



TULLI
TULL • CUSTOMS

**Tiedätkö, olet oman elämäsi
riskienhallintapäällikkö! Miten sovellat
riskienhallintaa omassa työssäsi?**

Pyry Heikkinen

Taustaa



ICT-tietoturvapääallikkö
Tullissa



OWASP Helsingin
hallituksen jäsen



VAHTI-sihteeristön jäsen



LinkedIn: [pyryheikkinen](https://www.linkedin.com/in/pyryheikkinen)

Tietoturvan ja
riskien
hallinta

ISC²
CISSP

ISACA
CISM

ITIL v3
Foundation

Tietosuoja ja
yksityisyyden
suoja

IAPP
CIPP/E

IAPP
CIPT

PRINCE2
Foundation

Tietoturva-
arkkitehtuuri

SABSA
SCF

CSA
CCSK

TOGAF 9
Certified

Kuka tekee riskienhallintaa?



- Me kaikki hallitsemme riskejä jatkuvasti, esim.
 - kun jätämme avaamatta epäilyttävän liitetiedoston
 - lähetämme viestin sähköpostilla tai lähetyksen postissa
 - kun lukitsemme tietokoneen tai työtilan kahvitauon ajaksi
 - kun suljemme kahvinkeitin päिवän päätteeksi
 - hankimme vakuutuksia tai ulkoistettuja palveluita
 - kun valitsemme toimittajaa osana hankintaa
 - suunnittelemme projektia tai hanketta
 - teemme vuosi- tai työvuorosuunnittelua



Mikä on riski?

”Tapahtuma tai tekijä, joka voi vaikuttaa kielteisesti tehtävien hoitamiseen, tavoitteiden saavuttamiseen tai toimintaan”

Työntekijälle on lähetetty maililla kiristyshaitta-ohjelma

Virustorjunta ei huomaa tätä ja henkilö ei osa varoa viestiä

Haittaohjelma lukitsee viraston tietokoneet

Viraston toiminta keskeytyy viikoksi

Juurisyys

- ”uhka”
- ”hyökkäys”

Heikkous

- ”alttius”
- ”haavoittuvuus”

Vaikutus

- ”seuraus”
- ”tapahtuma”

Vaikutus toimintaan

Käynnissä on liikaa projekteja samaan aikaan

Henkilöstöä on liian vähän ja kuormitusta ei seurata

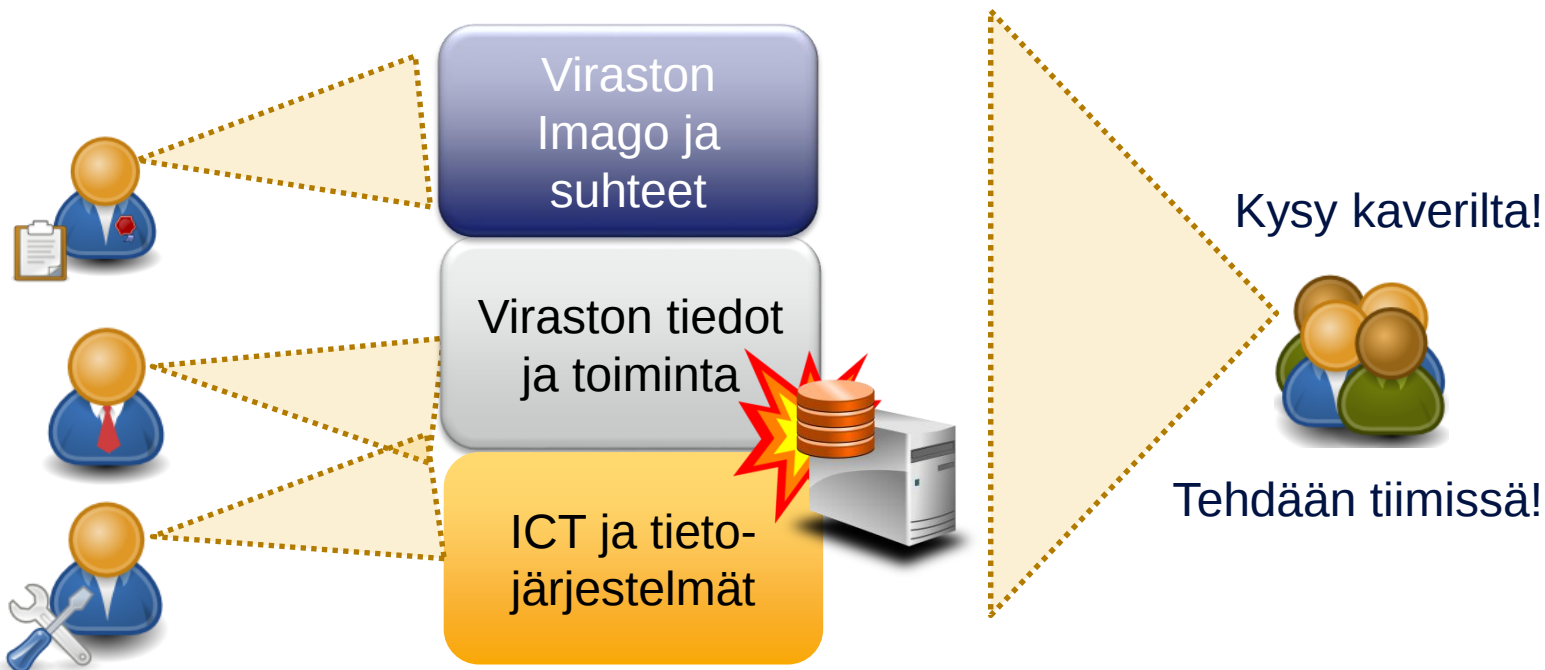
Laatu kärsii ja henkilöstö palaa loppuun

Lakisääteisiä muutoksia ei saada tehtyä

Miten riskejä ja uhkia voi tunnistaa?



Miten arvioida riskin todennäköisyyttä ja vaikutusta?



Mitä voisi tapahtua riskin toteutuessa?

Pysähdy ja
tutki alitajuntaa



Miten riskejä hallitaan?



- Ei aloiteta (vielä) uutta toimintaa tai hanketta
- Luovutaan riskialttiista toiminnasta
- Ei lähdetä työmatkalle riskimaahan

Vältetään
riski

- Muutetaan toimintaa
- Otetaan suojakeinoja käyttöön
- Tarkastetaan toimintaa tai sopimusvaatimuksia

Vähennetään
riskiä

Siirretään tai
jaetaan riski

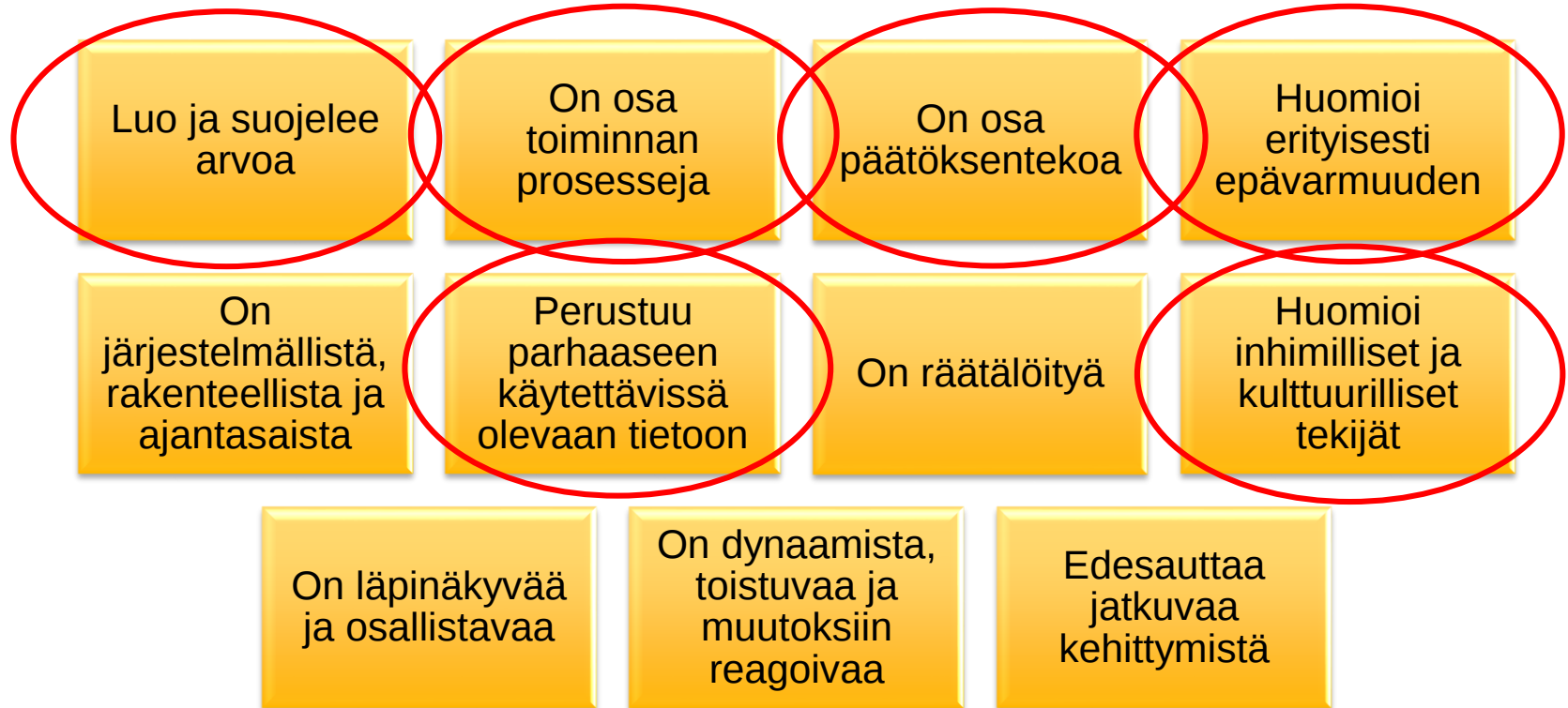
Otetaan riski
(harkitusti)

- Vakuutukset
- Leasing
- Ulkoistus (esim. palvelut ja ICT)

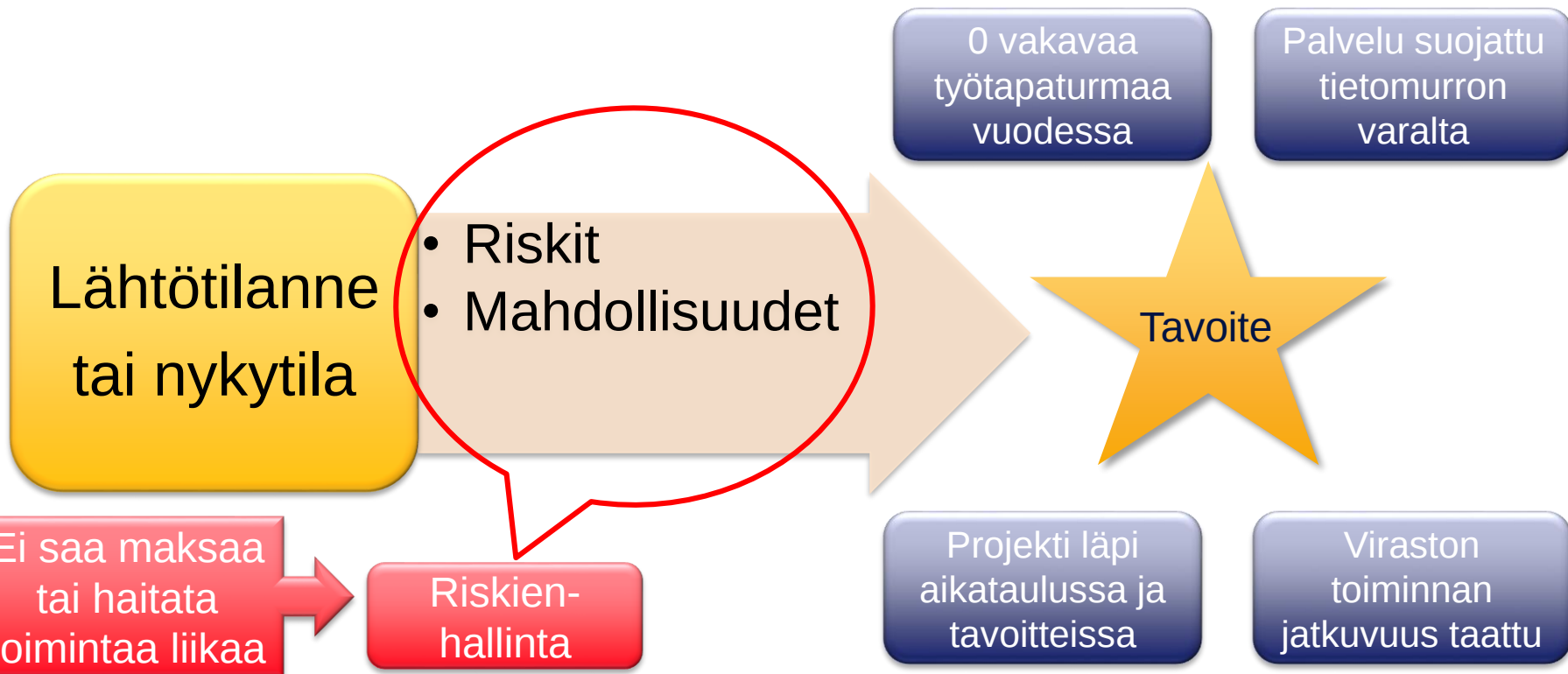
- Otetaan riski ja varaudutaan siihen
- Otetaan harkiten jäljelle jäänyt riski



Tehokas riskienhallinta..



Riskienhallinta, joka luo ja suojelee arvoa



Riskienhallinta, joka on osa toiminnan prosesseja



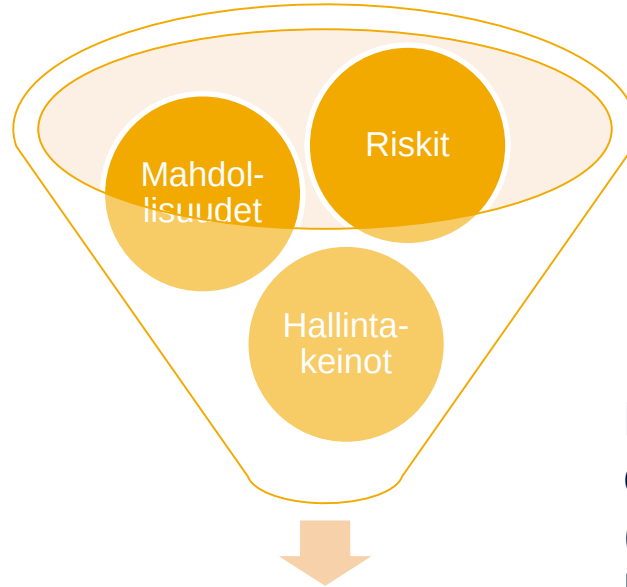
Riskienhallinta, joka on osa päätöksentekoa

Esim. Otetaanko käyttöön uusi virastolle kriittinen sovellus?

Jota ei olla ehditty kunnolla testata

Joka säästäisi merkittävästi joka kuukausi

Vanhaan sovellukseen ei pystytäkään palaamaan helposti



Otetaanko riski?



Riskin omistaja (vastuunkantaja)

Ohjausryhmä

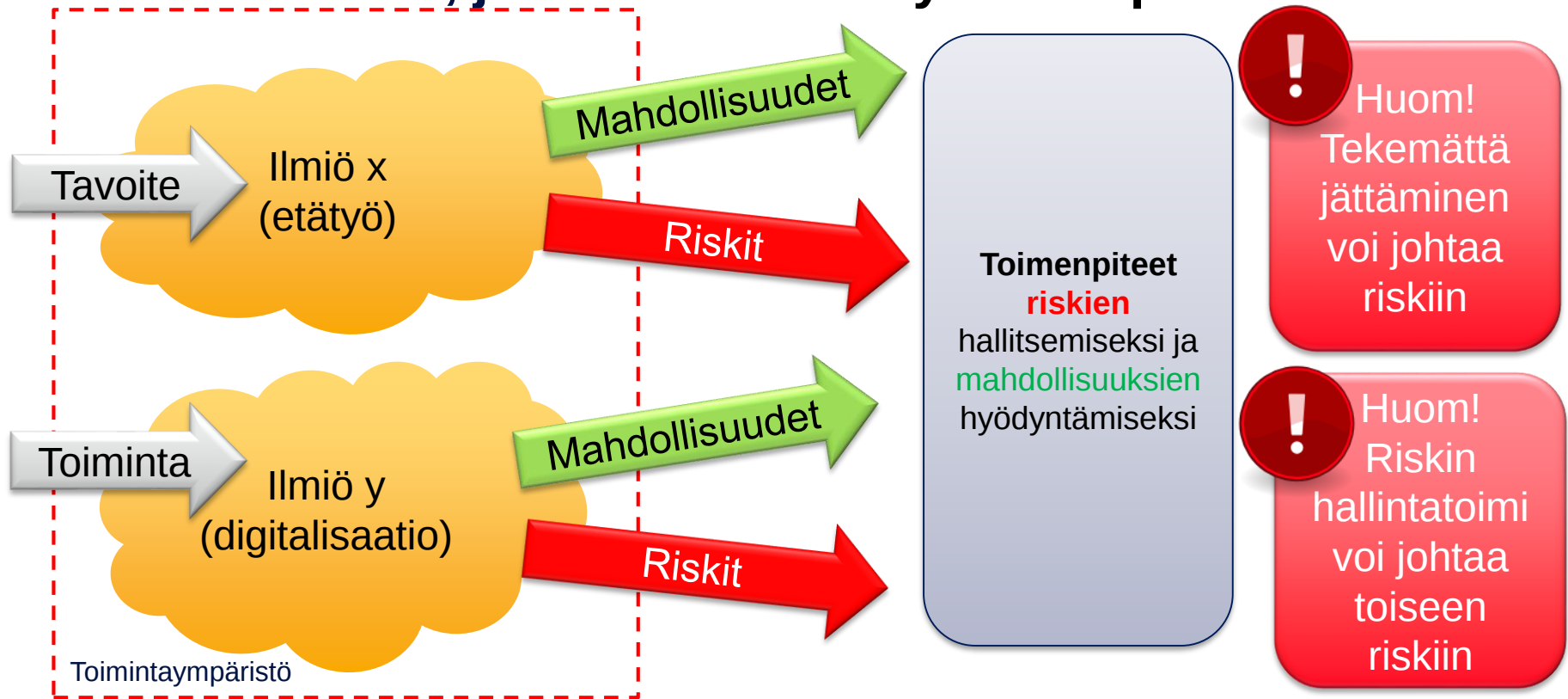
Tiedon omistaja

Palvelun omistaja

Rekisterin pitäjä

Esimies

Riskienhallinta, joka huomioi erityisesti epävarmuuden



Riskienhallinta, joka perustuu parhaaseen käytettävissä olevaan tietoon



Riskienhallinta, joka huomioi inhimilliset ja kulttuurilliset tekijät



Mustat
joutsenet



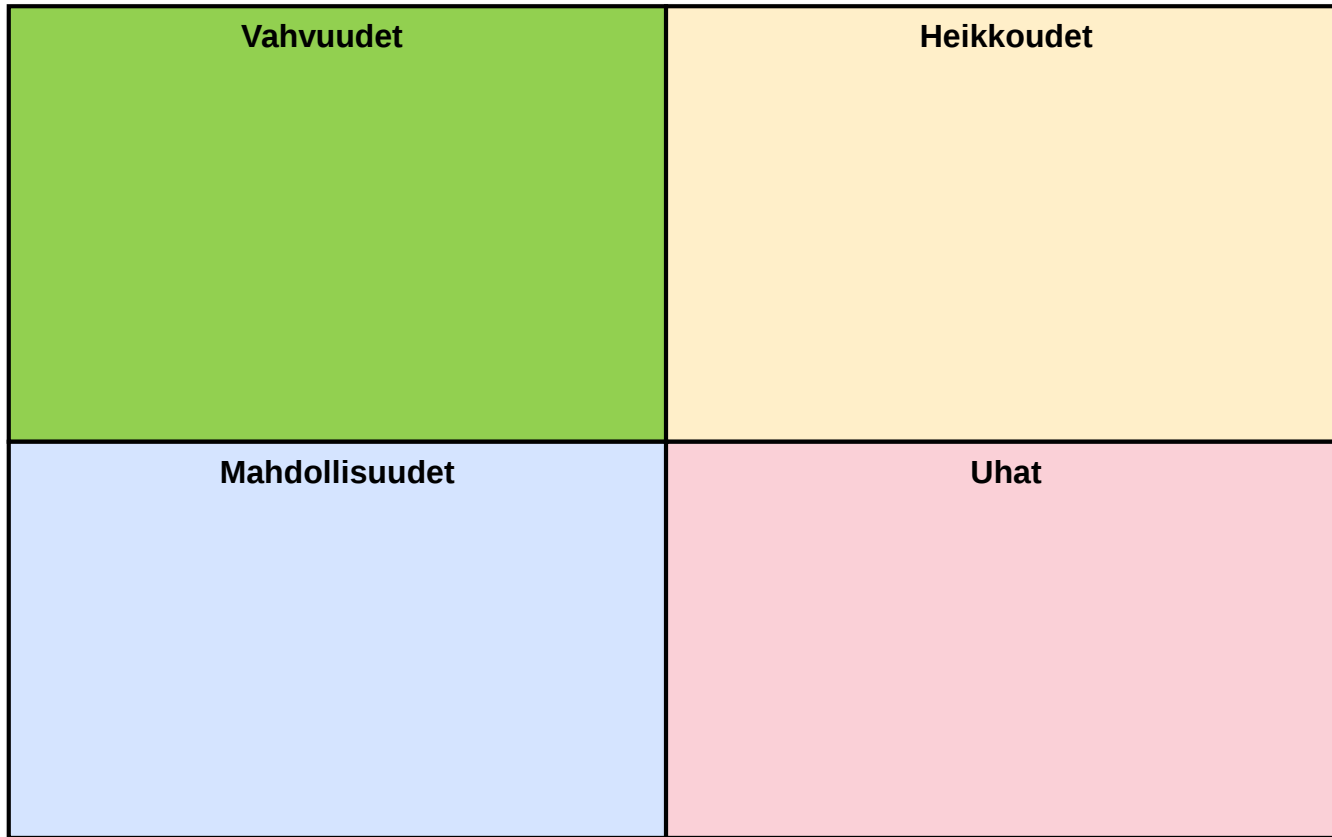
Median
vaikutus



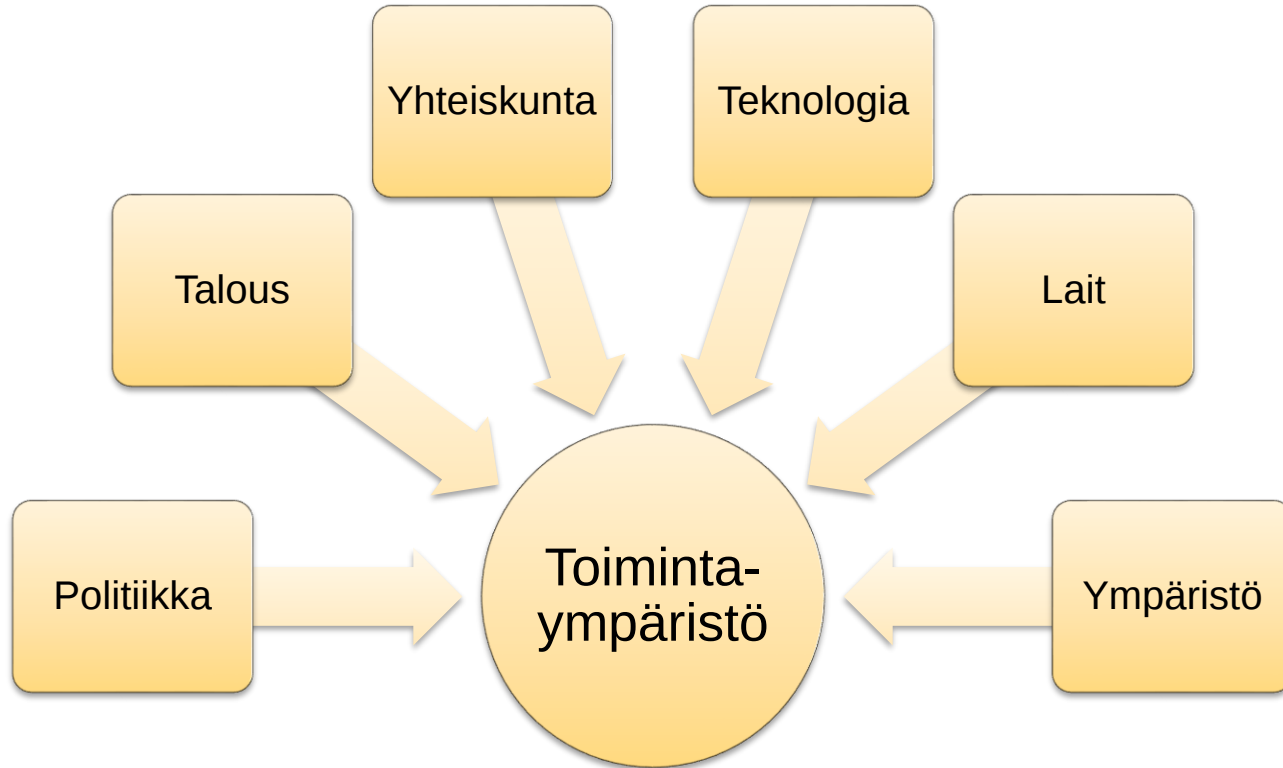
Psykologiset
vinoumat



Helppo tapa aloittaa järjestelmällistä riskienhallintaa: SWOT



PESTLE-malli auttaa huomioimaan eri toimintaympäristön osa-alueita





Kiitos!



Ikonit: Open Security Architecture
<http://www.opensecurityarchitecture.org>
Kuvat: Tulli

