkaan palautejärjestelmän kannalta mittaamisen pitäisi olla automaattista ja jatkuvaa.)

1. Millaista tietoa tietoturvan hallinnan osa-alueilta palautejärjestelmään kerätään?

2. Millaisia tietoturvamittareita toiminnalle on asetettu, mitä mitataan?

3. Millaisia tietoturvamittareita toiminnalle pitäisi olla, mitä pitäisi mitata?

4. Miten tietoturvamittareista saatua tietoa käsitellään ajatellen palautejärjestelmää?

5. Mikä on automatisoinnin aste?

Liite 5: GQM-mallia sovellettu standardien ISO/IEC 17799:2005 ja ISO/IEC 27001:2005 (Annex A) mukaisten kontrollien metriikan määrittelyihin.

Metriikan määrittelyssä olen käyttänyt seuraavaa kehityslomaketta:

Taulukko 1: Alkuperäinen GQM-malli (Basili et al, 1994)

Goal	Purpose Quality Issue Object Viewpoint	
Question		
Metrics		
Question		
Metrics		

Olen muokannut lomakkeen suomenkieliseen muotoon:

Taulukko 2: Oma käännös GQM-mallin taulukosta

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	
Kysymys		
Metriikka		
Kysymys		
Metriikka		

Aluksi tarkempi esimerkki siitä, miten ISO/IEC 27001 tietoturvatoiminnan osa-alue on purettu yllä olevaan lomakkeeseen. Esimerkkinä standardin ensimmäinen osa-alue: tietoturvapolitiikka (Security policy). Lopuista osa-aluista on valittu kaksi vaatimusta ilmentävää kontrollia ja tehty niistä GQM-lomake. Kuhunkin lomakkeeseen olen tehnyt kaksi kysymystä ja niitä vastaavat metriikat. Käytössäni on ollut standardin englannin-

kielinen versio, joten lainaukset ovat siitä enkä ole suomentanut niitä. GQM-lomakkeelle on sijoitettu suomenkieliset vapaamuotoisesti käännetyt termit. Todettakoon vielä, että standardissa on 11 tietoturva-aluetta, joissa 39 kontrollitavoitetta, joita tarkastellaan 131 kontrollin avulla. Standardista ISO/IEC 17799 saadaan kaikkiaan yli 1100 kontrolloitavaa elementtiä, joilla voidaan kontrollien toteutumista tarkastella. Jokaisesta elementistä voi tehdä kysymys/vastausparin. Toisaalta GQM-mallilla havaitaan, että useat kontrollielementit ovat yhteisiä monille kontrolleille.

Lainaus standardista ISO/IEC 27001:2005 (E):

> ***”A.5 Security policy***
>
> ***A.5.1 Information security policy***
>
> *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
>
> A.5.1.1 Information security policy document
>
> *Control*
>
> An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.
>
> A.5.1.2 Review of the information security policy
>
> *Control*
>
> The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.”

Lomakkeen kohta Tavoite, joka jakautuu neljään osaan, saadaan tietoturvan osa-alueen Objective-kohdasta (hallintatavoite) osittain seuraavasti:

> Tarkoitus: To provide management direction and support
>
> Laatutekijä: accordance with business requirements and relevant laws and reglations
>
> Kohde: Information security policy document
>
> Näkökulma: Management

Tavoitteen kohta Kohde saadaan osa-alueen (Clause, A.5) alakohdasta (Main security category, A.5.1), joka jakautuu kontrolloitaviin kohtiin (A.5.1.1, A.5.1.2). Osa kohteista voi tulla hallintatavoitteesta.

Kysymykset saadaan konrollilauseesta (Control, hallintavaatimus). Tukea kysymyksille saadaan hallintatavoitteesta. Esimerkiksi yllä olevasta lauseesta A.5.1.1 voidaan poimia seuraavat avainsanat kysymyksien pohjaksi: ”approved by management, published and communicated, all employees and relevant external parties.” Lisäksi tietoturvapolitiikan sisältöä voidaan kartoittaa hallintatavoitteen kohdilla (laatutekijät): ”business requirements ja relevants laws and regulations.”

Metriikkaa varten sisältöä saa esimerkiksi kontrollin toteutusohjeista (ISO/IEC 17799:2005), joita kohdalle A.5.1.1 on standardissa annettu 6 kappaletta. Metriikaksi pääsääntöisesti pitää saada lukuja (prosentteja, euroja, tunteja), mutta tarvittaessa kyllä/ei-taso on riittävä. Erityisesti näin silloin, kun metriikka perustuu auditointiin.

Edellä esitetyn purun perusteella voidaan tehdä GQM-mallin mukainen lomake koskien tietoturvapolitiikkaa ja tarkemmin sen dokumentointia:

GQM-taulukko: A.5.1: A.5.1.1

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Johdon ohjaus ja tuki tietoturvalle Liiketoiminnan vaatimusten, lakien ja määräysten huomioiminen Tietoturvapolitiikkadokumentti Organisaation johto
Kysymys		Onko tietoturvapolitiikka julkaistu?
Metriikka		% henkilöstöstä saanut tietoturvakoulutuksen, jossa politiikka käyty läpi
Kysymys		Miten tietoturvapolitiikka on ilmaistu kolmansille osapuolille?
Metriikka		Sopimusten määrä, joissa politiikka tai osa siitä on osana sopimusta

Edellä olevien esimerkkien lisäksi seuraavia kysymyksiä voi esittää: Onko johdon tekemää tietoturvapolitiikka? Mikä tärkein lainsäädäntö, joka koskee organisaatiota? Mitä liiketoimintavaatimuksia on? Näkökulma voisi olla myös henkilöstöhallinto, joka vastaa koulutuksesta tai lakiosasto, joka vastaa sopimusten ja organisaation toiminnan lainmukaisuudesta.

On huomattava, että ISO/IEC 27001 sisältää paljon vaatimuksia ja kontrolleja, jotka sopivat paremmin konsultin arvioinnin kohteeksi. Tietoturvapolitiikka on yksi tällainen, jossa sisällöstä on vaikea tehdä automatisoitavaa numeromuotoista metriikkaa.

Seuraavassa loput GQM-mallin kaavakkeet ISO/IEC 27001:sta valituille tietoturvan osa-alueiden kontrolleille. Tekijänoikeussyistä kontrolleista on vain numerotiedot, jotka vastaavat standardin Annex A numerointia. Edellisen esimerkin esitys on: GQM-taulukko: A.5.1: A.5.1.1.

ISO/IEC 27001 tietoturvatoiminnan osa-alue: tietoturvapolitiikka (Security policy)

GQM-taulukko: A.5.1: A.5.1.2

Tavoite	Tarkoitus	Johdon ohjaus ja tuki tietoturvalle
	Laatutekijä	Liiketoiminnan vaatimusten, lakien ja määräysten huomioiminen
	Kohde	Tietoturvapolitiikkadokumentin ylläpito
	Näkökulma	Organisaation johto
Kysymys		Onko tietoturvapolitiikalle määritelty säännölliset tarkastukset?
Metriikka		Tarkastusten aikataulu
Kysymys		Mitataanko tietoturvapolitiikan vaikutusta?
Metriikka		Tietoturvakulttuurin mittaus

ISO/IEC 27001 tietoturvatoiminnan osa-alue: tietoturvallisuuden organisointi (Organization of information security):

GQM-taulukko: A.6.1: A.6.1.5

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Organisaation tietoturvallisuuden hallinta Tiedon luottamuksellisuus Salassapitosopimukset Organisaation johto
Kysymys		Onko työsuhteeseen liitetty yleistä salassapitosopimusta?
Metriikka		Kyllä / ei / Salassapitosopimuksen kesto työsuhteen päätyttyä
Kysymys		Onko erillisiä salassapitosopimuksia?
Metriikka		Henkilökohtaisten salassapito-sopimusten määrä ja kesto / sopimus

GQM-taulukko: A.6.2: A.6.2.1

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Organisaation tietoturvallisuuden hallinta Pääsy- ja käyttöoikeudet Kolmannet osapuolet Käyttöoikeuksien hallinta
Kysymys		Kuinka monta ulkoista osapuolta organisaation tietojärjestelmiin pääsee?
Metriikka		Osapuolten määrä
Kysymys		Miten ulkoisten osapuolten luotettavuus on varmistettu?
Metriikka		% luotettavuuslausuntoja kaikista ulkoisista osapuolista

ISO/IEC 27001 tietoturvatoiminnan osa-alue: suojattavien kohteiden hallinta (Asset management)

GQM-taulukko: A.7.1: A.7.1.1

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Omaisuuden hallinta Tietovarantojen tunnistaminen Omaisuusvastuut Tiedon ja järjestelmien omistajat
Kysymys		Onko tietovarannot tunnistettu ja luetteloitu?
Metriikka		Tietovarantojen määrä / tietueet
Kysymys		Onko tietojärjestelmät tunnistettu ja luetteloitu?
Metriikka		Tietokoneiden, tietoliikennelaitteiden, siirrettävien medioiden määrä

GQM-taulukko: A.7.2: A.7.2.1

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Tiedon suojan varmistaminen Tiedon luokittelu arvon, luokittelun ja lakien mukaisesti Tietovaranto Tietovarannon omistajat
Kysymys		Onko tiedot ja järjestelmät luokiteltu kriittisyyden perusteella?
Metriikka		Kriittisten tietojen ja järjestelmien määrä
Kysymys		Onko tiedoille tehty arvoluokitus?
Metriikka		Tietojen määrä / arvoluokka

ISO/IEC 27001 tietoturvatoiminnan osa-alue: inhimillisten resurssien turvallisuus (Human resources security)

GQM-taulukko: A.8.1: A.8.1.1

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Varkauksien, petosten ja väärinkäytösten vähentäminen Vastuiden ja roolien määrittely Rekrytointi Henkilöstöhallinto
Kysymys		Onko työtehtävät luokiteltu?
Metriikka		Luokiteltujen määrä luokittain
Kysymys		Onko käytössä taustojen selvitys rekrytoinnissa?
Metriikka		Kyllä / ei / tehdyt selvitykset

GQM-taulukko: A.8.3: A.8.3.1

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Väärinkäytösten estäminen Käyttöoikeuksienhallinta Työsuhteen päättyminen tai muutos Henkilöstöhallinto
Kysymys		Onko kirjanpito työtekijän hallussa olevasta omaisuudesta?
Metriikka		Kyllä / ei / omaisuuden arvo / hlö
Kysymys		Kerrotaanko salassapitovelvollisuudet työsuhteen päättyessä?
Metriikka		Kyllä / ei

ISO/IEC 27001 tietoturvatoiminnan osa-alue: fyysinen - ja ympäristöturvallisuus (Physical and environmental security)

GQM-taulukko: A.9.1: A.9.1.1

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Suojata omaisuus väärinkäytöksiltä Fyysinen tietoturva Toimi- ja laitetilojen hallinta Omaisuudenhallinta (talous)
Kysymys		Onko toimi- ja laitetilat luokiteltu?
Metriikka		Luokiteltuja tiloja / luokitus
Kysymys		Kuinka kriittisiä tiloja valvotaan?
Metriikka		Hälytysjärjestelmien määrä / tila

GQM-taulukko: A.9.2: A.9.2.1

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Suojata omaisuus väärinkäytöksiltä Fyysinen tietoturva Laitteiden sijoitus ja suojaus Omaisuudenhallinta (talous)
Kysymys		Onko laitteet sijoitettu luokittelun mukaisiin tiloihin?
Metriikka		luokiteltuja laitteita / laitteiden määrä / luokiteltu tila
Kysymys		Onko laitetiloissa fyysisten olosuhteiden valvonta?
Metriikka		Valvottujen tilojen määrä / laitetilojen määrä

ISO/IEC 27001 tietoturvatoiminnan osa-alue: tietoliikenteen ja toiminnan hallinta (Communications and operations management)

GQM-taulukko: A.10.1: A.10.1.1

Tavoite	Tarkoitus	Oikean ja turvallisen operoinnin toteuttaminen
	Laatutekijä	Käyttöturvallisuus
	Kohde	Operoinnin ohjeet
	Näkökulma	Asiakirjahallinto
Kysymys		Onko operoinnilla ohjeet kaikkiin järjestelmiin?
Metriikka		Ohjeet / järjestelmä / järjestelmien ja ohjeiden määrä
Kysymys		Onko ohjeiden ylläpidolle määritelty menettelyt?
Metriikka		Kyllä / ei

GQM-taulukko: A.10.4: A.10.4.1

Tavoite	Tarkoitus	Suojata ohjelmia ja tietoja muutoksilta tai tuhoutumiselta
	Laatutekijä	Tiedon eheys ja käyttöturvallisuus
	Kohde	Haittaohjelmilta suojautuminen
	Näkökulma	Tietohallinto
Kysymys		Onko käytössä ohjelmistoja haittaohjelmia ja viruksia vastaan?
Metriikka		Ohjelmistojen määrä / järjestelmä
Kysymys		Valvotaanko torjuntaohjelmistojen toimintaa?
Metriikka		Hälytysten määrä / henkilö ja laite

ISO/IEC 27001 tietoturvatoiminnan osa-alue: pääsynvalvonta (Access control)

GQM-taulukko: A.11.1: A.11.1.1

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Liiketoimintavaatimusten huomioiminen pääsynvalvonnassa Tiedon suojaaminen Pääsyoikeuspolitiikka Liitetoimintayksiköt
Kysymys		Onko liiketoiminnan tarvitsemat tiedot tunnistettu?
Metriikka		Tiedot ja tietovirrat / liiketoiminta-sovellus
Kysymys		Onko työtehtäväkohtaiset käyttäjäprofiilit?
Metriikka		Käyttäjäprofiilien määrä / käyttäjien määrä / työtehtävien määrä

GQM-taulukko: A.11.2: A.11.2.1

Tavoite	Tarkoitus Laatutekijä Kohde Näkökulma	Käyttöoikeuksien mukainen pääsy tietoihin ja järjestelmiin Luottamuksellisuus, käytettävyys Käyttöoikeuksien myöntäminen Henkilöstöhallinto
Kysymys		Onko käyttöoikeuksien myöntämi-selle määrämuotoinen prosessi?
Metriikka		Kyllä / ei
Kysymys		Onko tietojärjestelmäkohtaisia luetteloita oikeuksien haltijoista?
Metriikka		Oikeuden haltijoita / oikeusryhmä / järjestelmä

ISO/IEC 27001 tietoturvatoiminnan osa-alue: tietojärjestelmien hankinta, kehitys ja ylläpito (Information system acquisition, development and maintenance)

GQM-taulukko: A.12.1: A.12.1.1

Tavoite	Tarkoitus	Tietoturvatarpeiden huomioiminen järjestelmäkehityksessä
	Laatutekijä	Käyttöturvallisuus
	Kohde	Tietojärjestelmien vaatimusten määrittely ja analysointi
	Näkökulma	Järjestelmäkehitys
Kysymys		Onko liiketoimintavaatimukset kirjattu järjestelmien kehitys-vaatimuksiin?
Metriikka		Kyllä / ei
Kysymys		Onko määrämuotoinen tapa huomioida tietoturvavaatimukset järjestelmäkehityksessä?
Metriikka		Kyllä / ei

GQM-taulukko: A.12.2: A.12.2.1

Tavoite	Tarkoitus	Estää tietojen virheet, katoaminen ja väärinkäytökset
	Laatutekijä	Käyttöturvallisuus
	Kohde	Syöttötietojen tarkistus
	Näkökulma	Järjestelmäkehitys
Kysymys		Onko järjestelmätestauksessa dokumentoitu tapa syöttötietojen tarkistamiseen?
Metriikka		Kyllä / ei
Kysymys		Kerätäänkö lokitietoja syöttövirheistä?
Metriikka		Virheiden määrä / sovellus

ISO/IEC 27001 tietoturvatoiminnan osa-alue: tietoturvatapahtumien hallinta
(Information security incident management)

GQM-taulukko: A.13.1: A.13.1.1

Tavoite	Tarkoitus	Mahdollisimman nopea tietoturva-tapahtumien ja -poikkeamien raportointi
	Laatutekijä	Vasteaika tapahtumasta raportointiin
	Kohde	Tietoturvatapahtumien raportointi
	Näkökulma	Tietoturvallisuuden hallinta
Kysymys		Onko tietoturvatapahtumille ja -poikkeamille määritelty vasteajat?
Metriikka		Vasteaika / tapahtumatyyppi / järjestelmä
Kysymys		Mitataanko raportointiaikoja?
Metriikka		Raportointi määräajassa / yli määräajan / keskiarvo

GQM-taulukko: A.13.2: A.13.2.2

Tavoite	Tarkoitus	Tietoturvatapahtumien hallinta ja hallinnan kehittäminen
	Laatutekijä	Yhtenäiset menettelyt ja tehokkuus
	Kohde	Tietoturvatapahtumista oppiminen
	Näkökulma	Tietoturvallisuuden johtaminen
Kysymys		Kirjataanko tietoturvatapahtumat luokitellusti?
Metriikka		Tietoturvatapahtumia / luokka
Kysymys		Mitataanko tietoturvatoimien kustannuksia ja työmääriä?
Metriikka		Henkilötyötunteja / tietoturva-tapahtuma

ISO/IEC 27001 tietoturvatoiminnan osa-alue: toiminnan jatkuvuuden hallinta (Business continuity management)

GQM-taulukko: A.14.1: A.14.1.1

Tavoite	Tarkoitus	Estää tai minimoida liiketoiminnan ja kriittisten prosessien katkokset
	Laatutekijä	Käytettävyys
	Kohde	Liitetoiminnan valmiussuunnitelmat
	Näkökulma	Liiketoiminnan johto
Kysymys		Onko toiminnan keskeytysten vaikutukset arvioitu?
Metriikka		Hinta / tunti
Kysymys		Onko kriittiset tiedot määritelty?
Metriikka		Tietojen määrä / toiminne

GQM-taulukko: A.14.1: A.14.1.2

Tavoite	Tarkoitus	Estää tai minimoida liiketoiminnan ja kriittisten prosessien katkokset
	Laatutekijä	Käytettävyys
	Kohde	Liiketoiminnan jatkuvuus ja riski-analyysi
	Näkökulma	Liiketoiminnan johto
Kysymys		Onko liiketoimintayksiköt mukana riskianalyysissä?
Metriikka		Kyllä / ei
Kysymys		Onko toimintojen ja järjestelmien riippuvuus toisistaan kuvattu liiketoimintayksiköille?
Metriikka		Kyllä / ei

ISO/IEC 27001 tietoturvatoiminnan osa-alue: vaatimusten mukaisuus (Compliance)

GQM-taulukko: A.15.1: A.15.1.1

Tavoite	Tarkoitus	Lakien, määräysten ja sopimusten mukainen toiminta
	Laatutekijä	Lainmukaisuus
	Kohde	Voimassa olevien lakien tunnistaminen
	Näkökulma	Organisaation johto
Kysymys		Onko lakien, määräysten ja sopimusten vaatimukset selvitetty?
Metriikka		Vaatimukset / järjestelmä
Kysymys		Ylläpidetäänkö vaatimusluetteloa muutosten mukaisesti?
Metriikka		Ylläpidon teko muutoshetkestä aikana

GQM-taulukko: A.15.3: A.15.3.1

Tavoite	Tarkoitus	Järjestelmien auditoinnin järjestäminen tehokkaasti toimintaa häiritsemättä
	Laatutekijä	Käytettävyys
	Kohde	Tietojärjestelmien auditointi
	Näkökulma	Tarkastus
Kysymys		Onko auditointisuunnitelmat olemassa?
Metriikka		Kyllä / ei / järjestelmäkohtaisesti
Kysymys		Onko auditoinnin menetelmät, tarpeet ja vastuut dokumentoitu?
Metriikka		Kyllä / ei / järjestelmäkohtaisesti