Tietoturvallisuuden hallinta: palautejärjestelmän vaatimukset ja toteutustavat

Diplomityöesitelmä
29.1.2008

Juha Kalander

Sisältö

- Esittely
- Tutkimusongelma
- Käytetyt metodit
- Työn sisällysluettelo
- Normiohjaus
- Hallintajärjestelmä
- Palautejärjestelmä
- Lopputulema
- Jatko

Esittely

- Työ tehty Puolustusvoimille 3/2007-11/2007
- Ohjaajana Kalevi Hyytiä Pääesikunta
- Valvojana prof. Raimo Kantola TKK

Tutkimusongelma

- VAHTI 1/2001: Tietoturvallisuuden ylläpito edellyttää jatkuvaa tietotototurvallisuuden seurantaa, sen perusteella ylimmälle johdolle tapahtuvaa raportointia sekä korjaavia toimenpiteitä.

- Miten palautejärjestelmä määritellään?
- Mitä vaatimuksia sille pitää asettaa?
- Mitä toteutustapoja on?

Käytetyt metodit

- Kirjallisuustutkimus
- Henkilöhaastattelu

Työn sisällys

Esipuhe

Sisällys

1 Johdanto

2 Normiohjaus

3 Tietoturvallisuuden hallintajärjestelmä

4 Tietoturvallisuuden hallinta: palautejärjestelmä

5 Pohdinta ja johtopäätökset

6 Lähdeluettelo

Liitteet

Normiohjaus

- Tärkeimmät lait: julkisuuslaki, arkistolaki, henkilötietolaki, valmiuslaki, viestinnän tietosuojalaki, perustuslaki
- Tärkeimmät standardit: ISO 27000 -sarja, ISO 21827, COBIT, Common Criteria, NIST 800 -sarja
- VAHTI-ohjeistus

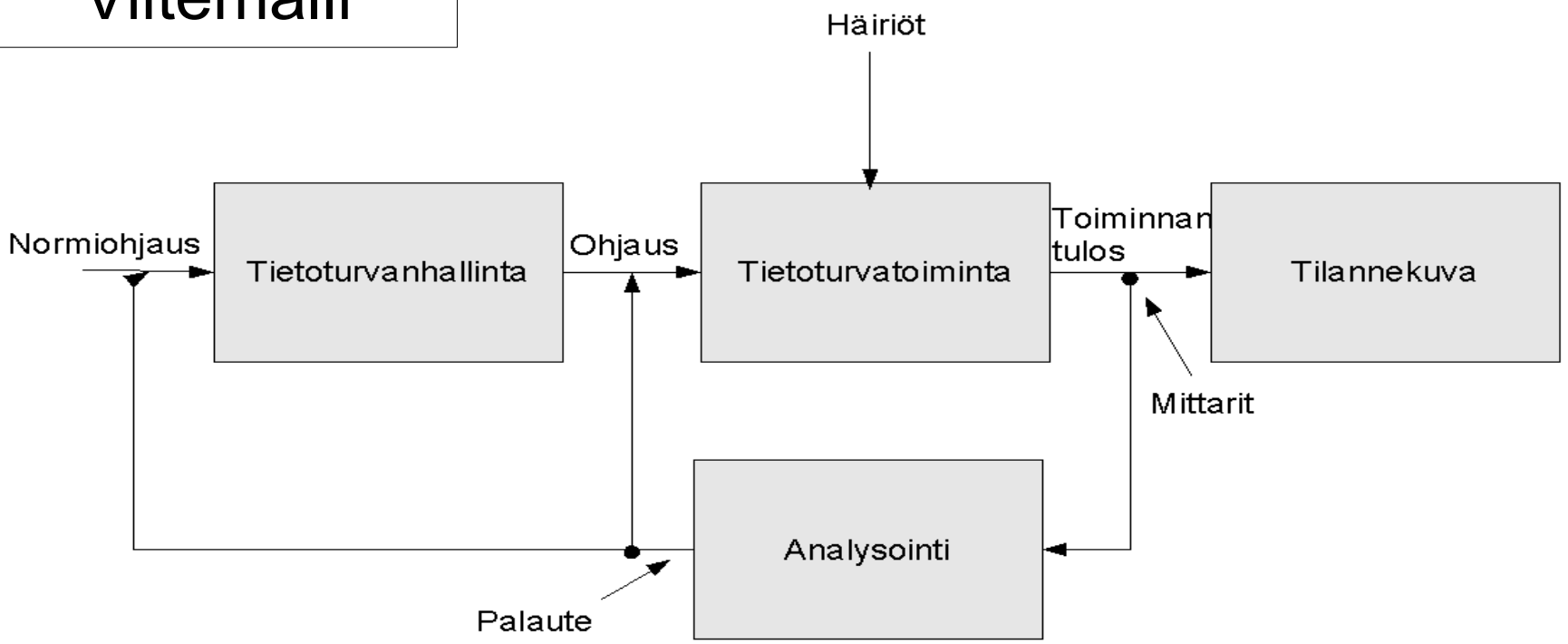
Hallintajärjestelmä

- Tietoturvallisuuspolitiikka ja toimintaperiaatteet
- Tietoturvallisuusstrategia
- Riskianalyysi
- Tietoturvallisuussuunnitelma ja -ohjeet
- Jatkuvuus- ja toipumissuunnitelma
- Valmiussuunnitelma
- Tietoturvallisuuden tulosohjaus
- Tietoturvallisuuden toteutustapa, organisointi ja vastuut
- Vuosisuunnitelmat ja budjetit
- Raportointi

Viite: VAHTI 3/2003

Palautejärjestelmä

Viitemalli



jatkuu ...

Palautejärjestelmä

Kirjallisuustutkimus:

- Hallintajärjestelmät
- Johtaminen
- Kehittäminen
- Mittaaminen/metriikka
- Riskienhallinta
- Taksonomiat
- Varmuudesta

Henkilöhaastattelut:

- Johtaminen
- Eri tasot
- Prosessituki
- Päätöksen teko
- Automatisointi
- Vaikuttavuus
- Läpinäkyvyys

jatkuu ...

Palautejärjestelmä

- Vaatimuksia edellisten perusteella
  - hallinnan kannalta
  - toiminnan kannalta
  - analysoinnin kannalta
- Palautejärjestelmän tuotettava oikea-aikaista ja oikein kohdennettua tietoa eri organisaatio-tasoille tietoturva-toiminnan tehokkuudesta ja tilannekuvan toden-mukaisuudesta
- Trendit
- Tietoturvakulttuurin taso

jatkuu ...

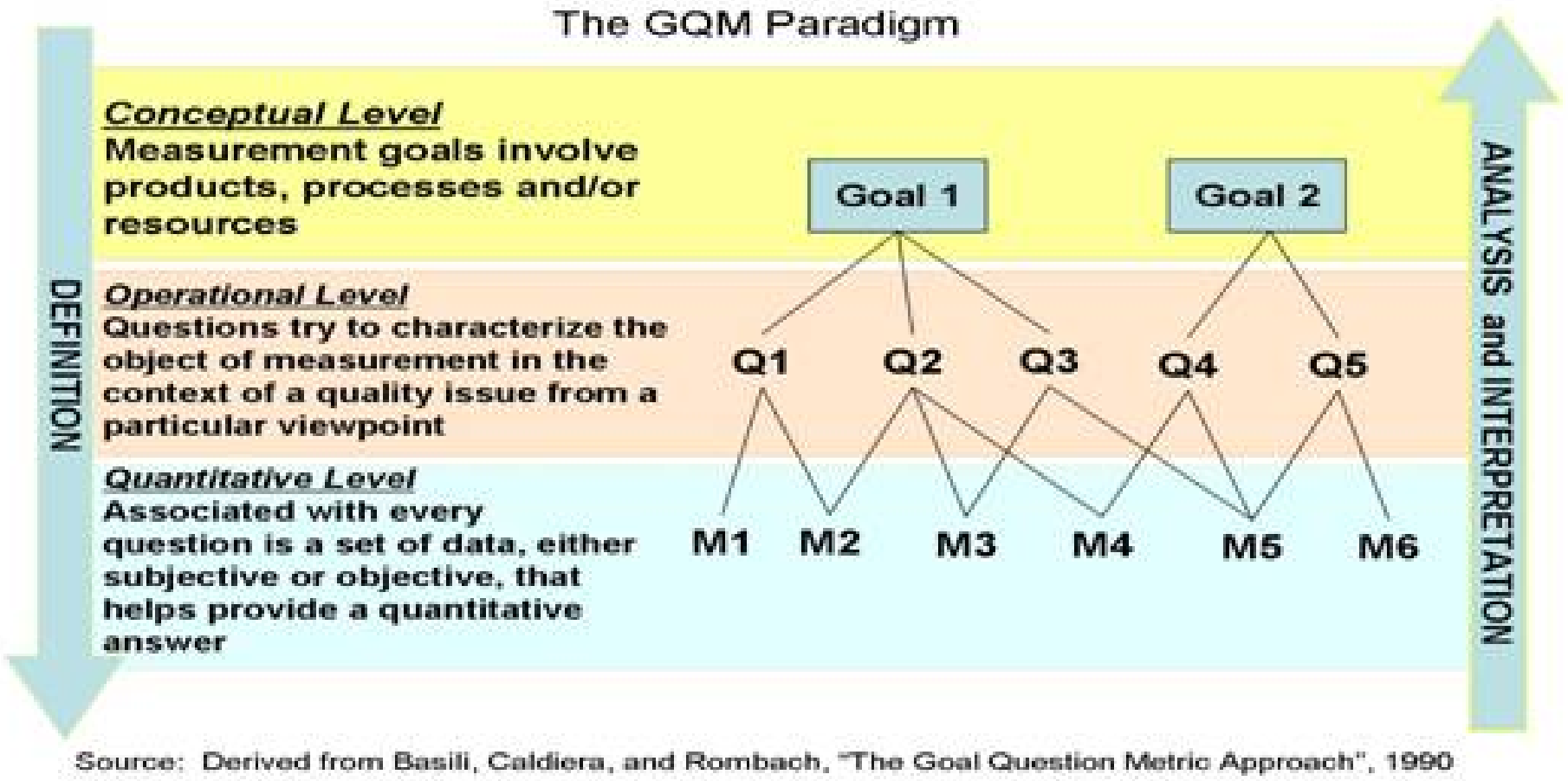
Palautejärjestelmä

- Takaisinkytkentä kulminoituu mittaamiseen ja mittaustulosten analysointiin (metriikka)
- Tietoturvallisuuden johtaminen on ihmisten johtamista

- Metriikan kehittäminen -> Goal Question Metric -malli
- Henkilöstön palautteen kerääminen (tietoturvakulttuuri) -> 360 asteen palaute -malli

jatkuu ...

Palautejärjestelmä



Source: Derived from Basili, Caldiera, and Rombach, "The Goal Question Metric Approach", 1990

jatkuu ...

Palautejärjestelmä

- 360 asteen palaute -mallissa saadaan näkemys
  - esimiestyöstä
  - alaisista
  - kollegoista
- Tietoturvakulttuurin mittaaminen kypsyystasomallin mukaisesti
- Tietoturvailmapiirin mittaaminen
- Tukena itsearvioinnit

jatkuu ...

Palautejärjestelmä

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

GQM-taulukko: A.5.1: A.5.1.2
ISO/IEC 27001 tietoturvatoiminnan osa-alue: tietoturvapolitiikka

Lopputulema

- Hallinnan ja toiminnan vaikuttavuus tietoturvaan
- Prosessimuotoisen toiminnan mittaaminen ja ohjaaminen prosessimallin mukaisesti (takaisin-kytkentä)
- Riskienhallinnan ja riskianalyysin tärkeys
- Standardin ja mallin valinta tärkeää
- Käytetty palautejärjestelmän viitemalli ei ratkaise kaikkea, esimerkiksi vakoilu

Jatko

- Tekniset toteutusmallit ja -tavat
- Tietoturvan oppimisympäristö
- Päätöksenteon ja epävarmuuden mallintaminen: Markov-prosessi, subjektiivinen logiikka