Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet

#tuki2018 #stöd2018

Työpaja #4 – 29.9.2017

- Rekisterinpitäjän velvollisuuksien toteuttaminen
- **Riskienhallinta osa 4, tietosuojanäkökulma**

Kuntaliitto Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintäteknikkakeskus

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto

Tilaisuuden ohjelma

#tuki2018 #stöd2018

- 8.30 Kahvi
- 9.00 Tilaisuuden avaus – Tuula Seppo, Kuntaliitto & Kimmo Rousku, valtiovarainministeriö
- 9.15 Rekisterinpitäjän velvollisuuksien toteuttaminen
- 10.30 Bio- ja jaloittelutauko
- 10.45 Työpaja jatkuu + ryhmätyö ja sen purku
- 12.00 Lounastauko (omakustanne)
- 13:00 Kokemuksia tietosuojasta – Anna Hautala, POHA
- **13.30 Riskienhallinta osa 4, tietosuojanäkökulma**
- 14.30 Kahvitauko
- **14.45 Työpaja jatkuu**
- **16.00 Yhteenveto ja kotitehtävä**
- 16.15 Työpaja päättyy

Riskienhallinta osa 4: Tietosuojanäkökulma

Työpajan sisältö

#tuki2018 #stöd2018

Riskienhallinnan tietosuojanäkökulma

- **Riskilähtöinen tietosuoja, rekisteröidyn riski, milloin rekisteröidylle aiheutuu suuri riski?**
- **Tietosuoja- ja tietosuojatoiminnan riskejä, tietosuojariskien vaikutuksia, tietosuojariskien kartta**

Riskienhallinnan kertaus aikaisemmista työpajoista

Kuntaliitto Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintäteknikkakeskus

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto

pauli.wihuri@kpmg.fi
+358 60 62344

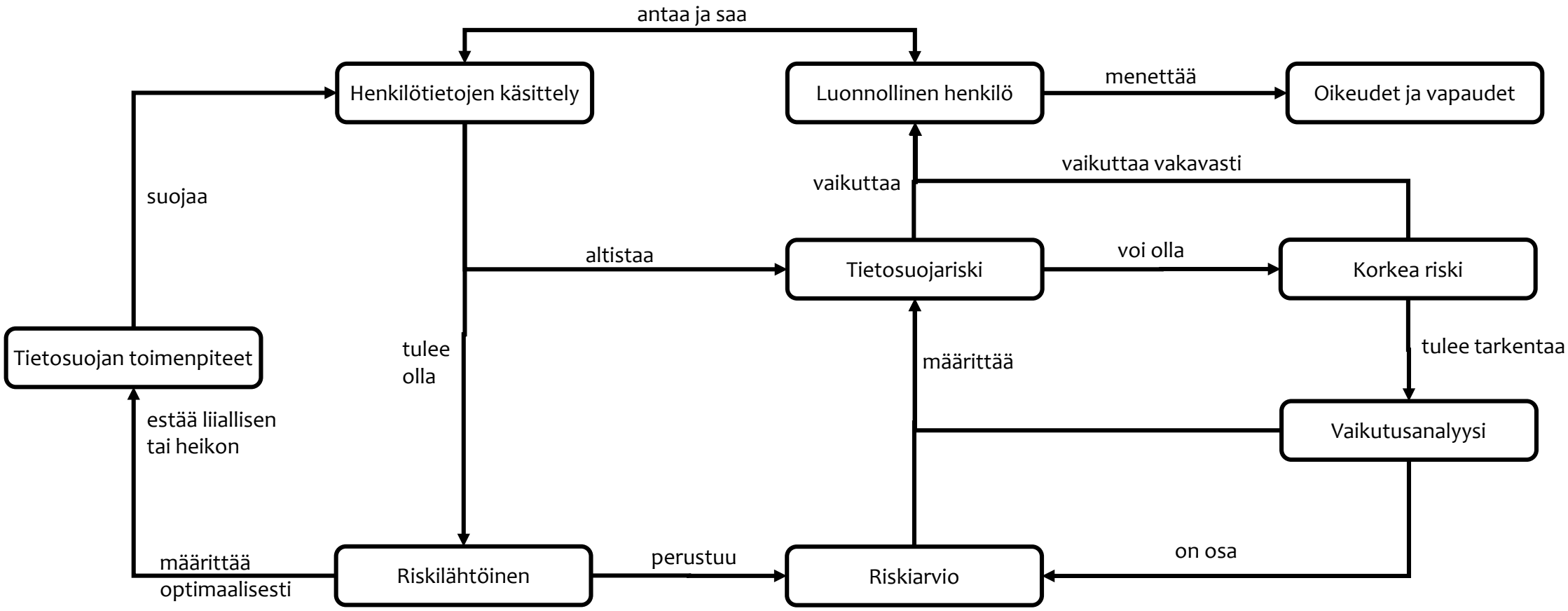
ISO 31000 standardin lainaus tai sovellus tai EU:n ohjaus

VAHTI 2/2017 ohje riskienhallintaan lainaus tai sovellus

Esittäjän sovellus

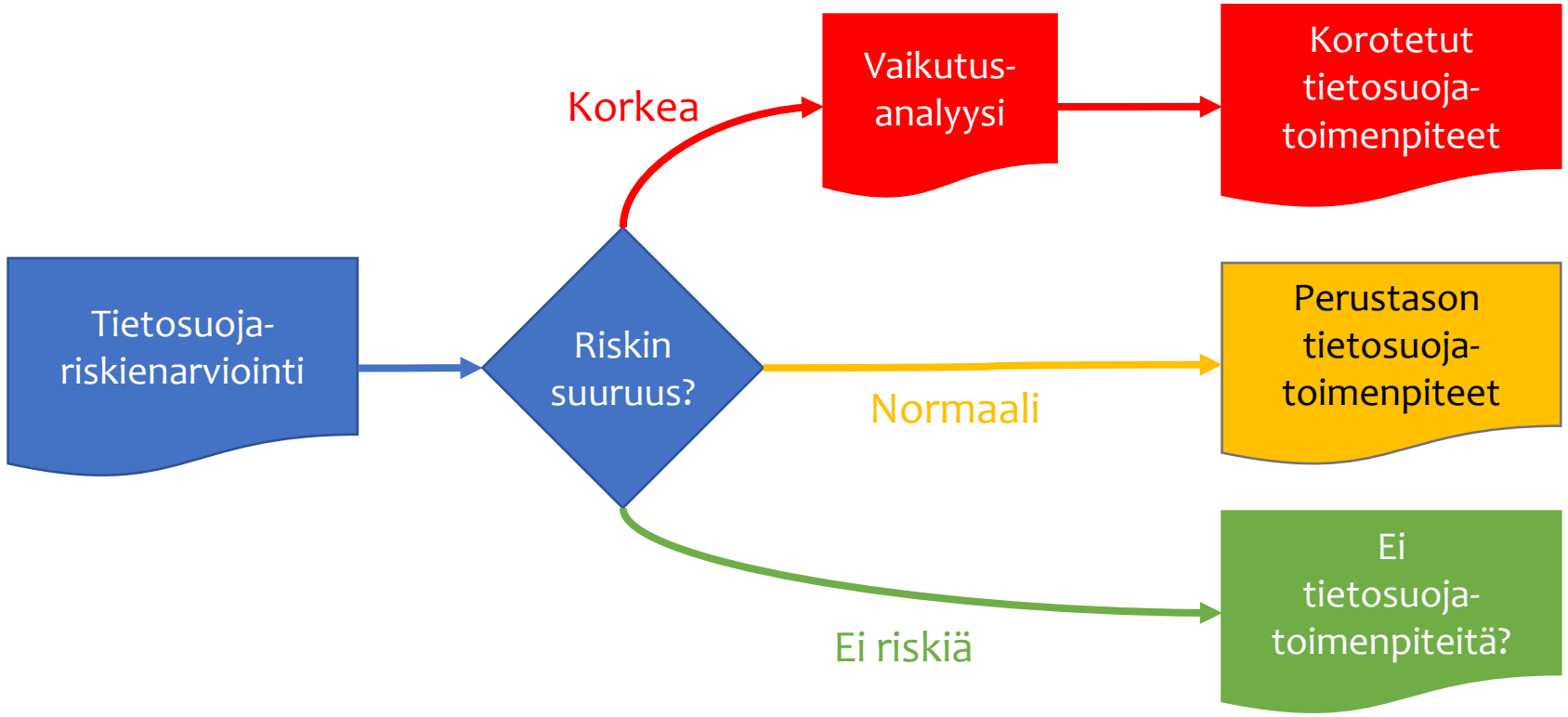
Riskilähtöinen henkilötietojen käsittely

#tuki2018 #stöd2018



Tietosuojariskeistä periytyvä tietosuojan taso

#tuki2018 #stöd2018



Riskilähtöinen tietosuoja suojatoimien suhteuttamiseksi

#tuki2018 #stöd2018

- Rekisterinpitäjän velvoitteiden määräytymisen osalta on omaksuttu riskiperusteinen lähestymistapa
- Tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin
- Pyritään suhteuttamaan tarpeelliset toimenpiteet kulloinkin henkilötietojen käsittelyyn liittyvän riskin mukaisesti ja välttämään matalariskisen toiminnan ylisääntelyä

Riski rekisteröidyn oikeuksille ja vapauksille

#tuki2018 #stöd2018

- Tietosuoja-asetuksen velvoitteet ja asianmukaiset **suojatoimet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin**
- Tietosuoja-asetuksessa riskeillä tarkoitetaan
  - henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja
  - esimerkiksi silloin, kun käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon tai pseudonymisoinnin kumoutumiseen

Rekisteröidyn vapaudet ja oikeudet

#tuki2018 #stöd2018

EUROOPAN UNIONIN PERUSOIKEUSKIRJA (2000/C 364/01)
I IHMISARVO
II VAPAUDET
III TASA-ARVO
IV YHTEISVASTUU
V KANSALAISTEN OIKEUDET
VI LAINKÄYTTÖ
VII YLEISET MÄÄRÄYKSET

Microsoft Word Document

Henkilötietojen käsittelyn riskiarvio

#tuki2018 #stöd2018

- **Rekisterinpitäjän on tehtävä perusteellinen arvio henkilötietojen käsittelyyn liittyvistä riskeistä,** jotta rekisterinpitäjä voi toteuttaa asetuksen sisäänrakennettua ja oletusarvoista tietosuojaa ja muita asetuksessa säädettyjä velvollisuuksia

Korkea riski

#tuki2018 #stöd2018

- Riski voi olla korkeampi silloin, kun käsitellään esimerkiksi
  - erityisiä henkilötietoryhmiin kuuluvia tietoja,
  - heikossa asemassa olevien (esimerkiksi lasten) tietoja
  - suuria määriä henkilötietoja ja käsittely koskee suurta rekisteröityjen määrää.
- Riski voi olla korkeampi myös, kun arvioidaan henkilökohtaisia ominaisuuksia − esimerkiksi silloin, kun kyseessä on henkilöprofilointia varten suoritettu analyysi.

Milloin henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin? *Jos kaksi tai useampi alla olevista täyttyy..*

#tuki2018 #stöd2018

1. **Henkilön arviointi, profilointi tai pisteytys** (talous, terveys, harrastukset, käyttäytyminen, sijainti, liikkuminen)
2. **Automatisoitu päätöksenteko tai vaikutus henkilön suhteen** (syrjinnän mahdollisuus virheestä)
3. **Järjestelmällinen valvonta ja kontrolli kohdistuu henkilöön** (tietoisuus valvonnasta ja kontrollista)
4. **Sensitiivinen / arkaluontoinen henkilötieto**
5. **Ihmismassojen henkilötietojen käsittely** (määrä, osuus populaatiosta, tiedon laajuus, kesto, maantieteellinen kattavuus)
6. **Henkilötietovarantojen yhdistäminen tai täsmäyttäminen** (eri toiminnot, rekisterinpitäjät, yllättää henkilön)
7. **Heikon/haavoittuvan/hauraan ihmisen henkilötietojen käsittely** (henkinen, suhteen epätasapaino, voimasuhde)
8. **Teknologisten ja organisatoristen ratkaisujen soveltaminen tai luova käyttö** (hahmontunnistus, seurausten epävarmuus)
9. **Tiedon siirtäminen EU:n ulkopuolelle** (maiden erilaiset käytännöt, jatkosiirto)
10. **Kun henkilötietojenkäsittelyn tarkoituksena on päättää tai estää palveluiden, sopimuksen tai oikeuksien käyttäminen** (pääsykontrolli, hyväksyntätilanne)

ARTICLE 29 DATA PROTECTION WORKING PARTY Guidelines on Data Protection Impact Assessment (DPIA) and **determining whether processing is "likely to result in a high risk"** for the purposes of Regulation 2016/679

Korkean riskin esimerkkejä

#tuki2018 #stöd2018

Henkilötietojen käsittely	Korkean riskin kriteerit	Tietosuojan vaikutusanalyysi?
Sairaalan potilasjärjestelmä	Sensitiivinen tieto (1) heikossa asemassa olevasta henkilöstä (2)	Kyllä
Maanteiden valvontajärjestelmä tunnistaa yksittäisiä rekisterikilpiä ja analysoi ajokäyttäytymistä	Järjestelmällinen valvonta (1) sekä luova teknologian käyttö ja soveltaminen (2)	
Yritys valvoo henkilöstön liikkumista, toimintaa, työpistettä ja tietojärjestelmien käyttöä	Järjestelmällinen valvonta (1) heikommassa asemassa olevasta henkilöstä (2)	
Sosiaalisen median käyttäytymisprofiilien ja kontaktiverkostojen kerääminen	Ihmismassojen (1) profilointi ja pisteytys (2) sekä automaattinen päätöksenteko (3)	
Verkkojulkaisun sähköpostilista lähettää päivittäisen koosteen verkkojulkaisun aiheista	Ei (riippuu verkkojulkaisun luonteesta)	Ei ehkä
Verkkokauppa näyttää kohdistettuja mainoksia perustuen aikaisempaan ostokäyttäytymiseen	Profilointi ja pisteytys (1), mutta ei järjestelmällistä tai laajaa	

Tietosuojariskit

Tietosuojariskit rekisteröidylle (=rekisteröidyn oikeudet tai vapaudet vaarantuvat tietoriskien vuoksi)

- Henkilötieto ei ole saatavilla organisaation virkamiehelle, henkilötiedon käsittelijälle ja/tai rekisteröidylle (asiakas, kansalainen, kumppani, työntekijä)
- Henkilötieto vuotaa organisaation sisällä tai ulkopuolelle sivullisille
- Henkilötieto on virheellinen, vanhentunut, puutteellinen tai hävinnyt
- Mihinkään henkilötietoon ei pääse laajan tietojärjestelmähäiriön vuoksi

Tietosuojatoiminnan riskit (=rekisteröidyn oikeudet tai vapaudet vaarantuvat tietosuojakyvykkyyden puutteen tai heikkouden vuoksi)

- Henkilötiedon käsittely ilman laissa määriteltyä perustetta (ml. asiakkaan suostumus)
- Henkilötietojen käsittely muussa kuin alkuperäisessä, määritellyssä käyttötarkoituksessa
- Rekisteröidyn oikeuksia ei pystytä toteuttamaan (esim. tietojen käsittelyn rajoittaminen)
- Henkilötietojen käsittely ei ole hallittua (esim. organisaation tai toimittajan toiminta on puutteellista tai virheellistä – ohjeistuksen, seurannan tai toimittajahallinnan/sopimuksien puutteet)
- *Henkilötiedon väärinkäytös (esim. henkilötiedon käsittelijä käyttää salassa pidettävää henkilötietoa rikolliseen tarkoitukseen, julkisuuden henkilön tietojen urkintaan tai kiristämiseen)*

Tietosuojariskien vaikutuksista

#tuki2018 #stöd2018

Tietosuojariski	Operatiivinen vaikutus yksikön toiminnalle	Vaikutus koko organisaatiolle	Tietosuojariski rekisteröidylle	Vaikutuksia rekisteröidylle
Henkilötieto ei ole saatavilla virkamiehelle, henkilötiedon käsittelijälle ja/tai rekisteröidylle (asiakas, työntekijä)	Valmistelu ja päätöksenteko viivästyy, määräajan ylitys, työajan hukkaaminen	Tuottavuuden lasku, maineen menetys, korjauskustannukset, oikeudenmenetykset, korvausvastuut ja sakot	Pääsy omiin tietoihin estyy, viivästynyt päätös tai toiminta, oikeuksien ja/tai vapauksien menetys	Potilaan hoitotoimenpiteiden viivästyminen, velkajärjestelyn viivästyminen ja taloudelliset menetykset
Henkilötieto vuotaa sisällä tai ulkopuolelle	Ilmoitusvelvollisuus valvontaviranomaiselle ja rekisteröidyille	Maineen menetys, korjauskustannukset, korvausvastuut ja sakot	Salassa pidettävien henkilötietojen luottamuksellisuuden menetys, syrjintä, vapauksien ja/tai oikeuksien menetys	Henkilön arkaluontoiset talous- tai terveystiedot tulevat yleiseen tietoon
Henkilötieto on virheellinen, vanhentunut, puutteellinen, hävinnyt tai tuhoutunut	Virheellinen päätös (jos ei huomata) tai toiminta, käsittelyä rajoitettava (jos huomataan) ja määräajan ylitys	Maineen menetys, korjauskustannukset, korvausvastuut ja sakot	Virheellinen tai viivästynyt päätös tai toiminta, oikeuksien ja/tai vapauksien menetys	Opiskelijan koulutuspaikka jää saamatta virheellisten todistusmerkintöjen vuoksi tai oppilas jätetään vaaralliseen paikkaan
Mihinkään henkilötietoon ei pääse (laaja verkko tai tietojärjestelmähäiriö)	Päätöksenteko viivästyy, määräajan ylitys, työajan hukkaaminen ja henkilöstön turhautuminen	Tuottavuuden lasku, maineen menetys, korjauskustannukset, korvausvastuut ja sakot	Pääsy omiin tietoihin estyy, viivästynyt päätös tai toiminta, oikeuksien ja/tai vapauksien menetys	Henkilöstön palkanmaksun viivästyminen

Tietosuojatoimintariskien vaikutuksista

#tuki2018 #stöd2018

Toimintariski	Operatiivinen vaikutus yksikön toiminnalle	Vaikutus koko organisaatiolle	Tietosuojariski rekisteröidylle	Vaikutuksia rekisteröidylle
Henkilötiedon käsittely ilman laissa määriteltyä perustetta	Velvoitteiden laiminlyönti. Puutteellisen toiminnan aiheuttama tietosuojariski. Sanktio. Toiminnan korjauskustannukset.	Maineen menetys, korjauskustannukset, korvausvastuut ja sanktiot	Tungettelun, syrjinnän ja/tai kaltoin kohtelun kohteeksi joutuminen. Oikeuksien ja/tai vapauksien menetys.	Turha ajankäyttö. Henkinen kärsimys. Korjaamisen vaiva.
Henkilötietojen käsittely muussa kuin määritellyssä käyttötarkoituksessa				
Rekisteröidyn oikeuksia ei pystytä toteuttamaan		Kaikki tietosuojariskit vaikutuksineen mahdollisia.		
Henkilötietojen käsittely ei ole hallittua				
Henkilötiedon väärinkäytös		Salakatselu → Tietovuotoriski tai kiristys. Tietoväärennös → Tietovirheriski. Vahingonteko → Saatavuusriski.		

Tietosuojariskien kartta (esimerkki)

#tuki2018 #stöd2018

1 Henkilötieto voi olla virheellistä, vanhentunutta tai tuhoutunut

Vääriä johtopäätöksiä ja päätöksiä. Asiakkaalle virheellisiä toimenpiteitä. Asiakas kärsii vahinkoja (tulevaisuus, terveys, talous) tai joutua hengenvaaraan. Organisaation korvausvelvollisuus. Organisaation maine voi kärsiä. Luottamus organisaation palveluihin laskee tai menetetään. Organisaation toiminnot kärsivät. Pitkällä tähtäimellä odotettu toimintojen tehokkuuden ja tuottavuuden kasvu jää toteutumatta.

2 Henkilötieto ei jalostu (joustavuus) toiminnan kehityksen mukana

Manuaaliset työt jatkuvat. Toimintaa ei voi kehittää tarpeen mukaan. Pitkällä tähtäimellä odotettu toimintojen asiakastyytyväisyyden, tehokkuuden ja tuottavuuden kasvu jää toteutumatta.

3 Tärkeä henkilötieto ei ole saatavilla, kun sitä tarvitsee

Työt hidastuvat tai estyvät toiminnoissa ja vääriä päätöksiä vanhoilla tiedoilla. Asiakkaalle vääriä toimenpiteitä. Asiakkaat eivät voi asioida. Asiakas kärsii vahinkoja (terveys, talous) tai joutuu hengenvaaraan. Organisaatio voi joutua korvausvelvolliseksi. Maine kärsii kolauksen. Luottamus palveluihin laskee.

4 Arkaluontoinen henkilötieto vuotaa sivullisille

Suuri ylimääräinen työ asian selvittämiseksi ja korjaamiseksi. Työtä menee tuottamattomaan asiaan. Asiakas kärsii henkisiä ja taloudellisia vahinkoja sekä menettää luottamuksen palveluihin. Mikäli tapaus saa laajasti julkisuutta, organisaation maine kärsii ison kolauksen, joka vaikuttaa pitkään organisaation maineeseen.

5 Laaja odottamaton katkos tietojärjestelmien käytössä

Työt estyvät laajasti toimialoilla. Toiminta estyy. Henkilötietoja ei pysty käsittelemään. Asiakkaat eivät saa palvelua. Asiakkaat eivät voi asioida ja kärsivät vahinkoja (mahdollisuuden menetys tai terveydellinen tai taloudellinen menetys) tai joutuvat hengenvaaraan. Organisaatio kärsii mittavia taloudellisia vahinkoja ja joutuu korvausvelvolliseksi. Laaja toimintahäiriö saa helposti laajasti julkisuutta ja organisaation kärsii ison kolauksen sekä vaikuttaa pitkään asioinnissa organisaation kanssa. Luottamus palveluihin kärsii.

Lähes varma (4)		4	2	5
Toden-näköinen (3)				3
Mahdol-linen (2)				1
Epätoden-näköinen (1)				
(↑) Toden-näköisyys Vaikutus (→)	Vähäinen (1)	Kohta-lainen (2)	Merkittävä (3)	Kriittinen (4)

4. työpajan riskienhallinnan ryhmätyö

#tuki2018 #stöd2018

Tehkää taulukko:

a) Mitkä organisaationne toimintojen henkilötietojen käsittelyt voivat aiheuttaa korkean riskin rekisteröidylle?

b) Mitkä organisaationne toimintojen henkilötietojen käsittely ei aiheuta korkeaa riskiä rekisteröidylle?

Henkilötietojen käsittely	Korkean riskin kriteerit	Tietosuojan vaikutusanalyysi?
Sairaalan potilasjärjestelmä	Sensitiivinen tieto (1) heikossa asemassa olevasta henkilöstä (2)	Kyllä
Maanteiden valvontajärjestelmä tunnistaa yksittäisiä rekisterikilpiä ja analysoi ajokäyttäytymistä	Järjestelmällinen valvonta (1) sekä luova teknologian käyttö ja soveltaminen (2)	
Yritys valvoo henkilöstön liikkumista, toimintaa, työpistettä ja tietojärjestelmien käyttöä	Järjestelmällinen valvonta (1) heikommassa asemassa olevasta henkilöstä (2)	
Sosiaalisen median käyttäytymisprofiilien ja kontaktiverkostojen kerääminen	Ihmismassojen (1) profilointi ja pisteytys (2) sekä automaattinen päätöksenteko (3)	
Verkkojulkaisun sähköpostilista lähettää päivittäisen koosteen verkkojulkaisun aiheista	Ei (riippuu verkkojulkaisun luonteesta)	Ei ehkä
Verkkokauppa näyttää kohdistettuja mainoksia perustuen aikaisempaan ostokäyttäytymiseen	Profilointi ja pisteytys (1), mutta ei järjestelmällistä tai laajaa	

Ohjeet

- **Valitkaa** keskustelun tuloksien kirjaaja
- **Tähän linkki** ryhmätyön tuloksien tallettamiseen
  Huom: Tehtävän vastaukset tullaan jakamaan ja julkaisemaan netissä osana kokonaisuuden materiaalia. Huomioithan, että **kaikki tiedot tulee olla julkisia**. Älä viittaa tässä organisaatioihin, henkilöihin tai muihin vastaaviin identifioiviin tietoihin.

Riskienhallinta osa 4: Tietosuojanäkökulma

Työpajan sisältö

#tuki2018 #stöd2018

↻ Riskienhallinnan kertaus aikaisemmista työpajoista

Kuntaliitto Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintäteknikkakeskus

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto

pauli.wihuri@kpmg.fi
+358 60 62344

ISO 31000 standardin lainaus tai sovellus

VAHTI 2/2017 ohje riskienhallintaan lainaus tai sovellus

Esittäjän sovellus

Mitä on riskienhallinta ja mikä on riski?

Riskienhallinta on toiminto, jolla johdetaan ja ohjataan organisaation riskejä.

Riskienhallintapolitiikka sisältää organisaation päättämät, kuvaamat ja dokumentoimat riskienhallintaan liittyvät periaatteet ja tavoitteet.

Riski tarkoittaa epävarmuuden vaikutusta tavoitteisiin, poikkeamaa odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna.

#tuki2018 #stöd2018

Staattinen riski
- Riski kohdistuu **omaisuuteen**
- Omaisuudella on ominaisuuksia, jotka asettavat omaisuuden riskeille alttiiksi (haavoittuvuus)
- Omaisuus tai osa siitä voidaan menettää
- Omaisuuden suojaaminen voidaan optimoida riskien mukaisesti
- **Tieto on omaisuutta,** jonka arvoa ei usein ymmärretä

Dynaaminen riski
- Riski kohdistuu **tavoitteeseen**
- Tavoitteen saavuttamisen toteutuksessa voi tapahtua odottamattomia asioita
- Vaikutus voi olla pysyvä tai tilapäinen
- Suunnitelmaa voidaan parantaa etukäteen riskien perusteella
- **Tietojen käsittely, hallinta ja kehittäminen ovat (dynaamisia) tavoitteita**

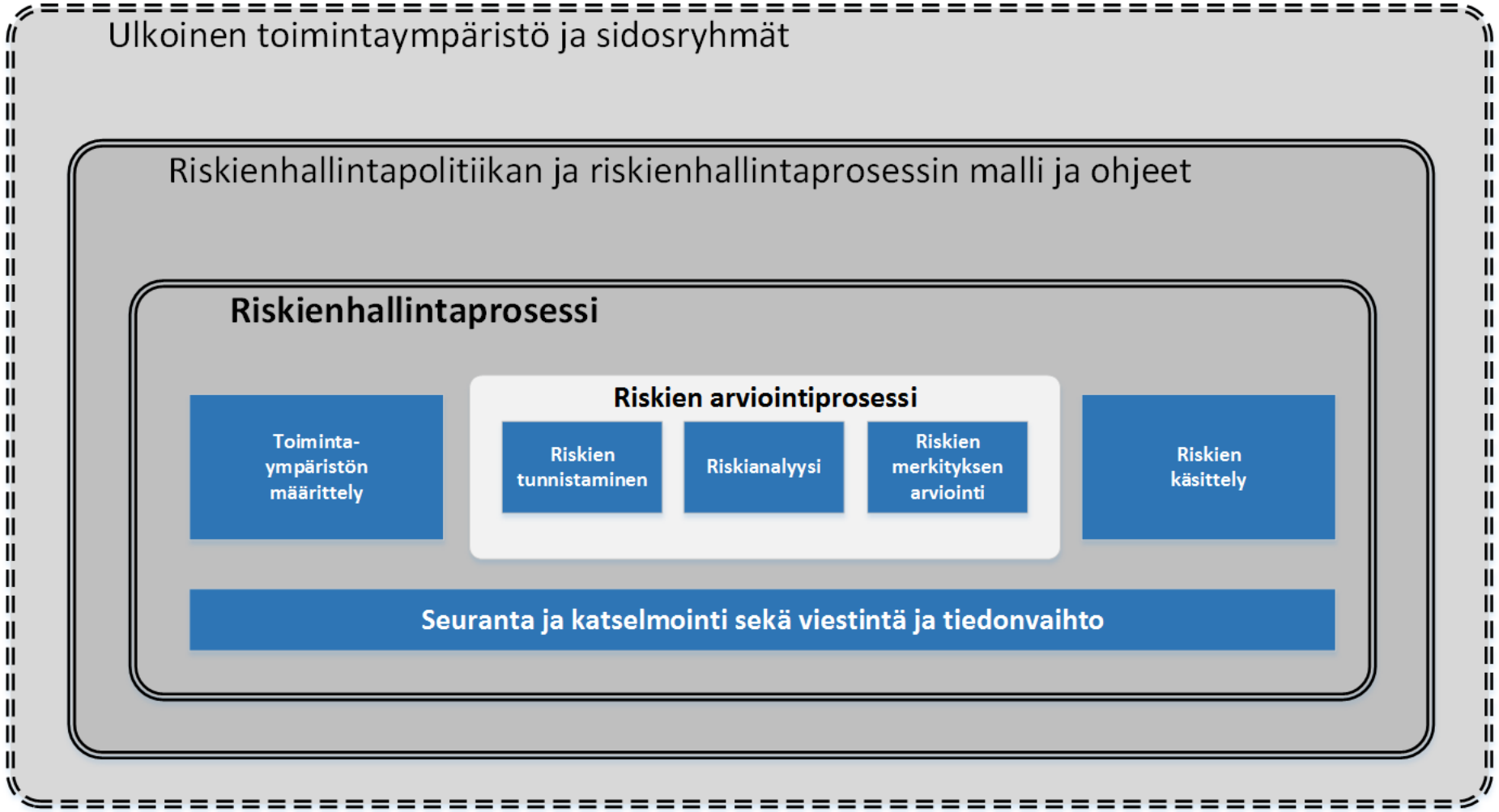
Tietoriski
- **Riski kohdistuu tietoon tai tiedon olomuotoon kuten esim. paperiarkistoon tai tietojärjestelmään, jolla käsitellään tietoa**
- Tietoon ei ehkä pääse tai sen käsittely voi olla vaikeaa/hidasta. Tieto voi vuotaa tai se voidaan menettää. Tieto voi olla virheellistä tai ei ehkä jalostu toiminnan mukaan riittävän ketterästi.
- Paperiarkistoon ei ehkä pääse katsomaan tietoa. Se voi tuhoutua tulipalossa. Arkistoon voidaan jättää laittamatta tietoa tai laittaa väärää tietoa. Se voi mennä sekaisin eikä tietoa löydy.
- Tietojärjestelmä voi lakata toimimasta tai siihen ei pääse kirjautumaan. Tietojärjestelmä voi olla monimutkainen, vaikeasti käytettävä tai kankea. Tietojärjestelmä voi tuottaa virheellisiä tuloksia. Luottamuksellinen tieto voi vuotaa asiaankuulumattomille.
- Organisaation (digitaalinen) omaisuus ja tavoitteissa onnistuminen ovat riippuvaisia tiedosta ja tietojärjestelmistä.
- Tiedon varmentaminen ja suojaaminen voidaan optimoida riskien perusteella

VAHTI 2/2017 ohje riskienhallintaan
lainaus

Esittäjän sovellus tietoriskeistä

Riskienhallinnan periaatteet, viitekehys ja prosessi

#tuki2018 #stöd2018



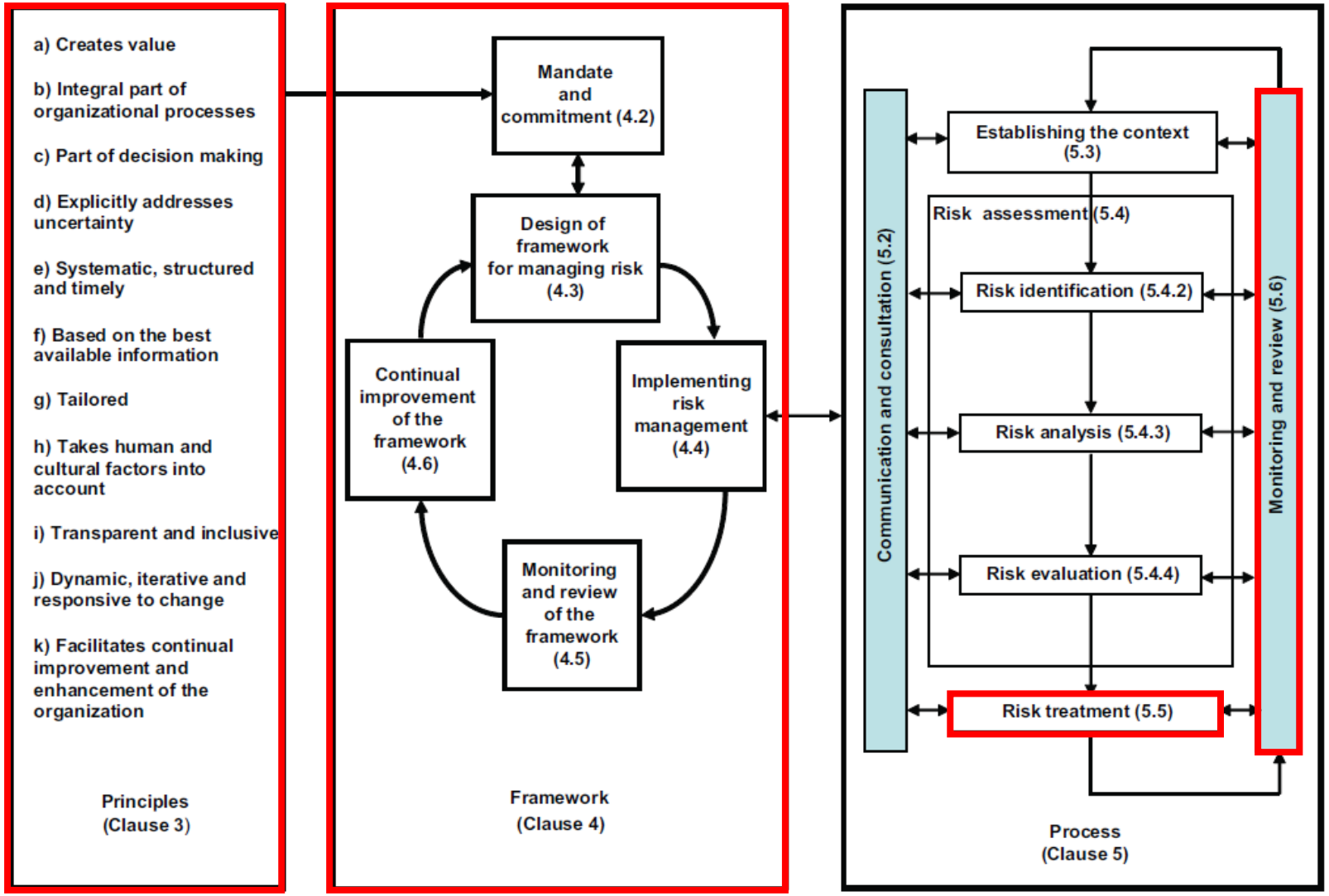
Työpajan pohjana on VAHTI 2/2017 ohje riskienhallintaan

Kuva VAHTI ohjeen sivulta 12

Riskienhallinnan periaatteet, viitekehys ja prosessi

#tuki2018 #stöd2018

Figure 1 — Relationships between the risk management principles, framework and process



Tässä työpajassa käsittelemme riskienhallinnan periaatteita, viitekehystä, riskien toimenpiteiden seurantaa ja riskiarviointityöpajan toteuttamista

ISO 31000 kuva sivulta vii

Riskienhallinnan viitekehys

Riskienhallinnan periaatteet ja organisaation ohjaus

Riskienhallinnan **VALTUUTUS** ja **SITOUTTAMINEN**

Riskienhallinnan **SUUNNITTELU** Toimintaympäristö, politiikka, integrointi, resurssit, viestintä ja raportointi

Riskienhallinnan **TOTEUTTAMINEN** Toimintamallin ja riskien hallintaprosessin jalkauttaminen

Riskienhallinnan **SEURANTA** Toimintamallin ja riskien hallintaprosessin toimivuuden arviointi ja seuranta

Riskienhallinnan **KEHITTÄMINEN** Toimintamallin ja riskien hallintaprosessin (jatkuva) kehittäminen

PDCA

"Riskienhallinnan toimintamalli"

#tuki2018 #stöd2018

Tarkennettu kuva VAHTI ohjeen liitteen sivulta 11

Riskien hallinta organisaation ydintoiminnoissa

Riskien hallintaprosessi (operatiivinen)

"Ydintoimintojen riskien hallintasuunnitelmat"

Riskienhallinnan sääntely

VALTIONEUVOSTON ASETUS TIETOTURVALLISUUDESTA VALTIONHALLINNOSSA (681/2010): *”Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava mm. siitä, että viranomaisen toimintaan liittyvät* ***tietoturvallisuusriskit*** *kartoitetaan.”*

LAKI VIRANOMAISEN TOIMINNAN JULKISUUDESTA (621/1999): *Viranomaisen on hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi* … otettava *huomioon tietojen merkitys ja käyttötarkoitus,* ***asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät****.*

KUNTALAKI (410/2015): *Valtuuston tulee päättää kunnan ja kuntakonsernin sisäisen valvonnan ja* ***riskienhallinnan*** *perusteista (14 § 7). Hallintosäännössä tulee olla myös tarpeelliset* ***määräykset hallinnon ja talouden riskienhallinnasta*** *(39 §, 47 §, 67 §, 90 §).* ***Riskienvalvonnan järjestäminen*** *tulee myös ilmetä kunnan toimintakertomuksesta (115 §). Tilintarkastajan on otettava myös kantaa, onko sisäinen valvonta ja* ***riskienhallinta*** *sekä konsernivalvonta* ***järjestetty asianmukaisesti*** *(123 §)*

ASETUS VALTION TALOUSARVIOSTA (1243/1992): *Viraston ja laitoksen johdon on huolehdittava asianmukaisista menettelyistä (sisäinen valvonta) talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin* ***riskeihin*** *nähden.*

Valikoituja lyhennettyjä lainauksia VAHTI 2/2017 ohje riskienhallintaan liitteestä

Lomake kohta 1.

#tuki2018 #stöd2018

ASETUS VIRANOMAISTEN TOIMINNAN JULKISUUDESTA JA HYVÄSTÄ TIEDONHALLINTATAVASTA (1030/1999): *Hyvän tiedonhallintatavan toteuttamiseksi viranomaisen on* ***selvitettävä ja arvioitava tietojen saatavuuteen, käytettävyyteen, laatuun ja suojaan sekä tietojärjestelmien turvallisuuteen vaikuttavat uhat****.*

TYÖTURVALLISUUSLAKI (738/2002): *Työnantajan on työn ja toiminnan luonne huomioon ottaen* ***riittävän järjestelmällisesti selvitettävä ja tunnistettava*** *työstä, työajoista, työtilasta, muusta työympäristöstä ja työolosuhteista aiheutuvat* ***haitta- ja vaaratekijät*** *sekä, jos niitä ei voida poistaa,* ***arvioitava niiden merkitys*** *työntekijöiden turvallisuudelle ja terveydelle.*

EU:N TIETOSUOJA-ASETUS (EU 679/2016): *Asetus edellyttää riskiperusteista lähestymistä. Lainaus asetuksen perusteluista:*

- **Rekisteröidyn oikeuksiin ja vapauksiin kohdistuvan riskin** todennäköisyys ja vakavuus olisi määriteltävä tietojenkäsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten mukaan. Riski olisi arvioitava objektiivisen arvioinnin perusteella, jolla todetaan, liittyykö tietojenkäsittelytoimiin riski tai korkea riski. (76)
- Tapauksissa, joissa **luonnollisten henkilöiden oikeuksiin tai vapauksiin kohdistuu korkea riski**, rekisterinpitäjän olisi kyseisen riskin erityisen todennäköisyyden ja vakavuuden arvioimiseksi käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten sekä riskin alkuperän huomioon ottaen tehtävä ennen tietojenkäsittelyä **tietosuojaa koskeva vaikutustenarviointi.** (90)

Tehokkaan riskienhallinnan periaatteet

a) **Riskienhallinta luo ja suojaa arvoa** varmentamalla organisaation tavoitteiden saavuttamista ja tuottavuuden kasvua.

b) **Riskienhallinta on sisäänrakennettu osaksi organisaation ydintoimintoja ja -prosesseja.** Riskienhallinta ei ole erillinen toiminto organisaatiossa vaan integroitu johtamiseen ja prosesseihin.

c) **Riskienhallinta tukee päättäjiä tekemään informoituja valintoja** toiminnan ja tekemisen tärkeysjärjestyksestä ja suunnasta.

d) **Riskienhallinta ottaa huomioon epävarmuudet**, niiden luonteen ja tekijät sekä miten toimia epävarmuuden keskellä.

e) **Järjestelmällinen ja ajankohtainen riskienhallinta** edesauttaa johdonmukaisten, vertailukelpoisten ja luotettavien tuloksien saavuttamisen kustannustehokkaasti.

f) **Riskienhallinta perustuu parhaaseen saatavilla olevaan informaatioon**, kun tiedon lähteenä on historiatieto, kokemus, palaute, havainnot, ennusteet ja asiantuntijuus tiedostaen tiedon mallintamisen epäkohdat ja asiantuntijoiden eriävät mielipiteet.

g) **Riskienhallinta on sovellettu organisaatioon**, sen sisäiseen ja ulkoiseen toimintaympäristöön ja epävarmuustekijöihin.

h) **Riskienhallinta ottaa huomioon inhimilliset ja kulttuurilliset tekijät** kuten ihmisten osaamisen, kyvyt ja tarkoitusperät, jotka voivat edesauttaa tai estää organisaation tavoitteiden saavuttamista.

i) **Riskienhallinta on osallistavaa ja läpinäkyvää** ottaen mukaan ajallaan sidosryhmät ja päättäjät kaikilla organisaatiotasoilla riskien määrittämiseen ja toimenpiteisiin.

j) **Riskienhallinta on jatkuvaa, toistuvaa, tarkentuvaa, uudistuvaa ja ketterää olosuhteiden, muutoksien ja tapahtumien suhteen.**

k) **Riskienhallinta tukee organisaation jatkuvaa kehittymistä** kun riskienhallintakin kehittyy organisaation kehityksen tahdissa.

Vapaasti suomennettu suoraan ISO 31000 riskienhallinnan standardista sivuilta 7-8 ja 22-23.

#tuki2018 #stöd2018

Keskimääräistä tehokkaamman riskienhallinnan ominaisuudet

1. **Riskienhallinnan jatkuvaan kehitykseen panostetaan** asettaen läpinäkyviä henkilö- ja organisaatiokohtaisia mitattavia tulostavoitteita sekä valiten seurantaan perustuvia kehityskohteita.
2. **Täysin omaksuttu tilivelvollisuus riskeistä ja riskienhallinnasta** varmistamalla koko organisaation riskitietoisuuden sekä riskien toimenpiteiden resurssit, osaamisen, seurannan ja suojauksien jatkuvan kehittämisen yhdessä sisäisten ja ulkoisten sidosryhmien kanssa.
3. **Kaikissa päätöksissä huomioidaan läpinäkyvästi riskit** riippumatta päätöksien tärkeydestä ja organisaatiotasosta, koska organisaatio on vakuuttunut riskienhallinnan tärkeydestä osana tehokasta hallintoa.
4. **Jatkuva riskien jakaminen ja raportoiminen sekä riskienhallinnan tehokkuuden viestintä** sisäisten ja ulkoisten sidosryhmien kanssa molempiin suuntiin.
5. **Täysin sisäänrakennettu riskienhallinta** on näkyvä osa yrityksen kulttuuria, kielenkäyttöä ja toimintatapoja sekä hallinta-, johtamis-, tavoiteasetanta- ja tulospalkitsemisjärjestelmiä, joiden ytimessä varmistajana on riskien hallitseminen.

Tehokkaan riskienhallinnan aikaansaannokset

- Organisaatiolla on oikea, ajankohtainen ja kattava ymmärrys riskeistään.
- Organisaatio toimii riskinsietokykynsä rajoissa.

Lomake kohta 2.

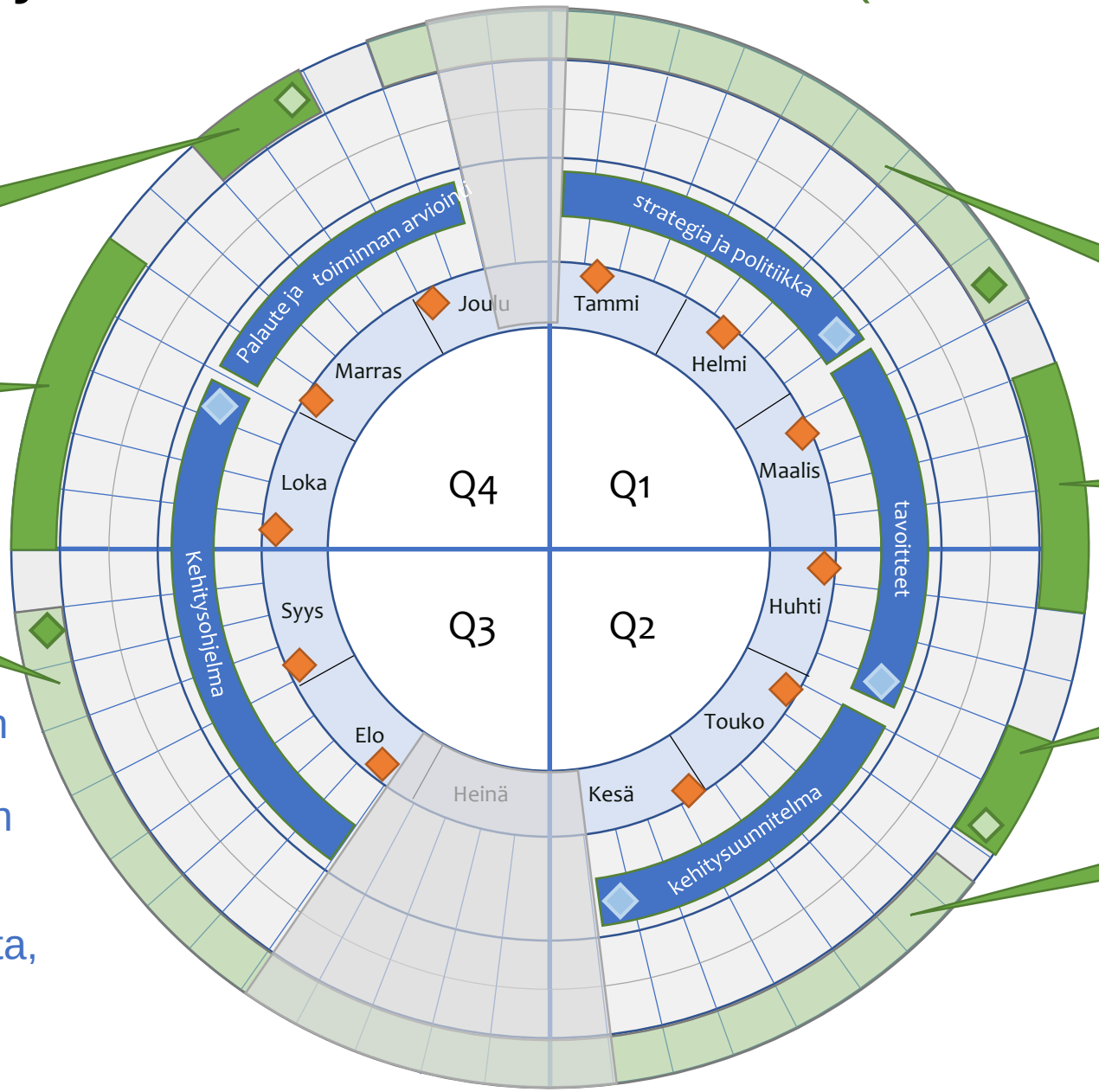
Riskienhallinnan ja riskien hallinnan vuosikello (esimerkki)

#tuki2018 #stöd2018

Riskiraportti (1.2.3)

Riskiarvioinnit (1.2.3)

Jatkuva riskien hallinta (2.13)



Jatkuva riskien hallinta (2.13)

Riskiarvioinnit (1.2.3)

Riskiraportti (1.2.3)

Jatkuva riskien hallinta (2.13)

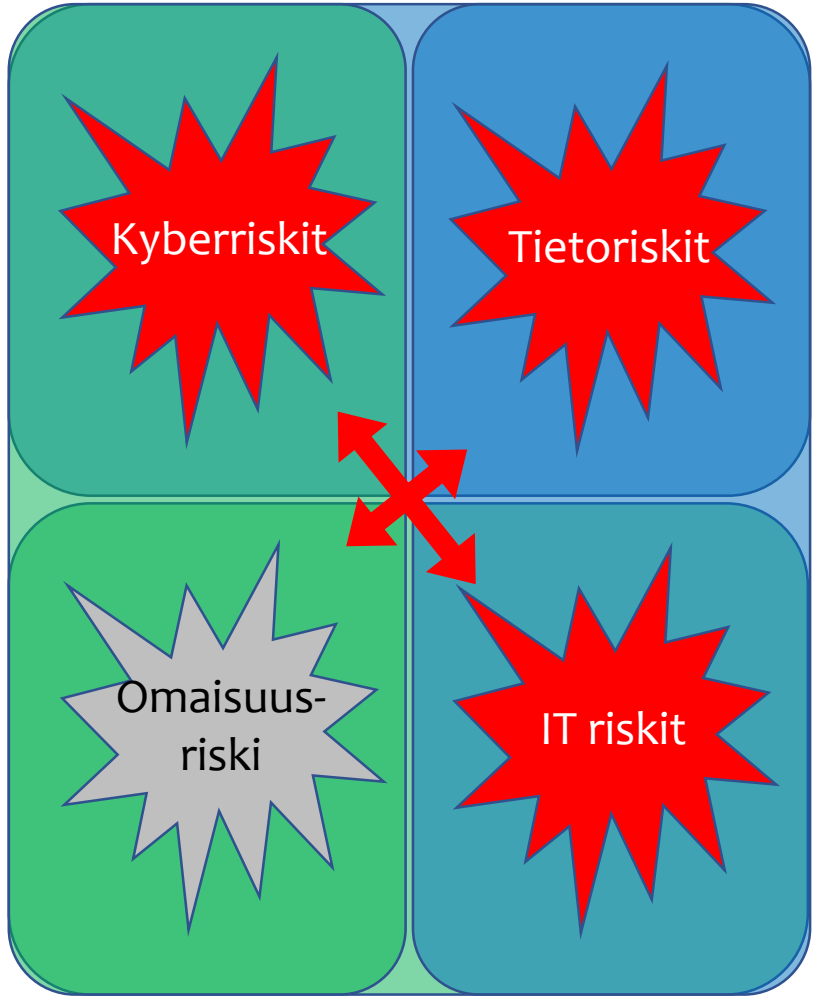
- Organisaation toiminnan tahdissa
- Sisäänrakennettu riskien hallinta organisaation ydintoiminnoissa
- Osa toiminnan johtamista, strategiaa, suunnittelua, toteutusta ja seurantaa

Sovellettu VAHTI 2/2017 riskienhallinnan ohjeesta (s. 22)

Fyysisten ja digitaalisten riskien avaruus (esimerkki)

- Hacktivisti → Automatisoidun toiminnan laitteet → Kaaos/kriisi (energialaitos, satama, infrastruktuuri, kiinteistöautomaatio, hälytyslaitteet, logistiikka, varastot)
- Rikollisjärjestö → Terveyslaitteet → Kiristys → Vammautuminen/kuolema

Lomake kohta 4.



Riskin (välitön) syy

Riskin (suora) vaikutus

Sisäinen, hacktivisti, rikollisjärjestö, valtio → hallinnon heikkous / tietojärjestelmän haavoittuvuus
→ tietovarkaus, tietoväärennös, tietokiristys, tietovuoto, palvelunesto

- (Tahallinen tai) vahinko (tuli, vesi, sähkö, verkkokaapeli), laiterautavika, inhimillinen virhe (muutos, kiire, osaaminen, kokemus) → tietojärjestelmä → palvelunesto
- Murtovaras → Laitevarkaus

Voiko näin rajusti yksinkertaistaa?

Riskien arviointiprosessi

#tuki2018 #stöd2018

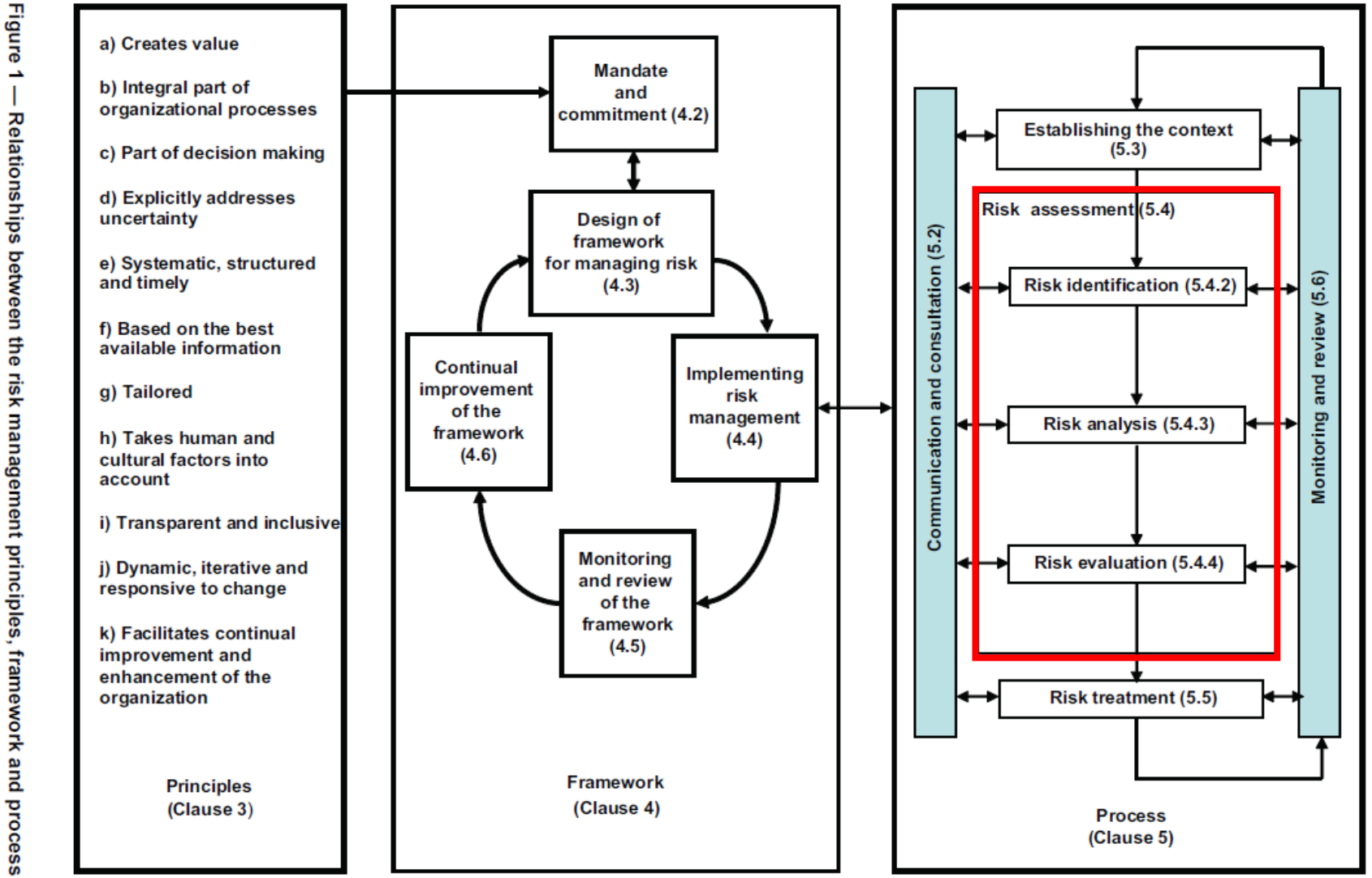


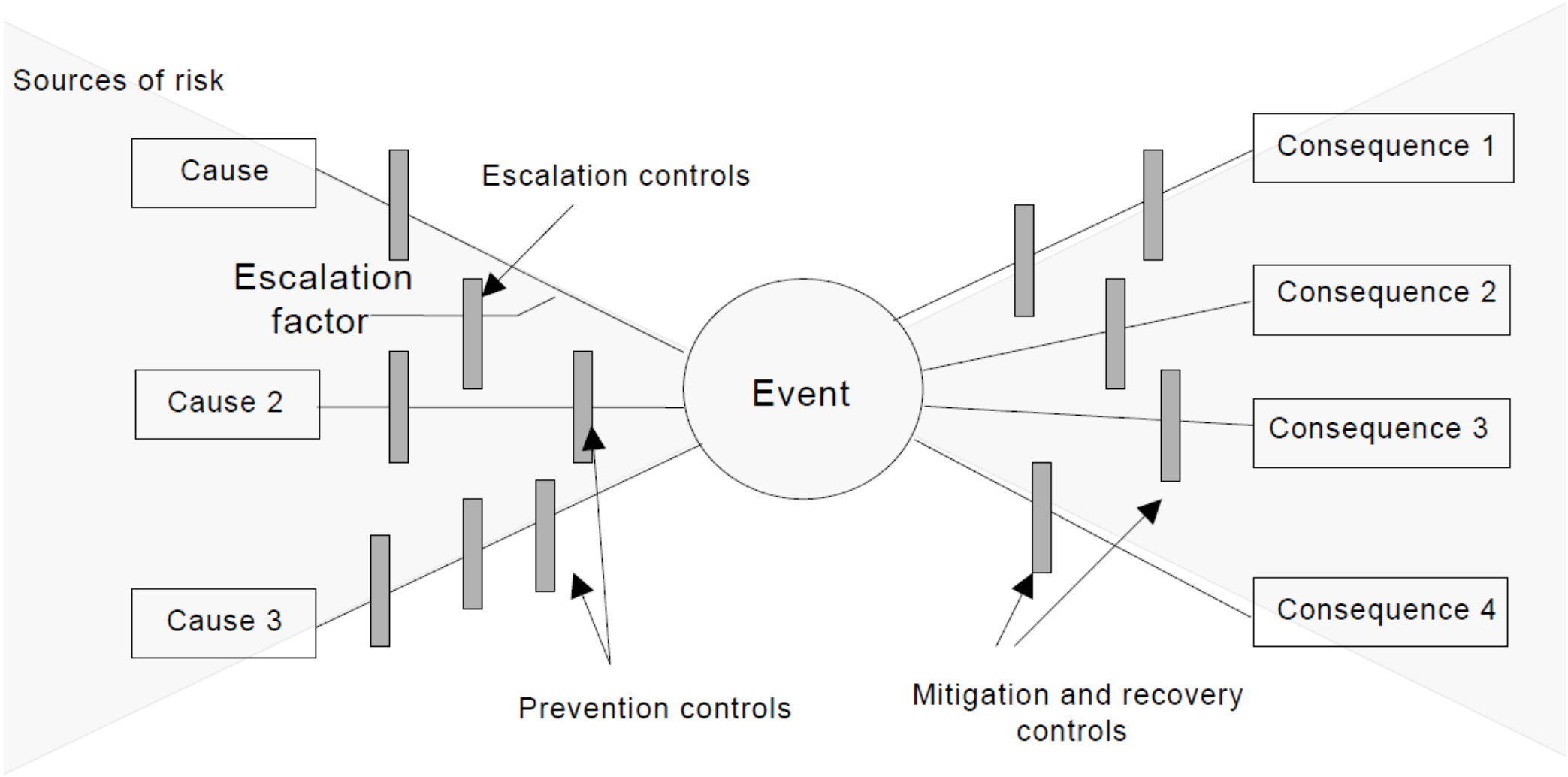
Figure 1 — Relationships between the risk management principles, framework and process

Tässä työpajassa kuljemme läpi yksinkertaistettua riskienarvioinnin prosessia

ISO 31000 kuva sivulta vii

Riskin syy-seuraus-rusetti (bowtie)

#tuki2018 #stöd2018



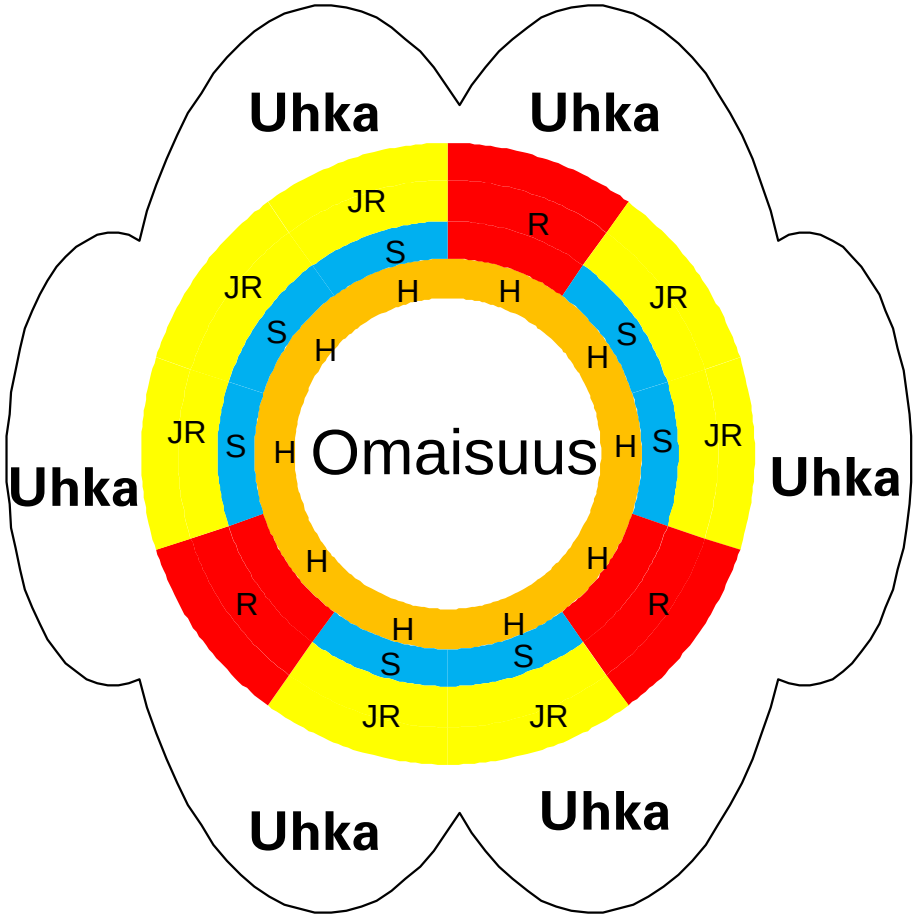
Tässä työpajassa sovellamme kevennettyä rusettianalyysia (bowtie) käyttäen vaikutus- (bia), juurisyy- (rca) ja syy-seuraus-analyysien (c&e) menetelmiä

ISO 31010 kuva sivulta 66

Ennakoiva riskiarvio ”staattiseen” omaisuuteen

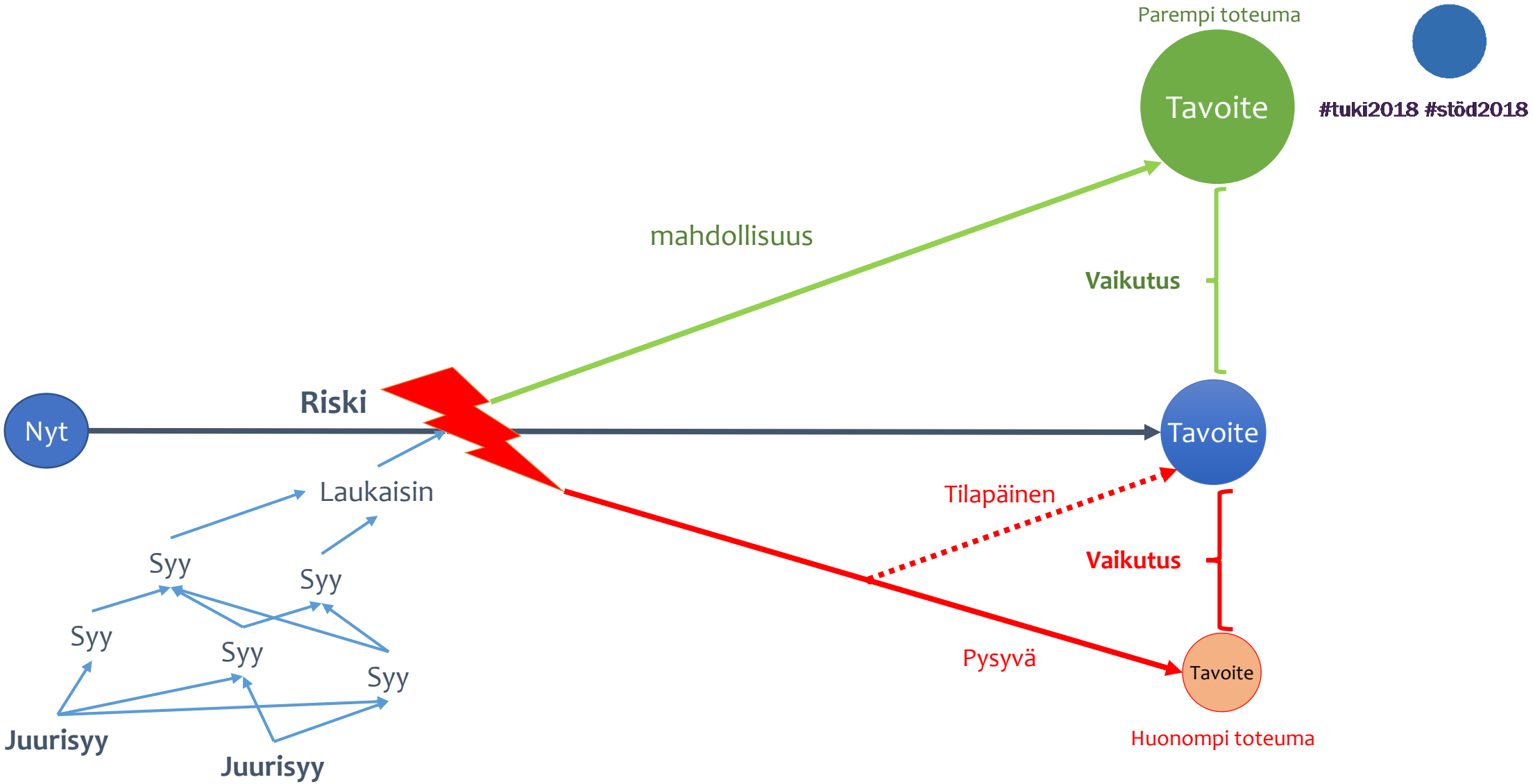
#tuki2018 #stöd2018

- Mitä on tieto-omaisuus?
- Voiko tiedolle tehdä omaisuusrekisterin?
- Mikä on tiedon arvo?
- Mitä arvoa tieto tuottaa toiminnalle?
- Mieltääkö organisaation vastuuhenkilöt omistavansa ulkoistetun tietojärjestelmän tiedon?



Haavoittuvuus
Riski
Suojaus
JäännösRiski

Ennakoiva riskiarvio dynaamiseen tavoitteeseen



Tietoriskien kartoituksen suunnittelu organisaatiolle

#tuki2018 #stöd2018

Lomake kohta 5.

- Kenelle kartoitus tehdään?
- Mitä kartoituksella tavoitellaan?
- Mitkä toiminnot valitaan kohteiksi?
- Kuka koordinoi kartoitusta?
- Ketkä suorittavat kartoituksen?
- Ketkä osallistuvat kartoitukseen?
- Miten kartoitus tehdään?
- Keille riskikartoituksen tulokset raportoidaan?
- Miten päätetään riskien omistuksesta?
- Miten sovitaan toimenpiteistä ja niiden integroinnista osaksi ydintoimintoja?
- Miten toimenpiteitä seurataan?

Tietoriskien arviointityöpajojen asialista

- **Tausta, tavoite ja odotukset**
  Mikä on organisaation määritelmä tietoriskille?
- **Arvion <kohteen>, omaisuuden ja tavoitteiden kuvaukset**
  Ominaisuudet, arvo ja tärkeys
- **Tietoriskien tunnistaminen**
  Puhtaalta pöydältä tai etukäteisskenaarioilla
- **Tietoriskien vaikutuksia**
  a) <kohteelle>, b) sidosryhmille c) organisaatiolle
- **Tietoriskien syitä**
  Toistuva ”Miksi?” juurisyiden löytämiseksi
- **Tietoriskien sietokyky**
  a) <kohteelle> b) asiakkaalle c) organisaatiolle
- **Tietoriskien suuruuden arviointi**
  Todennäköisyys- ja vaikutusluokat, riskikartta ja suhteuttaminen

Esittäjän sovellus

#tuki2018 #stöd2018

- **Tietoriskien omistajat**
  Organisaatiossa henkilö, joka kärsii riskin seurauksista, ja joka päättää mitä riskille tehdään
- **Riskipäätökset**
  Otetaan, seurataan, vältetään, siirretään tai hallitaan
- **Tietoriskien toimenpidesuunnitelmat ja vastuuhenkilöt**
  Syiden vähentäminen ja vaikutuksien rajoittaminen
- **Riskienhallinnan seurannasta ja raportoinnista sopiminen**
- **Riskien jakamisen ja viestinnän suunnittelu**

A. Tiedon arvon ja/tai tavoitteiden tärkeyden kuvaus:

B. Valitse harjoitusriski: *Tietoon ei pääse / Tieto vuotaa / Tieto on virheellistä / Tieto ei jalostu / Tieto ei ole käytettävissä*

C. Kuvaa riskin vaikutuksia

1) **Toiminnalle (välitön operatiivinen)**

2) **Asiakkaalle**

3) **Koko organisaatiolle**

D. Arvioi riskin syitä (alleviivaa juurisyyt)

1) **Ihminen / organisaatio / hallinto**

2) **Prosessi / palvelu**

3) **Teknologia**

E. Sijoita riski karttaan.

Valitse todennäköisyysluokka suhteessa historiaan (onko riski toteutunut aikaisemmin / kuinka usein?) ja olemassa olevien kontrollien tehokkuuteen.

Valitse vaikutuksen luokka suhteessa omaisuuden arvoon tai tavoitteen tärkeyteen.

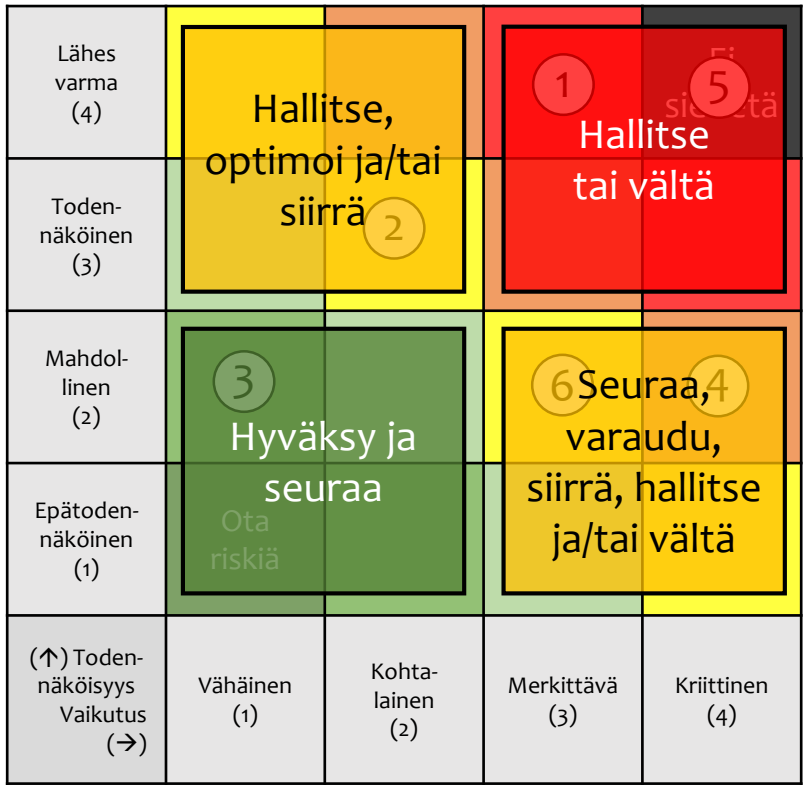
(↑) Todennäköisyys Vaikutus (→)	Vähäinen (1)	Kohtalainen (2)	Merkittävä (3)	Kriittinen (4)
Lähes varma (4)				
Todennäköinen (3)				
Mahdollinen (2)				
Epätodennäköinen (1)				

F. Piirrä karttaan riskinsietokyvyn ja riskinottohalun rajat ja määrittele ne:

Riskipäätökset (esimerkki)

#tuki2018 #stöd2018

1. **Henkilötieto voi olla virheellistä, vanhentunutta tai tuhoutunut**
2. **Henkilötieto ei jalostu joustavasti toiminnan kehityksen mukana**
3. **Tärkeä henkilötieto ei ole saatavilla, kun sitä tarvitsee**
4. **Salassa pidettävä arkaluontoinen henkilötieto vuotaa sivullisille**
5. **Laaja odottamaton katkos tietojärjestelmien käytössä**
6. **Henkilötietoa käytetään väärin**



- **Kriittinen tai ei siedettävissä oleva riski** vaatii välittömiä toimia ja/tai toiminnasta pidättäytymistä.
- **Merkittäville tai nopeasti toimenpiteitä vaativille riskeille** on luotava suunnitelma, jolla sitä hallitaan.
- **Huomioitaville tai seurattaville** riskeille välittömät toimenpiteet eivät ole välttämättömiä, mutta riskiin voidaan varautua ja riskin kehittymistä on seurattava.
- **Ei riskiä tai hyvin matala riski** ei vaadi välittömiä toimenpiteitä.
- **Jäännösriski** on riskin osa, joka on tehtyjen toimenpiteiden jälkeen jäljellä, vaikka riskin vaikutusta tai todennäköisyyttä on pienennetty.
- **Otettavalle riskille** ei tehdä mitään, koska halutaan hyötyä riskin mahdollisuuksista.

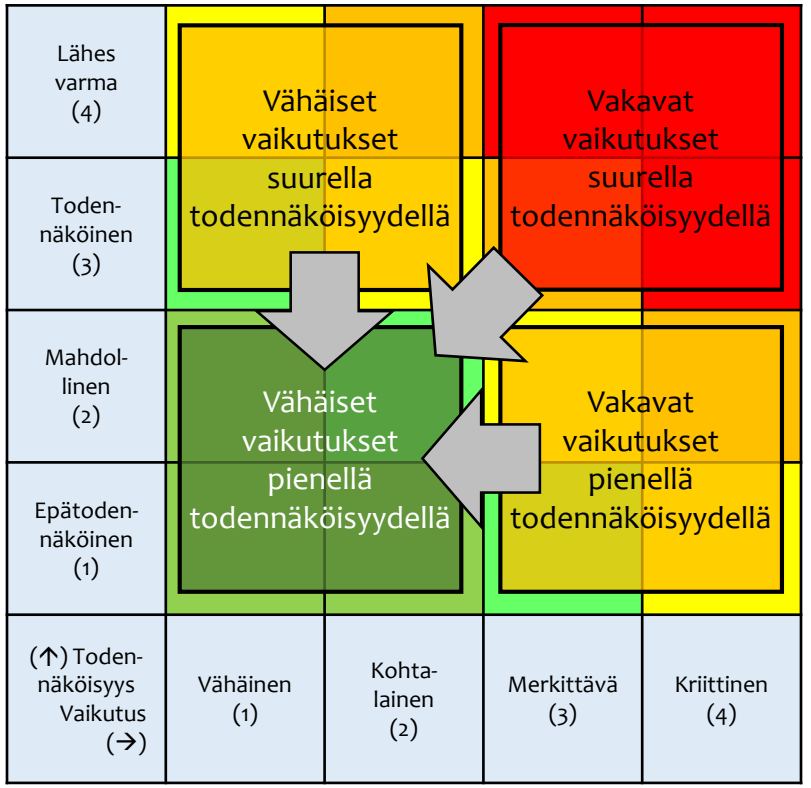
Lomake kohta 6.

Sovellettuja VAHTI 2/2017 riskienhallinnan ohjeesta (kuva 5) ja sen liitteestä (kuva 1.5.3)

Riskien toimenpiteiden vaihtoehdot

#tuki2018 #stöd2018

- **Välttäminen** tai torjuminen pidättäytymällä riskejä aiheuttavasta toiminnasta
- **Hallitseminen**
  - Poistamalla (juuri)syyt tai pienentämällä todennäköisyyttä
  - Varautumalla vaikutuksiin ja/tai rajaamalla vaikutuksia
  - Jakamalla tai siirtämällä kokonaan tai osittain riski toiselle osapuolelle (vakuutus ja ulkoistus)
- **Seuraamalla** riskin suuruuteen vaikuttavia tekijöitä (tilanteen säilyttäminen)
- **Ottamalla** riski (mahdollisuuksien saavuttamiseksi)



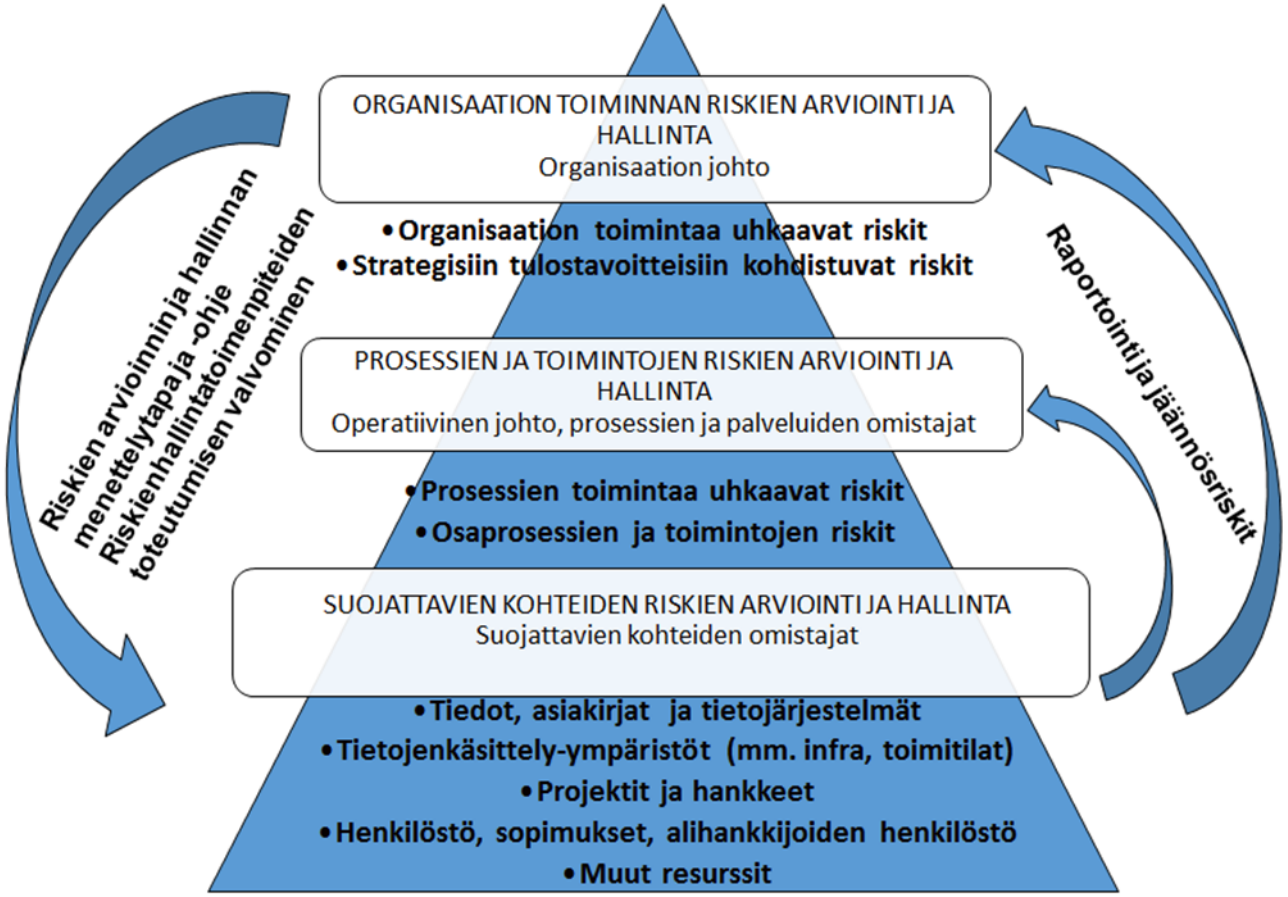
Lomake kohta 6.

Sovellettuja VAHTI 2/2017 riskienhallinnan ohjeesta (kuva 5) ja sen liitteestä (kuva 1.5.3)

Riskienhallinta organisaatiotasoittain

Lomake kohta 7.

#tuki2018 #stöd2018



Kuva L4.4 VAHTI ohjeen liitteen sivulta 18

- Miten saadaan aikaan riskien jakaminen organisaation eri toimintojen välillä?
- Miten huomataan järjestelmällinen riskin toistuminen useissa toiminnoissa?
- Miten saadaan aikaan riskien yhteismitallisuus päätöksiä ja raportointia varten?
- Miten huomataan saman riskin raportointi useiden kanavien kautta?

3. työpajan riskienhallinnan kotitehtävä

#tuki2018 #stöd2018

Riippuen työnkuvastasi ja roolistasi organisaatiossasi sekä organisaatiosi tarpeesta, valitse oikealla olevista kotitehtävistä sopivin ja/tai mielenkiintoisin

Käytä lähteenä VAHTI 22/2017 ohje riskienhallintaan ja työpajojen materiaaleja

1. Tee korkean riskin arviointitaulukko organisaatiosi henkilötietojen käsittelytapauksista (esim. henkilörekisterittäin)
2. Pidä organisaatiosi johtoryhmälle esitys riskilähtöisyydestä tietosuojassa (Miksi? Mitä? Miten?)
3. Tee tietosuojariskiarvio jostain korkean riskin henkilötietojen käsittelyprosessista

Kertaus

#tuki2018 #stöd2018

1. Toimitamme linkin tilaisuuden palautekyselyyn ja materiaaleihin
2. Tee kotitehtävät – varmista että työpajassa käsitellyt asiat etenevät organisaatiossasi
3. Ilmoittaudu seuraavaan työpajaan kun laitamme sinulle linkin
4. Vastaa viikkoa ennen seuraavaa työpajaa toimittamaamme kyselyyn koskien kotitehtävien suorittamista
5. Katso Arjen tietosuoja-videot ja suorita nettitesti – huolehdi, että organisaatiosi huolehtii sen levittämisestä henkilöstölle viimeistään syksyn aikana – sekä kerää tiedot ja varmistaa, että henkilöstö katsoo sen ja suorittaa nettitestin hyväksytysti

Kysymyksiä ja keskustelua

VAHTI 22/2017 ohje riskienhallintaan
- Julkaisusivu
- Ohje riskienhallintaan
- Liitteet
- Riskienhallintatyökalu
  - Excel - perusversio
  - Excel - laajempi versio
  - Ohje työkaluun

#tuki2018 #stöd2018

Kuntaliitto Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintäteknikkakeskus

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto

pauli.wihuri@kpmg.fi
+358 60 62344

Lisäkalvot keskustelun perusteella →