Tieto- ja kyberturvallisuuden hallinta ja johtaminen

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisvälineen (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopealla toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.

TURKU AMK

Euroopan unionin rahoittama

NextGenerationEU

Rahoittaja

Jatkuvan oppimisen ja työllisyyden palvelukeskus

Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisvälineen (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopealla toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.

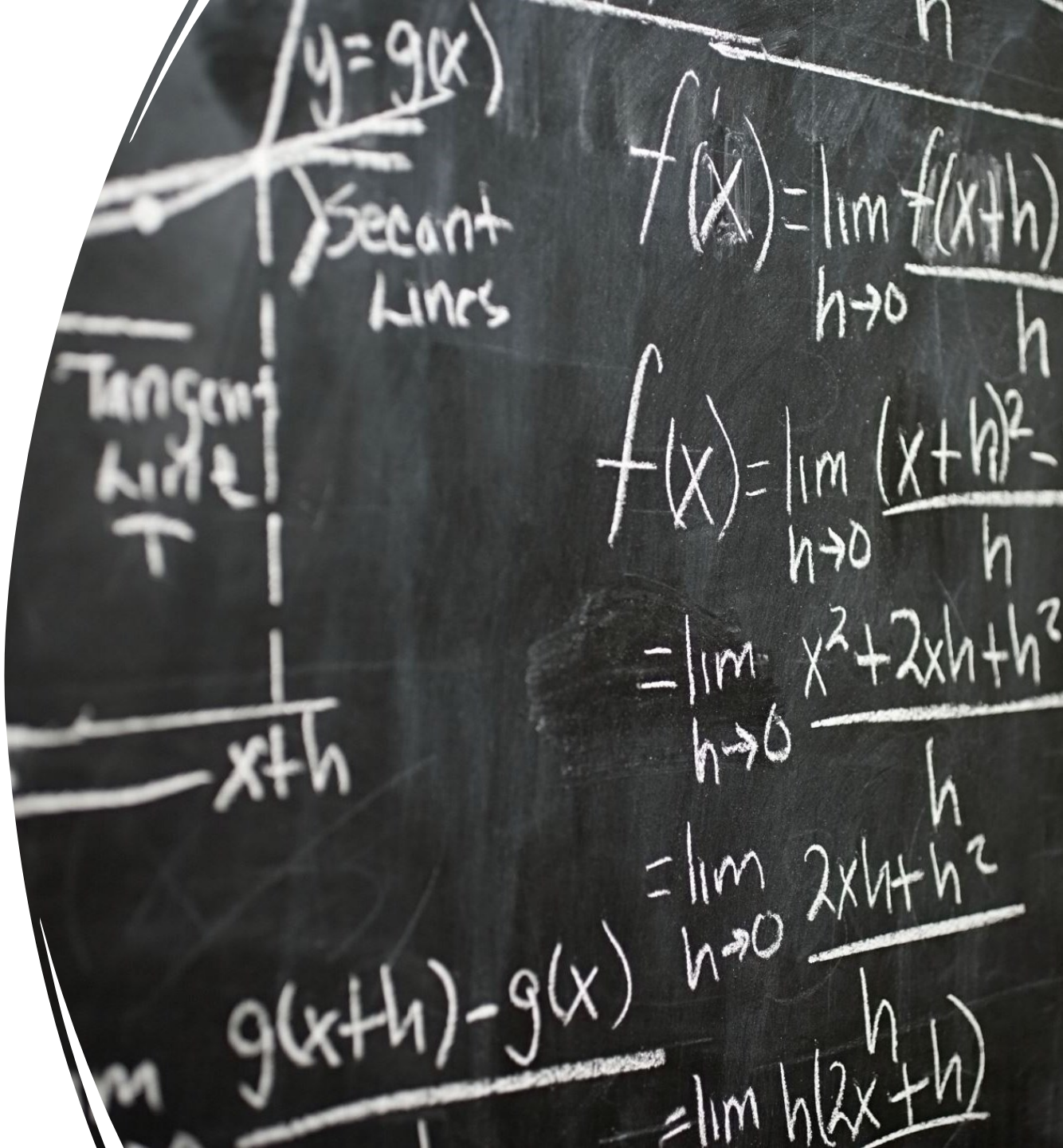
Tavoitteet

Opintojakson suoritettuaan opiskelija

- Ymmärtää tieto- ja kyberturvallisuuden johtamisen merkityksen organisaation liiketoiminnalle
- osaa suunnitella ja toteuttaa tietoturvan johtamis-/hallintajärjestelmän organisaatiossa
- ymmärtää johtamisjärjestelmään liittyvät prosessit, kontrollit ja henkilöstöön liittyvät kysymykset ja pystyy arvioimaan tietoturvariskejä
- Ymmärtää mittaamisen ja auditointien merkityksen organisaation tietoturvallisuudelle ja liiketoiminnalle
- Ymmärtää jatkuvan kehittämisen merkityksen tietoturvallisuuden hallintajärjestelmän ylläpidolle
- Ymmärtää tilannekuvan ja tiedonvaihdon sekä viranomaisyhteistyön merkityksen tietoturvallisuuden johtamisessa
- Ymmärtää harjoittelun merkityksen tietoturvallisuuden johtamiselle

Arviointi

- Palautetut tehtävät arvioidaan asteikolla 0-5
- Arvosana on tehtäväpalautusten keskiarvo
- Palauttamattomat tehtävät laskevat arvosanaa
- Alle 50% palautuksista tehty – arvosana hylätty
- Lähipäivien poissaolosta korvaava tehtävä



Uutinen

Tietoevryn asiakas ilmoitti yli 6 miljoonan menetyksistä – syynä kyberhyökkäyksen vaikutukset

Jyri Tuominen 26.1.2024 23:35 SIJOITTAMINEN TIETOTURVA

Tietojärjestelmien häiriöt ovat johtaneet ongelmiin muun muassa myymälöiden toimitusketjujärjestelmässä sekä markkinointikampanjoiden ja omien verkkosivujen hyödyntämisessä. Lisäksi yhtiön verkkokauppa-alustalle ei ole päässyt häiriöiden alettua, ja kassajärjestelmien kapasiteetti on aiempaa rajallisempi.

Tulosvaikutuksia. Rustan mukaan tietojärjestelmähäiriöt syövät yhtiön myyntiä monesta suunnasta, eikä tietoa tilanteen ratkeamisaikataulusta ole. EEVI KARVINEN

Uutinen

It-talo joutui tietomurron kohteeksi, asiakkaat menettivät kaiken datansa – ”En usko yrityksen selviytyvän”

Aleksi Kolehmainen 23.8.2023 12:18 | päivitetty 23.8.2023 13:35 PILVIPALVELUT KIRISTYSHAITTAOHJELMAT

Tanskalaisen CloudNordicin asiakkaat joutuvat pystyttämään järjestelmänsä täysin puhtaalta pöydältä ilman mitään asiakastietoja.

cloudnordic
The Nordic Cloud Experts

Määritelmiä – tietoturvallisuuden hallinta

- Tietoturvallisuuden hallinta on kokonaisvaltaista ja suunnitelmallista toimintaa turvallisuuden edistämiseksi.
- Pitää sisällään kaikki ne menettelytavat ja toiminnot, joilla hyvään kokonaisturvallisuuteen päästään.
- Dokumentoitua
- Henkilöstöä sitouttavaa

Euroopan unionin rahoittama
NextGenerationEU
Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

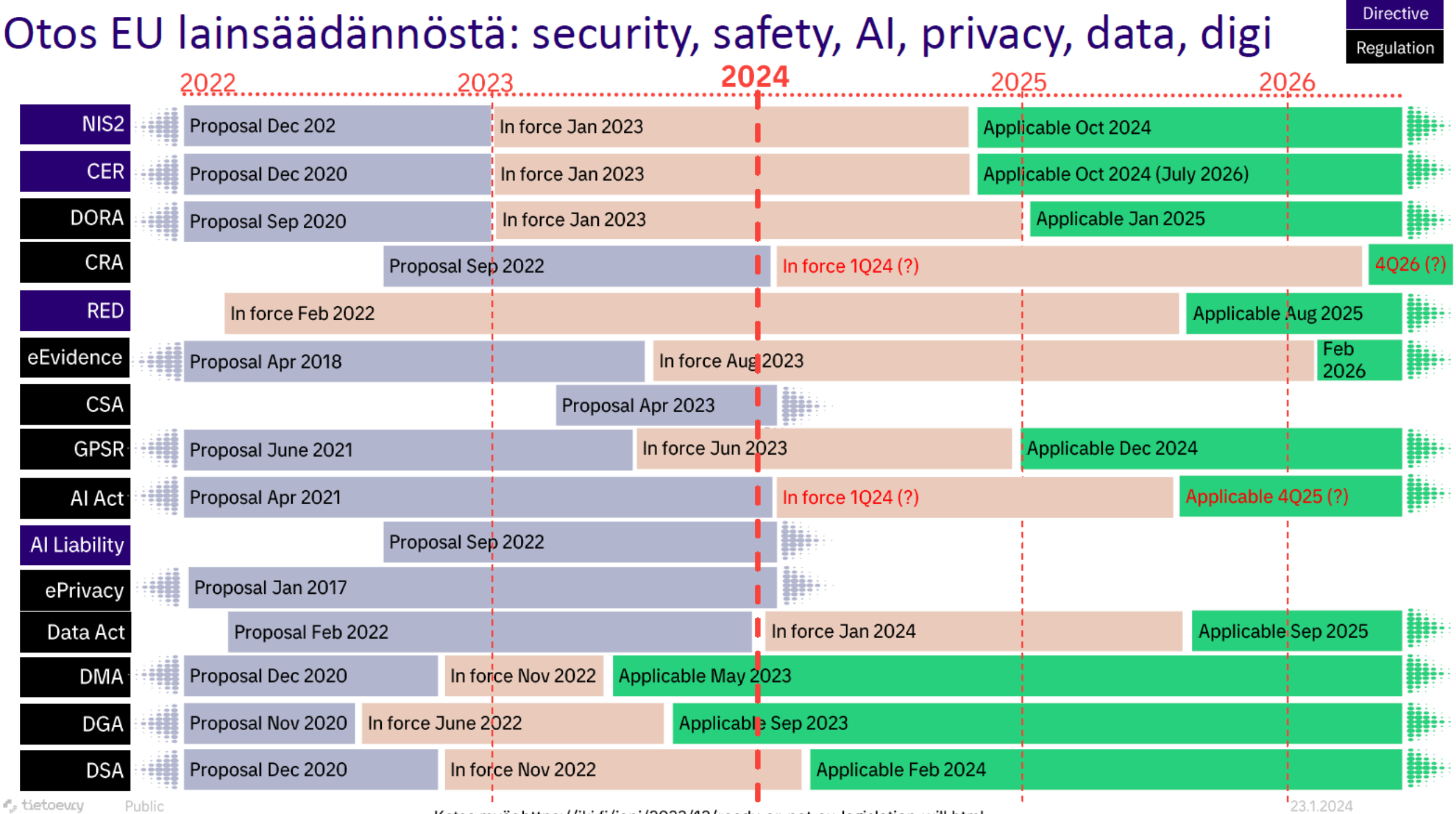
Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Miten tieto- ja kyberturvallisuuden johtaminen eroaa muusta johtamisesta?

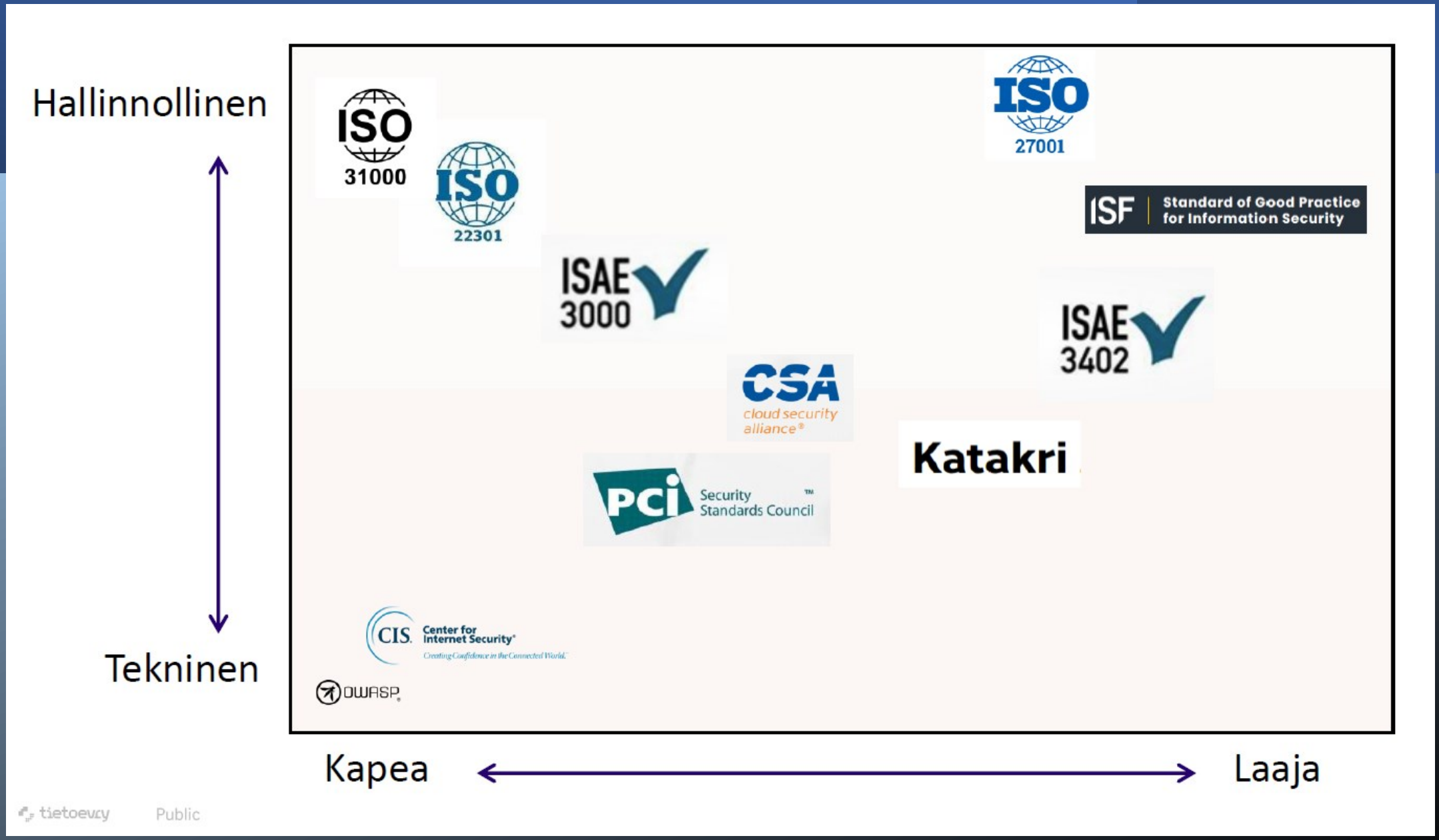
TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Otos EU lainsäädännöstä: security, safety, AI, privacy, data, digi



Katso myös https://iki.fi/japi/2023/12/ready-or-not-eu-legislation-will.html

Viitekehykset ja vaikuttavuus



Mikä on johtamisjärjestelmä?

Määritelmiä – johtamis-/hallintajärjestelmä

- Johtamisjärjestelmä on henkilöstön, resurssien, toimintapolitiikkojen ja menettelyjen kaikentasoinen yhdistelmä.
- Osien välillä on organisoitua vuorovaikutusta annetun tehtävän toteuttamiseksi tai määritellyn tuloksen saavuttamiseksi tai ylläpitämiseksi.
- Toimii johtamisen työkaluna, joka mahdollistaa jatkuvan parantamisen sekä muutoksen johtamisen

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Rooli on muuttunut teknisestä hallinnollisempaan

Tietoturvan johtaminen

Nivoutuminen liiketoiminnan keskeiseksi elementiksi vaatii tietoturvajohtajilta uudenlaista osaamista

https://www.infosecurity-magazine.com/news/isf-outlines-skillsets-modern-ciso/

Tunniste	HAL-01, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Periaatteet
Vaatimus	Organisaatiolla on ylimmän johdon hyväksymät tietoturvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan sekä ovat tietojen suojaamisen kannalta kattavat ja tarkoituksenmukaiset.
Yleiskuvaus	Ylimmän johdon hyväksymillä tietoturvallisuusperiaatteilla osoitetaan, että johto on sitoutunut organisaation tietoturvallisuusperiaatteisiin ja periaatteet edustavat johdon tahtotilaa sekä tukevat organisaation toimintaa. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina tai osana yleisiä toimintaperiaatteita, politiikkaa tai strategiaa.
Toteutusesimerkki	
Lainsäädäntö	TihL 4 § 2 mom, 13 §
Viitteet	Katakri: T-01
Muita lisätietoja	ISO/IEC 27002:2022 5.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01

Tunniste	HAL-02, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto
Nimi	Tehtävät ja vastuut
Vaatimus	Organisaatio on määritellyt ja dokumentoinut tietoturvallisuuden hoitamisen tehtävät ja vastuut sisältäen myös palveluntuottajille kuuluvat vastuut.
Yleiskuvaus	Tietoturvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan, että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa. Organisaation johdon tehtävänä on määritellä tiedonhallintaan liittyvät vastuut. Kysymys ei ole tiedonhallintavastuiden delegoinnista, vaan niiden määrittelystä. Vastuut tulisi määritellä erityisesti turvallisuusohjeiden ylläpidosta, riskienhallinnasta, varautumisesta sekä turvallisuuden kokonaisvastuussa olevista henkilöistä. Tietoturvallisuuden vastuualueet määritellään yleensä osana turvallisuuden kokonaisvastuuta. Vastuiden määrittelyssä tulee ottaa huomioon myös toimittajan vastuulla olevat tehtävät. Pilvipalveluita käytettäessä on huomioitava erilaiset palvelumallit sekä niihin liittyvät vastuujakojen erot asiakkaan ja palvelun tuottajan välillä.
Toteutusesimerkki	Organisaatio on määritellyt turvallisuuden toteuttamisen tehtävät ja niihin liittyvät vastuut seuraavilta osin: a) turvallisuusjohtaminen b) fyysinen turvallisuus c) tekninen turvallisuus d) varautuminen ja jatkuvuudenhallinta e) tietosuoja f) riskienhallinta g) turvallisuuden kokonaisvastuu

Miten johtaminen onnistuu?

> “Organisaation turvallisuuskulttuuri ei synny ohjeistuksesta tai kamerasta – se täytyy jalkauttaa organisaatioon ja ihmisten keskuuteen.”

Kai Himberg FAZER

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Turvallisuuspolitiikka	• sisältää päämäärät • näkyy johdon sitoutuminen • näkyy henkilöstön merkitys turvallisuuden toteuttamisessa
Turvallisuusjohtamisen organisointi	• järjestelmällisten toimintatapojen luominen • toimintavastuiden ja velvollisuuksien määrittäminen • linjaesimiesten resurssien varmistaminen
Käytännön toiminta	• riskien arviointi • osaamisen varmistaminen • toimenpiteiden toteutus • tiedon kulun varmistaminen • mittaaminen ja seuranta

Tietoturvallisuuden johtaminen

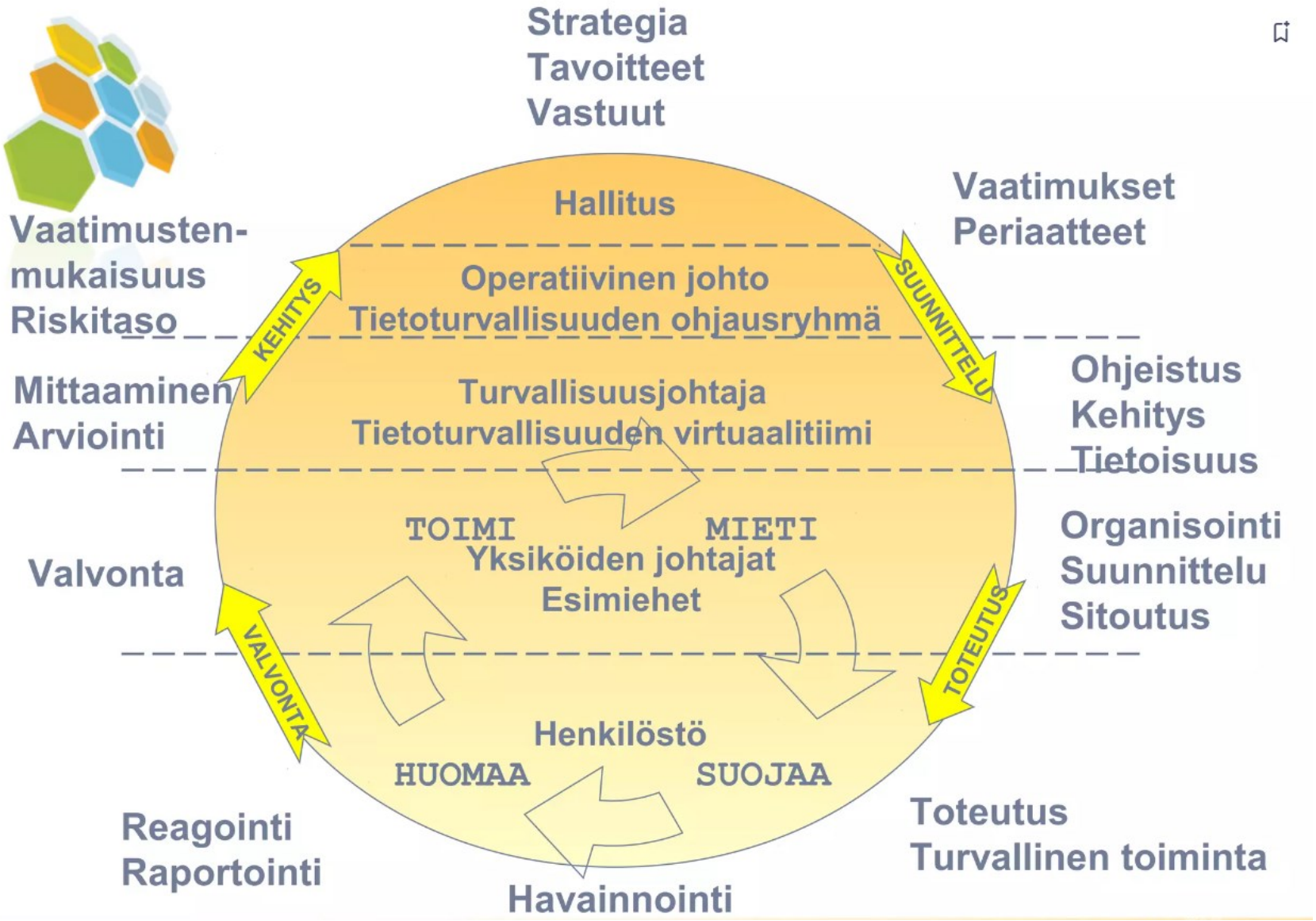
- Tieto- ja kyberturvallisuuden johtaminen on **tavoitteiden kyvykkyyksien johtamista**
  - Ihmisten osaaminen
  - Käytänteet
  - Prosessit
  - Teknologia

- **Ylimmän johdon vastuulla**

  ” Ylimmän johdon on osoitettava johtajuutta ja sitoutumista tietoturvallisuuden hallintajärjestelmään”

  - Varmistamalla, viestimällä, ohjaamalla, edistämällä, tukemalla

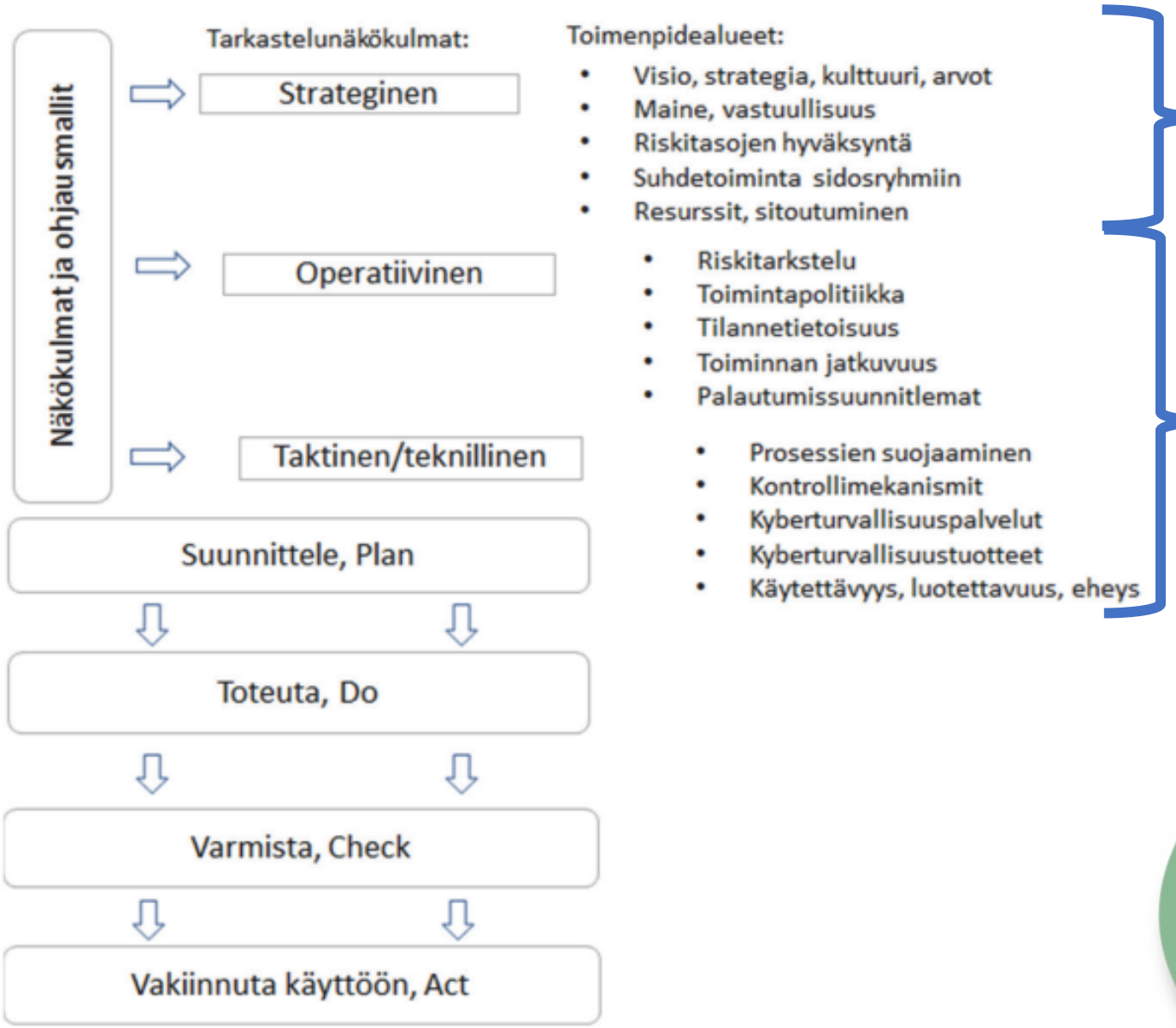
Häiriötilanteet aiheuttavat lähes aina toiminnan keskeytymisen



https://www.slideshare.net/japijapi/idc-helsinki19913

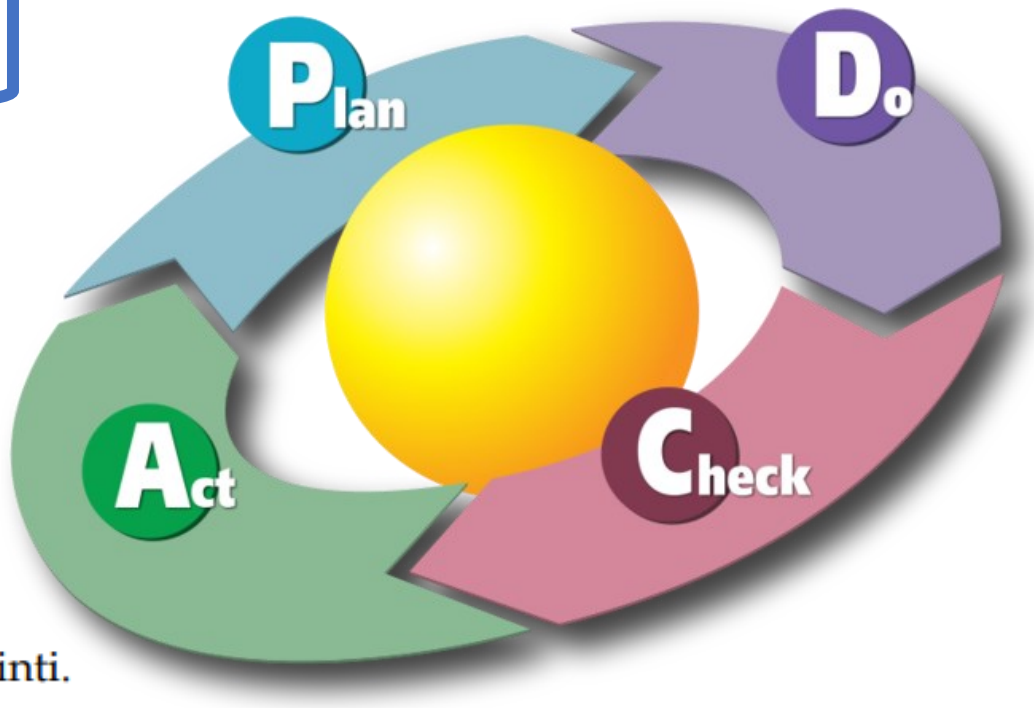
”Strategia on se, mitä organisaatio tahtoo, tekee ja puhuu. Strateginen johtaminen on tuon tahtomisen, tekemisen ja puheen aikaansaamista.”

https://jyx.jyu.fi/handle/123456789/71395



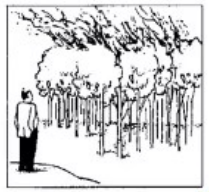
Miksi? Mitä?

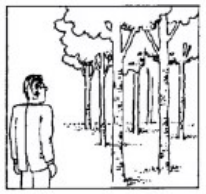
Miten?



KUVIO 25 Kyberturvallisuuden kehitystoimenpiteiden implementointi.

Tietoturvan johtaminen





Strategginen

Taktinen

Operatiivinen

Raportointi

Mittaaminen

Valvonta

Seuranta

Hallitus

Konsernin johtoryhmä

Turvallisuusosasto

Yksiköiden johtajat
Yksiköiden joryt

Osastopäälliköt
Henkilöstö

KEHITÄ

SUUNNITTELE

VALVO

TOTEUTA

HAVAITSE

TOIMI

ARVIOI

PÄÄTÄ

Strategia, resurssit

Ohjaus (konserni)

Ohjaus (yksikkö, osasto)

Toteutus

https://www.slideshare.net/japijapi/kokemuksia-tietoturvallisuuden-johtamisesta

Johtamisen rakentaminen

Visio:

- Luottamuksen ja toimintakyvyn saavuttaminen/pitäminen

→ Strategia:

- Puolustava strategia – uhkiin ja heikkouksiin keskittyvä
- Mahdollisuuksiin keskittyvä

→ Operatiivinen:

- Käytännön toimenpiteet, ohjeet ja politiikat – johdon sitoutuminen
- Edistetään strategisia tavoitteita

→ Tekninen/Taktinen:

- Toteutetaan käytännön toimenpiteet → kyvykkyydet

Tavoitteet ja hyödyt

- Organisaation ja liiketoiminnan tietojen, palveluiden ja infrastruktuurin suojaaminen
- Toimitusketjujen varmistaminen ja suojaaminen
- Vaatimuksenmukaisuuden varmistaminen – liitynnät muihin vaatimuskehikoihin
- Luottamus ja maine
- Kohdennettua
- Ennakoivaa ja reagoivaa
- Riskienarviointiin perustuvaa
- Sietokykyä rakentavaa – varautuminen ja jatkuvuus
- Tavoitteellista, vastuutettua ja loogisesti järjestettyä
- Toteutumista seurataan
- Suorituskykyä mitataan
- Suunnittelu, arviointi ja kehittäminen on systemaattista
- Johdon sitoutuminen

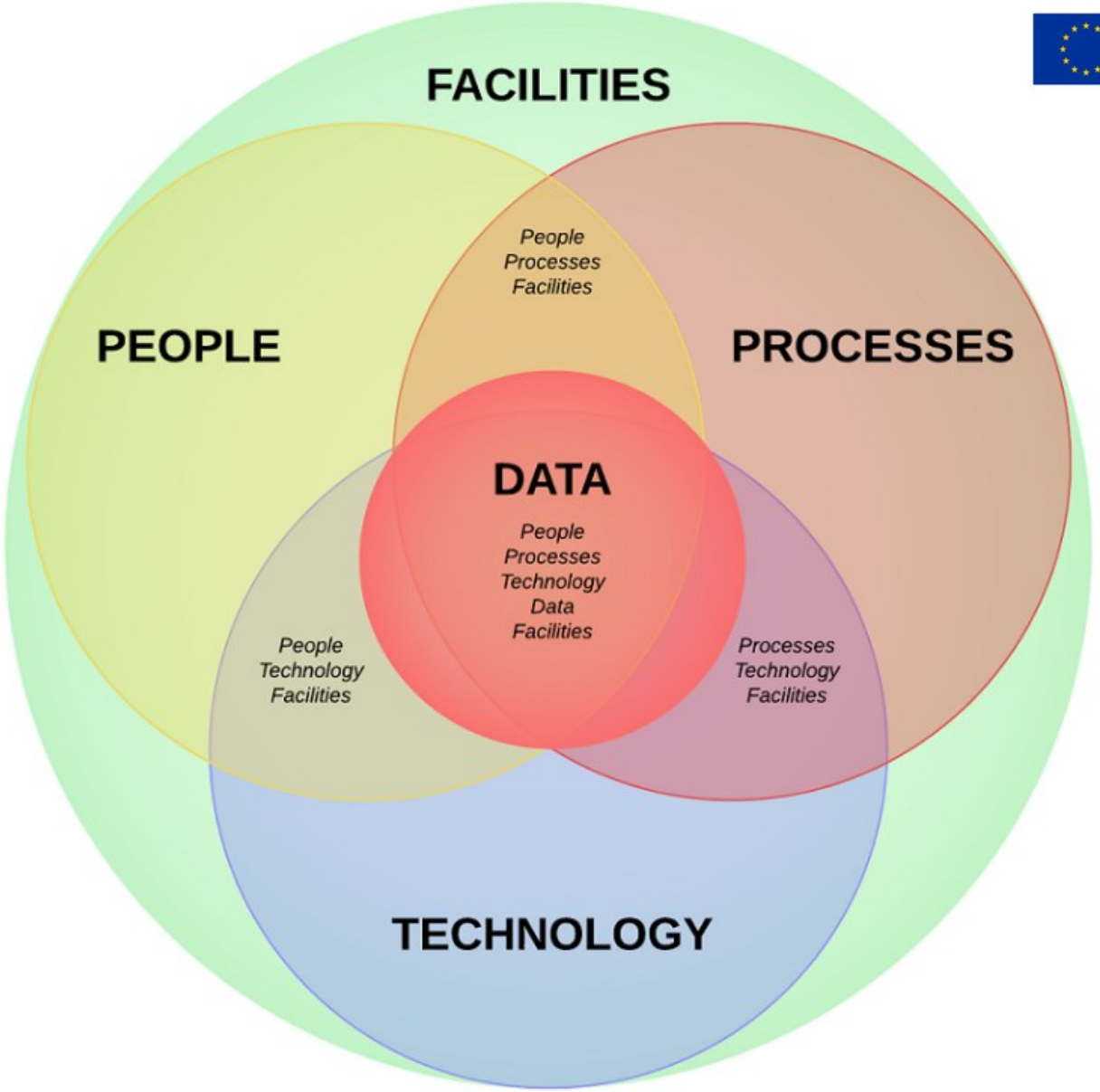
Euroopan unionin rahoittama
NextGenerationEU
Rahoittaja
Jatkuvan oppimis
työllisyyden palve

TURKU AMK

Euroopan unionin rahoittama
NextGenerationEU
Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

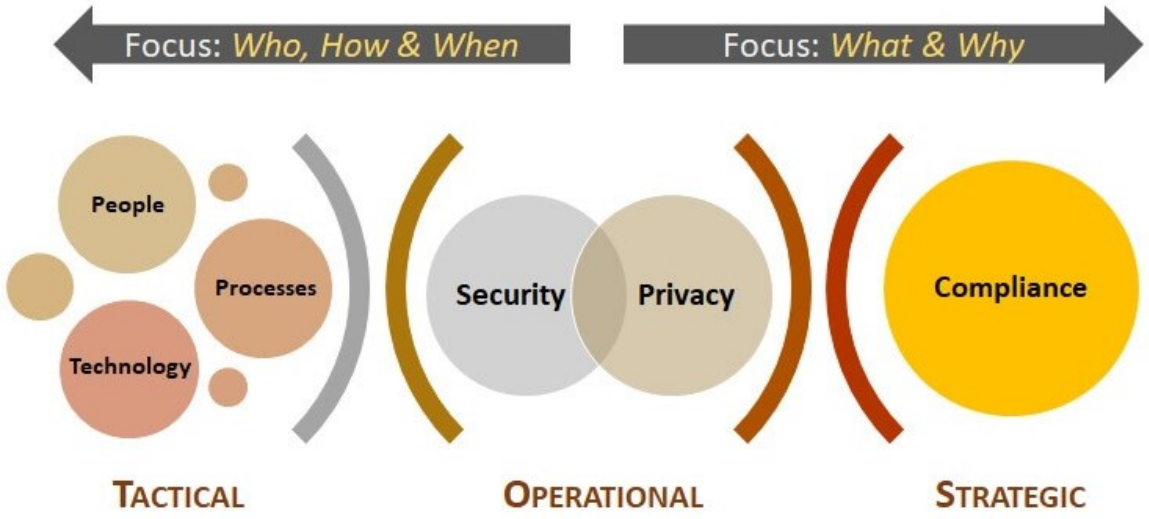
PPTDF – malli

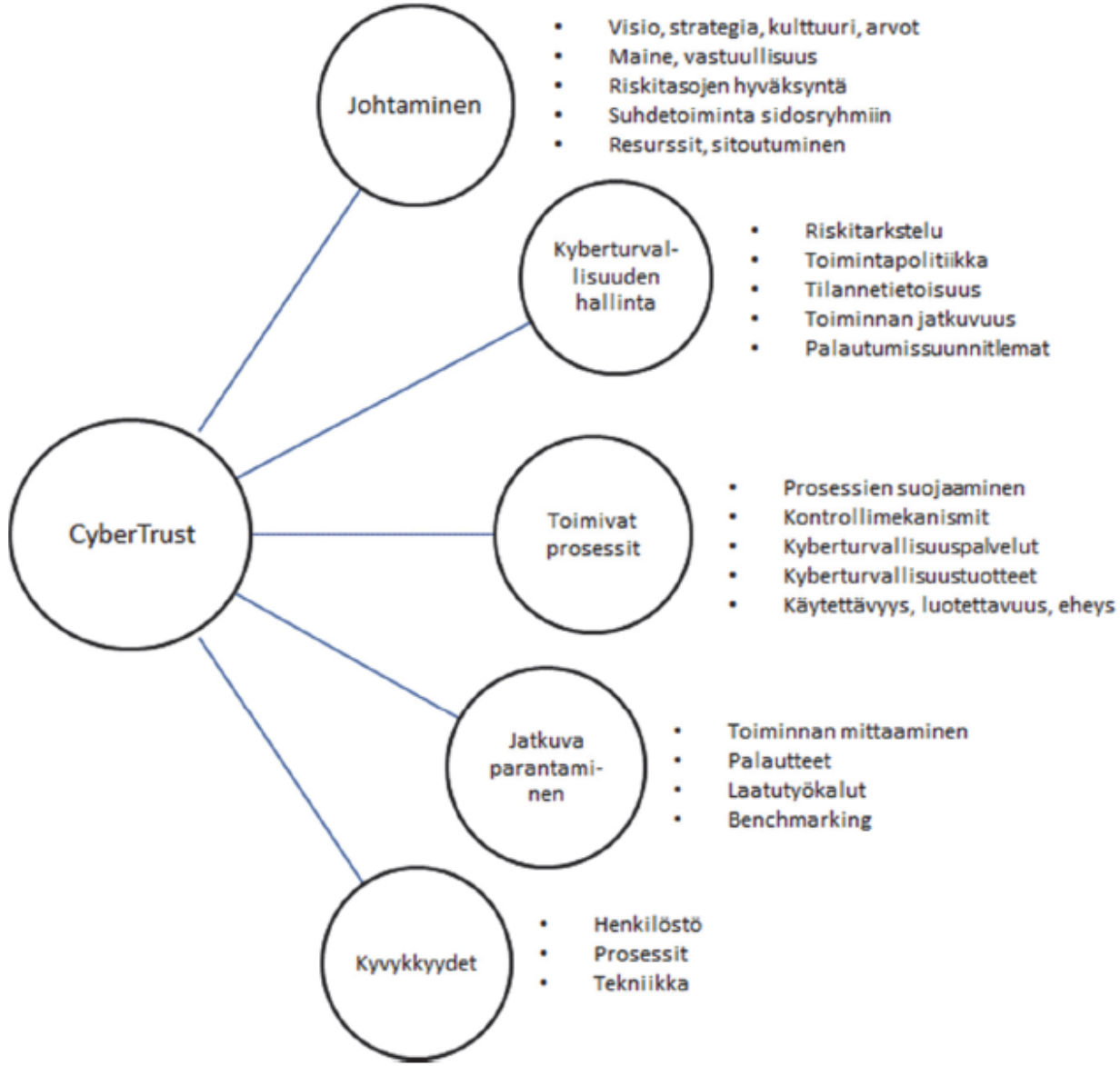
(24.1.2024)



People, Processes, Technology, Data, and Facilities (PPTDF) - Secure Controls Framework

Tavoitteen saavuttaminen





KUVIO 3 Organisaation kyberluottamusta lisääviä toimenpiteitä.

https://jyx.jyu.fi/handle/123456789/71395

Vuosisuunnittelu ja strateginen päätös

Talous | Tietotekniikka

Suomalaista ohjelmistoyhtiötä kiristetään verkkohyökkäyksellä

Ruotsalaislehden mukaan kiristyksen takana on venäläinen hakkeriryhmä.

Ohjelmistoyhtiö Tietoevryn toimitusjohtaja Kimmo Alkio. KUVA: KALLE KOPONEN / HS

Petri Sajari HS, Liisa Niemi HS
22.1. 12:41 | Päivitetty 22.1. 19:03

OHJELMISTOYHTIÖ Tietoevry on joutunut Ruotsissa verkkohyökkäyksen kohteeksi.

Muuttuva uhkaympäristö

- Vaatii jatkuvaa seurantaa ja arviointia
- Teknisen suojauksen tehokasta ylläpitoa
- Tietoisuuden ja ymmärryksen lisäämistä
- Nopeaa reagointikykyä
- Tiivistä yhteistyötä ja tiedonjakoa
- Johdon tilannekuvaa
- Toimintaympäristötuntemusta
- Resurssien kohdentamista

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Roolit, vastuut ja valtuudet

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Tavoitteiden saavuttaminen - prosessijohtaminen

- Tieto-ja kyberturvallisuuden päätöksenteon tulee olla nopeaa ja joustavaa.
- Jatkuvan oppimisen prosessi
- Toimii organisaatiorajat ylittävänä

  - Suojattavien kohteiden tunnistaminen
  - Prosessien kuvaaminen
  - Prosessien suojaamisen kuvaaminen
  - Prosessien suojaamisen toteuttaminen

  → Jatkuva parantaminen = jatkuva arviointi

  - Henkilöstön huomioiminen kaikilla organisaation tasoilla

Muuttuva organisaation toimintaympäristö

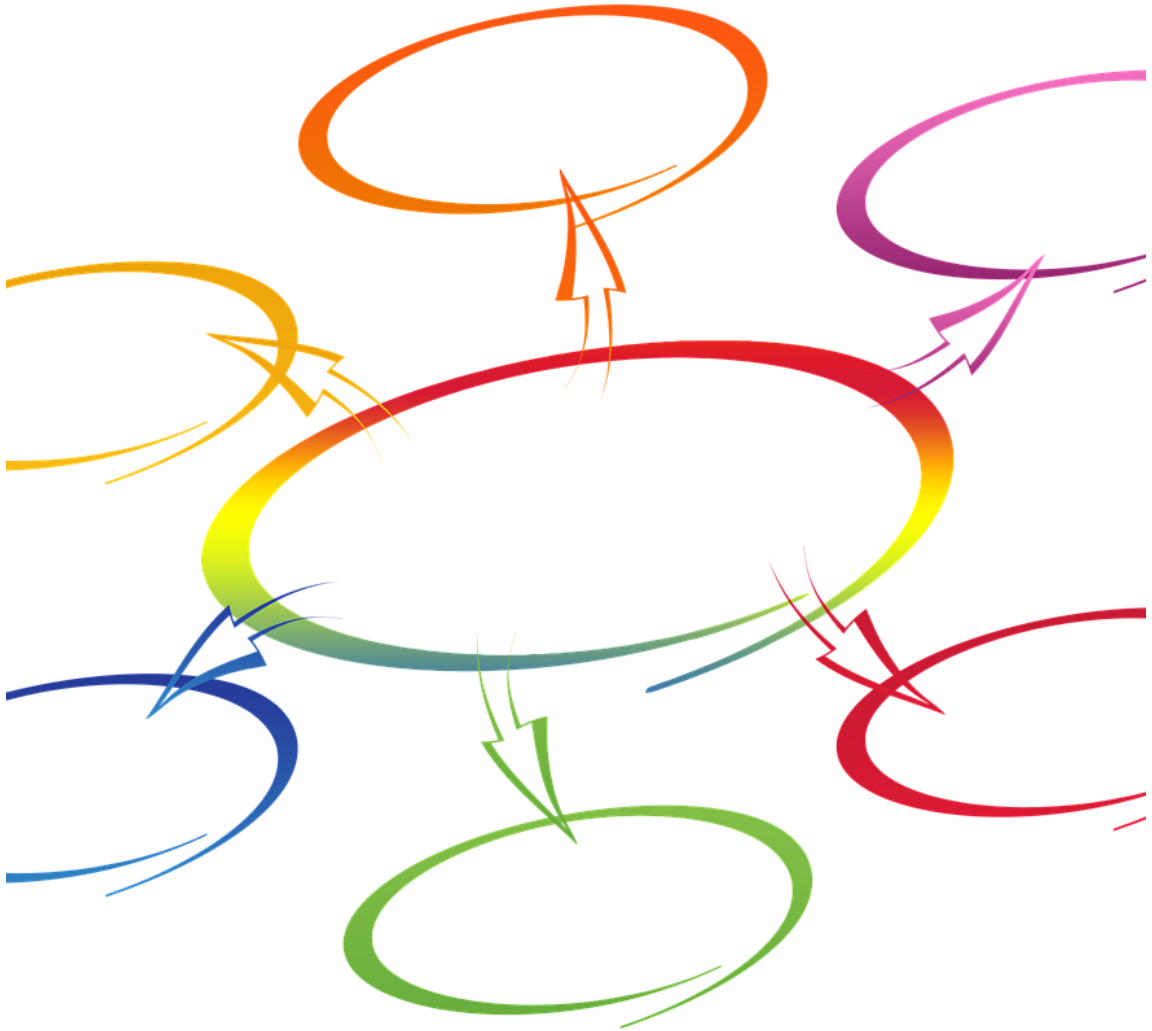
- Organisaation toimintaympäristön määrittäminen
  - Sisäiset toimijat – tieto-ja kyberturvallisuuden tahtotila
  - Ulkoiset toimijat – tietoturvallisuuden hallinnan kannalta olennaiset sidosryhmät
  - Toimitusketjumuutokset

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Mihin muutokset kohdistuvat

- Liiketoimintastrategiaan
- Tekniseen ympäristöön
- Viranomaismääräyksiin, asetuksiin, lakeihin, sopimuksiin
- Tieto- ja kyberturvallisuusriskeihin
- Uhkaympäristöön



TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Haasteita

- Toimintaympäristön ja liiketoiminnan tuntemus
- Toimintaympäristöön kohdistuvien riskien tunnistaminen ja hallinta
- Tavoitteiden asettaminen
- Tietoturvan huomioiminen läpi organisaation – ajoissa!
- Tietojen omistajuus
- Kohdennettu koulutus
- Liiketoiminnan jatkuvuus
- Tekniikka edellä
- Viitekehys edellä

- Miten tieto- ja kyberturvallisuuden tulisi olla resursoitu?

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Realismi

- Johtaminen ja tekeminen on siiloutunut
- Selkeyden puute – liian iso kakku?
- Resurssirealismi (OTO – 0€)
- Pistemäistä tulipalojen sammuttamista
- Knowing – Doing –Gap
- Ulkoistukset

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

KESKUSTELU

Miten organisaatiosi tieto- ja kyberturvallisuuden toteutumista mitataan?

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

TURKU AMK

Mittaaminen ja tilannekuva

- Johdon tahtotilan toteutuminen
- Osaamisen taso
- Auditointien tulokset
- Riskienhallinnan nostot
- Poikkeamien lukumäärä
- MIM –caset
- Asiakastyytyväisyys
- …..

Liiketoiminnan mittarit tuottavat tietoturvallisuuden mittarit!

Kysymyksiä, jotka hallitus voi esittää toimivalle johdolle

What are the key **threats** against our top assets?

How do we **protect** our assets from cyber security threats?

Whose **responsibility** it is to protect our top assets?

How do we monitor the **effectiveness** of our controls?

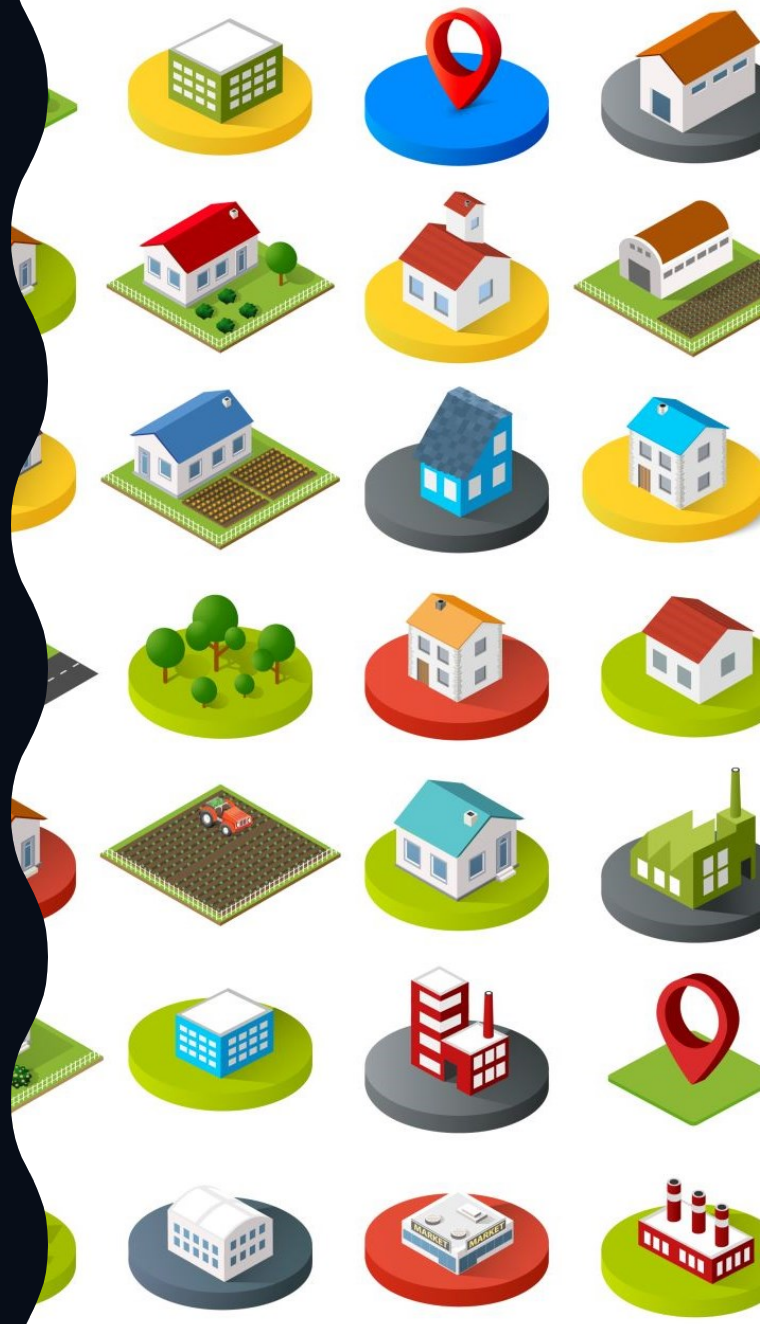
Have we defined an **acceptable risk level**?

FINAVIA

Kuinka ”johdetaan” johtoryhmää?

https://www.slideshare.net/japijapi/idc-helsinki19913


n
v
r
$r_\perp$
$r_\parallel$
$v = v_\parallel + v_\perp$
$v_\parallel = k(k \cdot v)$
$v_\perp = -k \times (k \times v) = v - k(k \cdot v)$
$r = r_\parallel + r_\perp$
$r_\parallel = n(n \cdot r)$
$r_\perp = -n \times (n \times r) = r - n(n \cdot r)$
Mg
√3
√2
Drehung
Punktspiegelung
Keep it simple

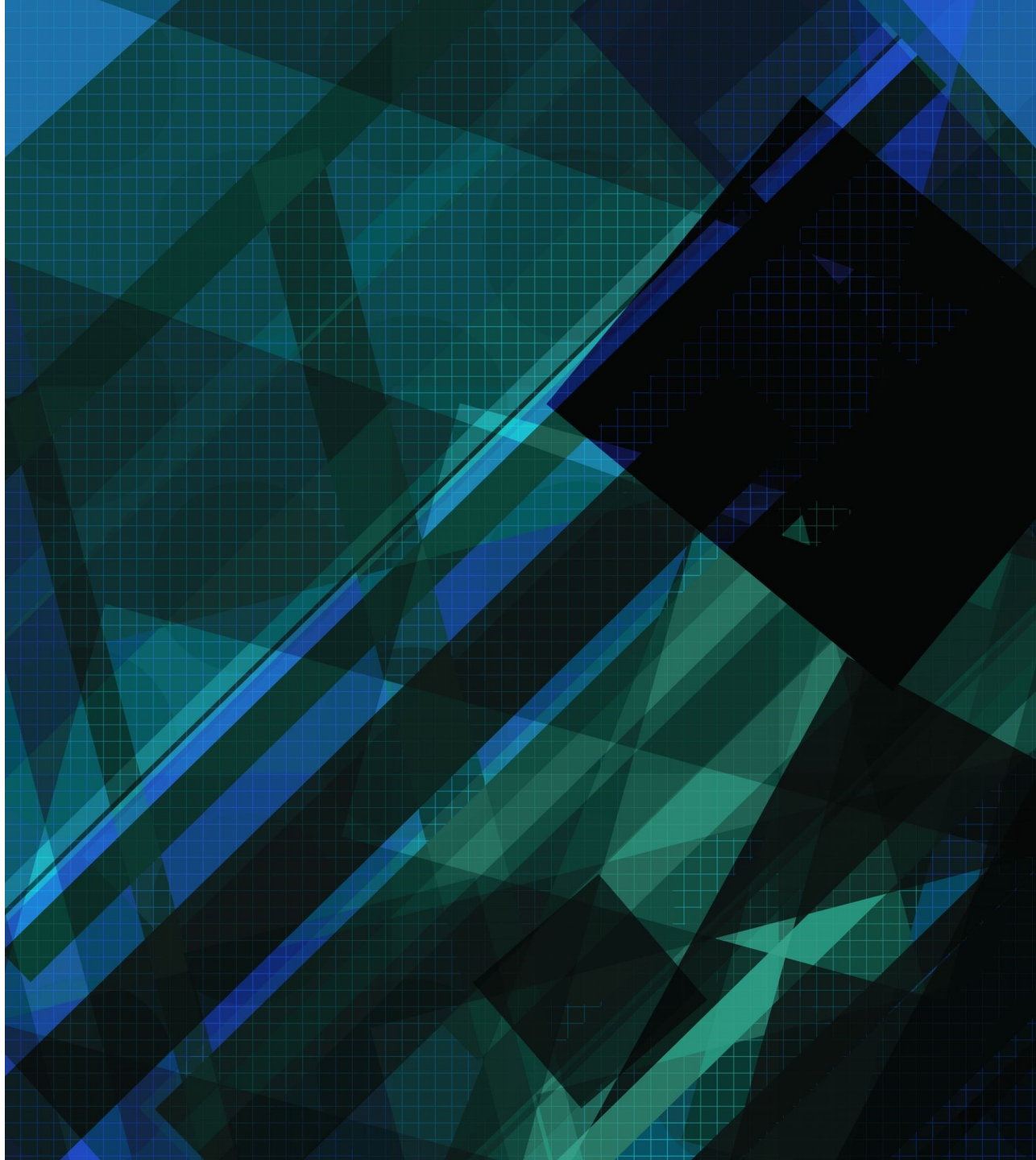


Materiaalia

- turvallisuusjohtaminen.p65 (turvallisuusuutiset.fi)
- NIXU_CyberSecurity_Index_Report_2022_FINAL.pdf
- 28-2018-Kyberturvallisuuden strateginen johtaminen.pdf (valtioneuvosto.fi)
- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) – Suositus ja kriteeristö (valtioneuvosto.fi)
- Mitä on hallinnollinen tietoturvallisuus? (seclion.fi)
- Turvallisuusjohtamisen perusteita (seclion.fi)
- Kybermittari-aineistot | Kyberturvallisuuskeskus
- SFS Online ISO27001 – FINNA kirjastopalvelusta omilla tunnuksilla
- Jouni Pöyhönen, https://jyx.jyu.fi/handle/123456789/71395
- https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf
- Katakri 2020 (um.fi)
- Turvallisuus- ja yritysjohdon yhteistyö: https://www.slideshare.net/japijapi/idc-helsinki19913

Kiitos!

TURKU AMK



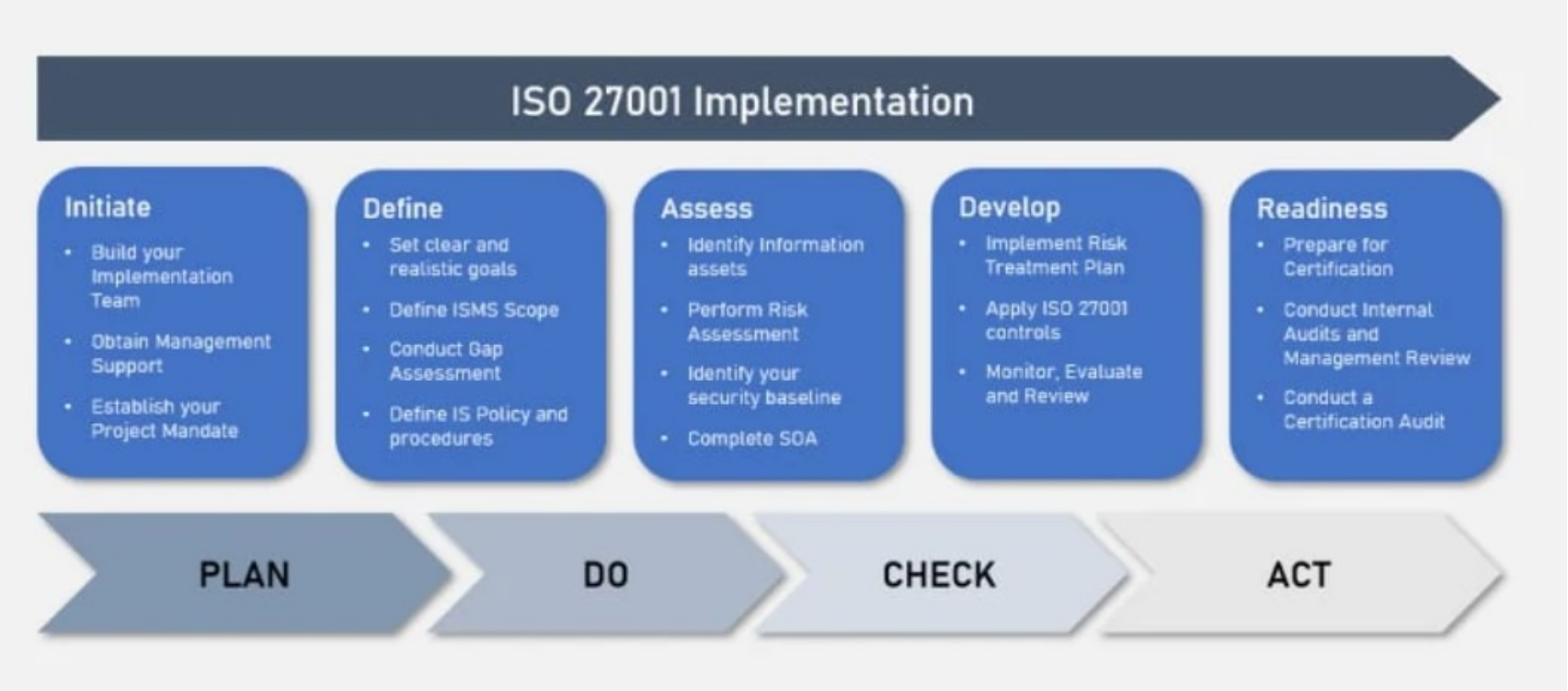
Tieto- ja kyberturvallisuuden johtaminen

- Miten organisaatiosi toimii **KUN** jotain tapahtuu?

Kattavuus

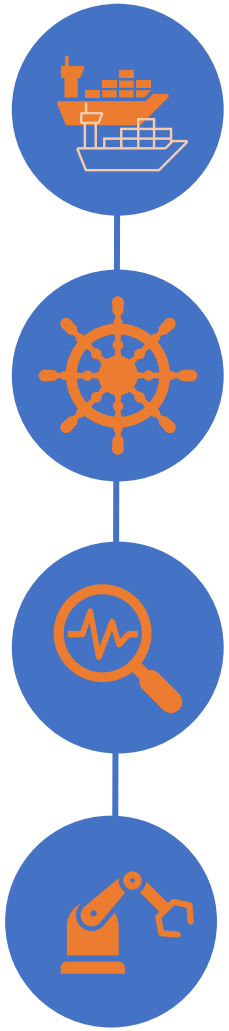
https://www.kolide.com/blog/the-business-guide-to-iso-27001-compliance-and-certification

Jatkuva prosessi



https://www.businesstechweekly.com/legal-and-compliance/iso27001-certification/iso-27001-implementation/

Toteutus



Nykymaturiteetti vs. tavoiteltava taso

Resursointi ja vastuut

Johtaminen/johdon sitoutuminen

Aikataulu

Suojattavien kohteiden tunnistaminen ja tiedon luokittelu

Rajaukset - laajennukset

Jatkuva kehittäminen ja ylläpito

ISMS mahdollista ilman sertifiointia

Kokonaisuus

Tärkeimmät pointit

- Ylimmän johdon tuki ja liiketoimintajohdon ymmärrys
- Realistinen GAP –analyysi
- Projektin asettaminen
- Resursointi ja osaamisen varmistaminen
- Jalkautus, koulutus, viestintä
- Ylläpito

Johtamisjärjestelmä

- Johdonmukainen ja looginen malli

- **Kuinka hallinnollinen tietoturva otetaan mukaan yrityksen strategiaan?**
- Tietoturvan hallintajärjestelmän käyttöönotto tapahtuu useimmiten projektina, joka alkaa organisaation tarpeiden kartoittamisella ja niihin sopivan järjestelmän valitsemisella. Tämän jälkeen tehdään analyysi siitä, kuinka käytännöt poikkeavat ja missä on puutteita haluttuun järjestelmään verrattuna. Kun nämä on löydetty, tehdään analyysi siitä mitä vaaditaan, jotta halutun järjestelmän vaatimuksenmukaisuudet täyttyvät. Tämän jälkeen prosesseja, käytäntöjä ja organisaation kulttuuria lähdetään systemaattisesti rakentamaan, jotta haluttu järjestelmä voidaan ottaa käyttöön. Käyttöönoton jälkeen osa yrityksistä haluaa virallisen sertifikaatin järjestelmän käytöstä, mutta tämä ei kaikissa tapauksissa ole tarpeellista.
- Projektin kestoon ja työmääriin vaikuttavat oleellisesti yrityksen lähtötilanne. Jossain organisaatioissa tietoturva on jo viety hyvin pitkälle ilman hallintajärjestelmää, kun taas osassa yrityksiä tietoturvakäytännöt ovat vasta alussa.
- Hallinnollinen tietoturva auttaa yrityksiä sekä erilaisia organisaatioita hallitsemaan tietoturvaa kokonaisuutena, ei vain osana tietohallinnon tehtäviä. Modernissa liiketoiminnassa digitaaliset palvelut ovat osa yrityksen kaikkia toimintoja, jolloin tietoturvasta huolehtiminen vaatii organisaatioilta kokonaisvaltaisuutta. Tietoturvasta huolehtiminen kokonaisuutena kuitenkin kannattaa, sillä se auttaa yritystä pienentämään monia erilaisia riskejä, jotka voivat realisoitua tietoturvaloukkauksen uhriksi joutumisen vuoksia näin ollen auttaa kehittämään liiketoimintaa, sekä takaa toiminnan jatkuvuuden mahdollisen tietoturvapoikkeaman jälkeen.

- Puolustava strategia –uhkiin ja heikkouksiin keskittyvä
- Mahdollisuuksiin keskittyvä
- Missä heikkoudet on ja mitä niille tehdään
- Työaema, prosessi, riskienhallinta, operatiivinen toiminta
- Hidas poikkeamiin reagointi
- Pitää vahvistaa incident reaktioaikaa
- Kyky eristää
- Mihin vaikuttaa?
- Ylimmän johdon priorisointi → Kuinka laaja strategia? Kuinka pitkälle?
- Erilaisia edustajia pohtimaan → eri prosessien , toimittajat

Viestintä!

Uutinen

F-Secure varoittaa: yli 200 000 suomalaisen tiedot vuotaneet LinkedInistä

Joakim Kullas 31.10.2022 08:19 | päivitetty 31.10.2022 08:19 TIETOVUODOT TIETOMURROT SOSIAALINEN MEDIA HAKKERIT

LinkedIn kiistää väitteet tietomurrosta ja korostaa työskentelevänsä tietoturvan eteen päivittäin.

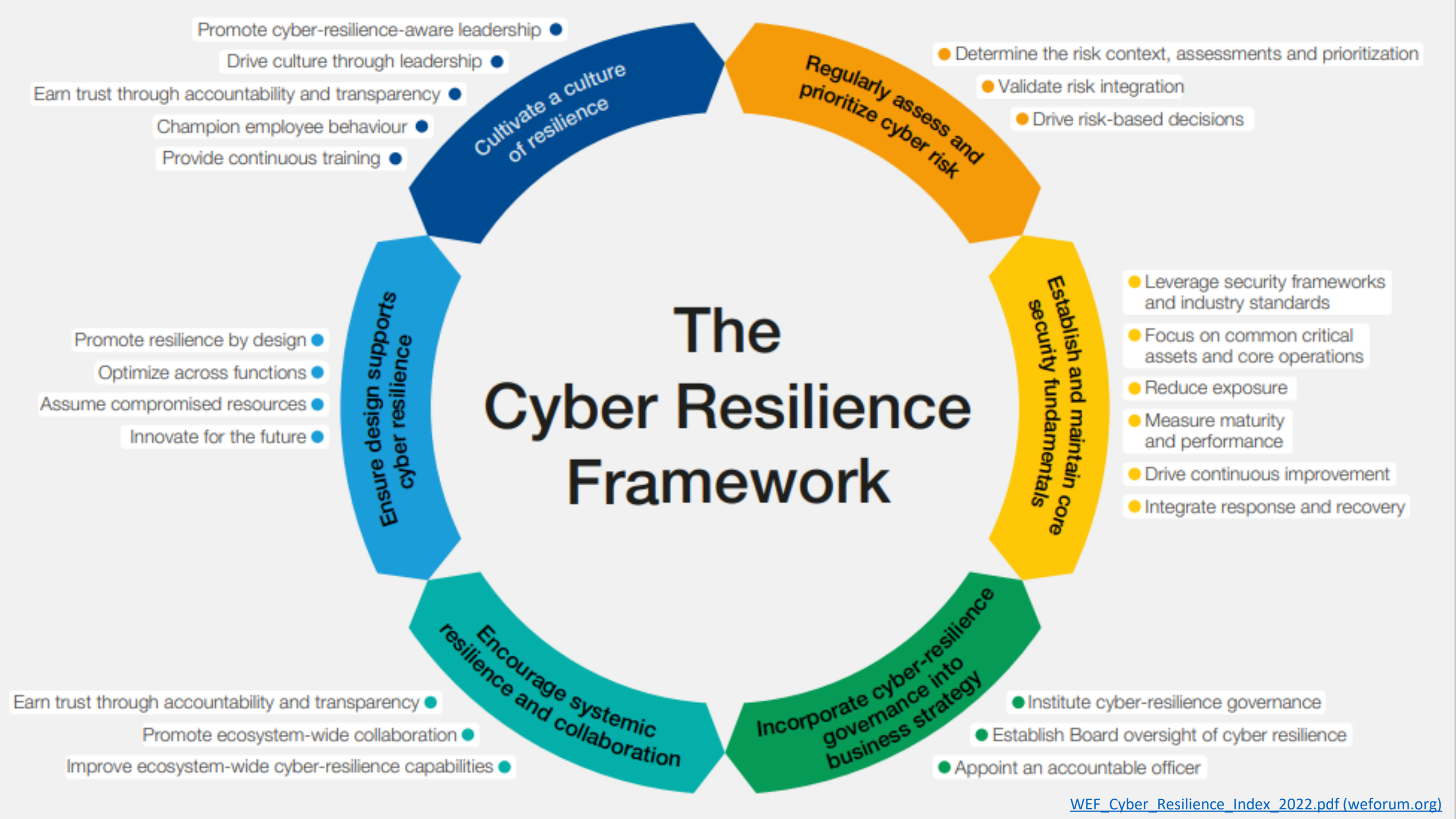
Tietovuoto. Vuotaneita tietoja saatetaan käyttää tarkasti kohdennettuihin kalasteluhyökkäyksiin. THOMAS TRUTSCHEL

Uponoriin epäillään kohdistuneen tietomurto kiristyshyökkäyksen yhteydessä – koskee myös asiakkaita

Mahdollinen tietomurto koskee Uponorin työntekijöiden, asiakkaiden ja kumppanien tietoja. LEHTIKUVA

JULKAISTU 18.11.2022 10:36

Kaksi viikkoa sitten kiristyshaittaohjelmalla tehdyn hyökkäyksen kohteeksi joutunut Uponor kertoo löytäneensä merkkejä tietomurrosta järjestelmiinsä.



WEF_Cyber_Resilience_Index_2022.pdf (weforum.org)

Kybernyrkki pöytään

Kyberturvallisuudesta puhutaan paljon, mutta silti Suomelta puuttuu suunnitelma kyberhyökkäyksen varalle, sanoo Catharina Candolin, joka tuntee aiheen monipuolisemmin kuin juuri kukaan muu.

TILAAJILLE

Elina Lappalainen HS
13.1. 7:00 | Päivitetty 13.1. 13:58

JOS joku maa tekisi lamauttavan kyberiskun suomalaiseen energiainfrastruktuuriin, pankkiin tai muuhun kriittiseen kohteeseen, miten Suomi reagoisi?

Mitkä olisivat vastatoimet? Kuka johtaisi operaatiota?

Politiikka | **Kyberpuolustus**

Moni maa ottaa Suomesta mallia, sanoo valtion kyberturvallisuus-johtaja

Asiantuntija Catharina Candolin kritisoi Suomen kyberturvallisuutta. Puolustusministeriön tietohallintojohtaja ja valtion kyberturvallisuusjohtaja vastaavat arvosteluun. Ministeriössä selvitetään muun muassa sitä, miten Suomi voi tulevaisuudessa vastata kyberhyökkäyksiin.

Puolustusministeriön tietohallintojohtaja Mikko Soikkeli (vas.) ja valtion kyberturvallisuusjohtaja Rauli Paananen ottavat kantaa Catharina Candolinin esittämään arvosteluun.
KUVA: PUOLUSTUSVOIMAT, MIKA RANTA / HS & JUSSI NUKARI / LEHTIKUVA

Veli-Pekka Lehtonen HS
13.1. 19:45

VALTION kyberturvallisuusjohtaja **Rauli Paanasen** mielestä julkishallinnon arvostelu kyberturvallisuusasioissa ei osu maaliin. ”Väite, että kyberasioihin ei olisi reagoitu, ei pidä paikkaansa”, Paananen sanoo.

Määritelmiä - turvallisuuskulttuuri

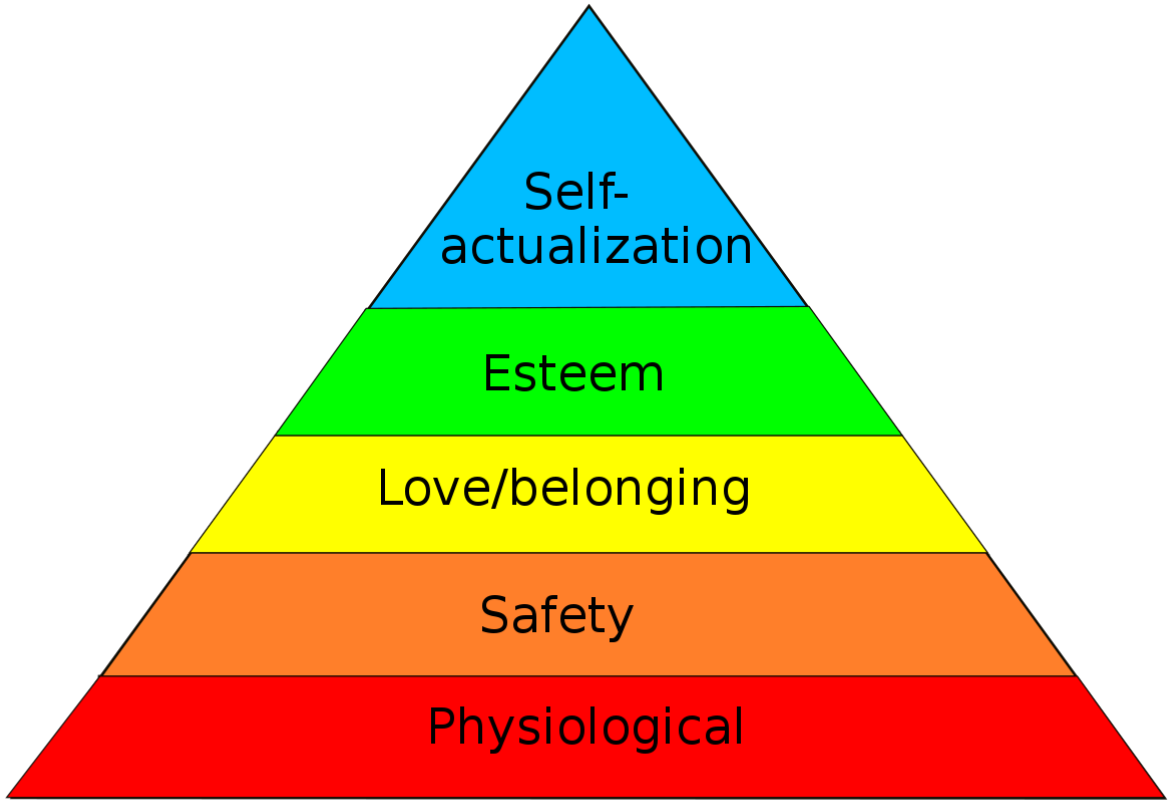
- Turvallisuuskulttuuri heijastaa organisaation perusarvoja, normeja, olettamuksia ja odotuksia, jotka sisältyvät yrityksen toimintaperiaatteisiin.

Määritelmiä – riskien arviointi

- Riskien arviointi on laaja-alaista ja järjestelmällistä vaarojen ja tunnistamista ja niiden merkityksen arvioimista.
- Riskien arvioinnin tavoitteena on turvallisuuden parantaminen.

Määritelmiä – riskienhallinta

- Riskienhallinta on osa turvallisuusjohtamista. Se on järjestelmällistä työtä toiminnan jatkuvuuden varmistamiseksi.
- Riskienhallinta tarkoittaa kaikkea organisaatiossa tehtävää toimintaa riskien pienentämiseksi tai poistamiseksi.
- Käytännön työelämässä riskienhallinta on turvallisuusjohtamisen työväline



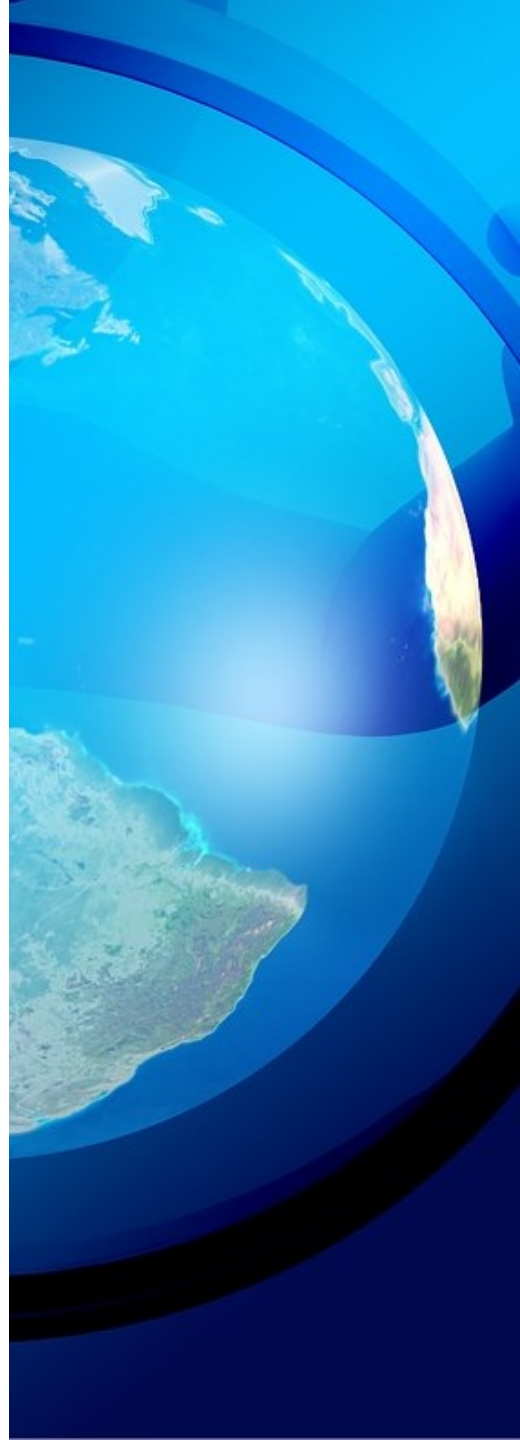
Miten turvallisuudentunnetta voidaan organisaatiossa vahvistaa?

KESKUSTELU


Strategia
Riskienhallinta
Turvallisuusjohtaminen
Suunnittele
Toteuta
Arvioi
Paranna
Tieto-
turvallisuus
Tuotannon
ja toiminnan
turvallisuus
Toimitila-
ja kiinteistö-
turvallisuus
Työ-
turvallisuus
Liiketoiminnan
jatkuvuus,
turvallisuus ja
vaatimusten-
mukaisuus
Varautuminen
ja kriisin-
hallinta
Ympäristö-
turvallisuus
Väärinkäytösten
ja poikkeamien
hallinta
Henkilöstö-
turvallisuus
Pelastus-
turvallisuus
Turvallisuuskulttuuri

Suunnittele

- Suojattavien kohteiden määrittely
- Luokittelu ja taso
- Riippuvuudet
- Järjestys
- Kontrollit
- Osaaminen
- Viestintä
- Arviointi
- Kehittäminen




Compliance
Security Policies
Organization of Information Security
Asset Management
Access Management
Communications Security
Physical & Environmental Security
Operations Security
Cryptography
Supplier Relationship
System Acquisition, Development & Maintenance
Information Security Aspects of Business Continuity Management
Information Security Incident Management
Human Resource Security
MAINTAIN & IMPROVE
SECURITY & POLICY OBJECTIVES
RISK ASSESSMENT & CONTROLS
IMPLEMENT RISK TREATMENT PLAN
MONITOR & REVIEW ISMS
ISMS
Management Responsibility
Competence Awareness Training
Requirement Documentation

- Miten tieto- ja kyberturvallisuus tulisi olla resursoitu?
- Osa-alueet
- Vastuut
- Mitä eri vaihtoehtoja
- Titujoht liitoksissa kaikkeen
- Johtaminen samaa, konteksi tietoturva
  - Yhteistyö
  - Viestintä
  - Mitä johtamiseen kuuluu
  - Riskienarviointi
  - Osaaminen

- Mitä kehitettävää tietoturvan johtamisessa omassa organisaatiossasi on
- Eri toteutusten plussat ja miinukset?
- Siiloutuminen
- Sidosryhmänalyysi

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Monimutkaisuus, riippuvuudet

Suojattavat kohteet, mitä suojataan, miksi, miltä?

- Työsuhteenaikaiset uhat

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

- Vuosikello?
- Kybermittari

Yrityksen tietojen luokittelu voidaan toteuttaa esimerkiksi neliportaisesti (Taulukko 8).

TIEDON LUOKKA	TIEDON ILMITULON VAIKUTUS YRITYKSEEN
4	Tiedon ilmitulo ei aiheuta vahinkoa yritykselle
3	Tiedon ilmitulo aiheuttaa vähäisiä taloudellisia tai toiminnallisia vahinkoja yritykselle
2	Tiedon ilmitulo aiheuttaa merkittäviä lyhytaikaisia seurauksia toiminnalle tai operatiivisten tavoitteiden saavuttamiselle
1	Tiedon ilmitulo aiheuttaa vakavia seurauksia strategisten tavoitteiden saavuttamiselle tai vaarantaa yrityksen olemassaolon

Taulukko 8: Esimerkki tiedon luokittelusta ja luokittelukriteereistä (mukaillen ISO 27002 2017)

	ITSENÄINEN TOIMIJA	VÄRVÄTTY
TEKIJÄ	Useimmiten tutkija, insinööri, ohjelmoija tai myyjä	Sekä tekniset että ei-tekniset työntekijät
TEON AIKAIKKUNA	Yleensä 60 päivää ennen tai jälkeen työpaikassa lopettamisen	Tapahtuu pitkän ajan kuluessa
		Ensimmäisen teon jälkeen voi kulua pitkä aika ennen seuraavaa tekoa
MOTIVAATIO-TEKIJÄ	Oman kilpailevan toiminnan aloittaminen	Taloudelliset ongelmat tai ahneus
	Uuden työpaikan saaminen	Tyytymättömyys nykyiseen asemaan
		Kolmas osapuoli: Ulkomainen tiedustelupalvelu tai ulkomainen organisaatio (yritys tai rikollisjärjestö)
TEON TOTEUTUS-TAPA	Tiedon siirtäminen pois työpaikalta sähköpostitse, usb-muistivälineellä, paperisina asiakirjoina, jne	Kattaa kaikki toteutustavat
TEON KOHDE	Vie yrityksestä tietoa, jonka kanssa ovat työskennelleet	Vie pyydettyä tietoa yrityksestä, pyrkii peittämään teon jäljet

Taulukko 3: Insider-uhkaprofiilit (mukaillen Kont ym. 2015, 15)

Training and Policies: practical considerations

- Security people do not enjoy the best reputation; they are often seen as an obstacle for operations

- This leads to Shadow IT
- And it makes your job impossible

- So try to implement enforceable, fair policies that have management backing, and memorable, continuous training