Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet

#tuki2018 #stöd2018

Työpaja #3 – 4.9.2017

- Tietoturvallisuuden toteuttaminen organisaation toiminnassa – mitä asetus edellyttää, ja miten vaatimukset käytännössä toteutetaan
- **Riskienhallinta osa 3, riskien hallinta ja toimenpiteiden seuranta sekä arviointityöpajojen toteuttaminen**

Kuntaliitto Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintätekniikkakeskus

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto

Tilaisuuden ohjelma

#tuki2018 #stöd2018

- 8.30 Kahvi
- 9.00 Tilaisuuden avaus – Tuula Seppo, Kuntaliitto & Kimmo Rousku, valtiovarainministeriö
- 9.15 Mikä on tarvittava tietoturvallisuuden vähimmäistaso?
- 10.10 Bio- ja jaloittelutauko
- 10.30 Työpaja jatkuu: Tietoturvallisuuden toteuttaminen organisaation toiminnassa – mitä asetus edellyttää ja miten vaatimukset käytännössä toteutetaan
- 12.00 Lounastauko (omakustanne)
- **13.00 Riskienhallinta osa 3, riskien hallinta ja toimenpiteiden seuranta sekä arviointityöpajojen toteuttaminen**
- 14.30 Kahvitauko
- **14.45 Työpaja jatkuu**
- **16.00 Yhteenveto ja kotitehtävä**
- 16.15 Työpaja päättyy

Riskienhallinta osa 3
Työpajan sisältö

#tuki2018 #stöd2018

Riskienhallinnan ohjaus, periaatteet ja viitekehys

Riskiarviointityöpajan toteuttaminen

Riskipäätökset, toimenpiteet ja seuranta

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

Riskienhallinnan periaatteet, viitekehys ja prosessi

#tuki2018 #stöd2018

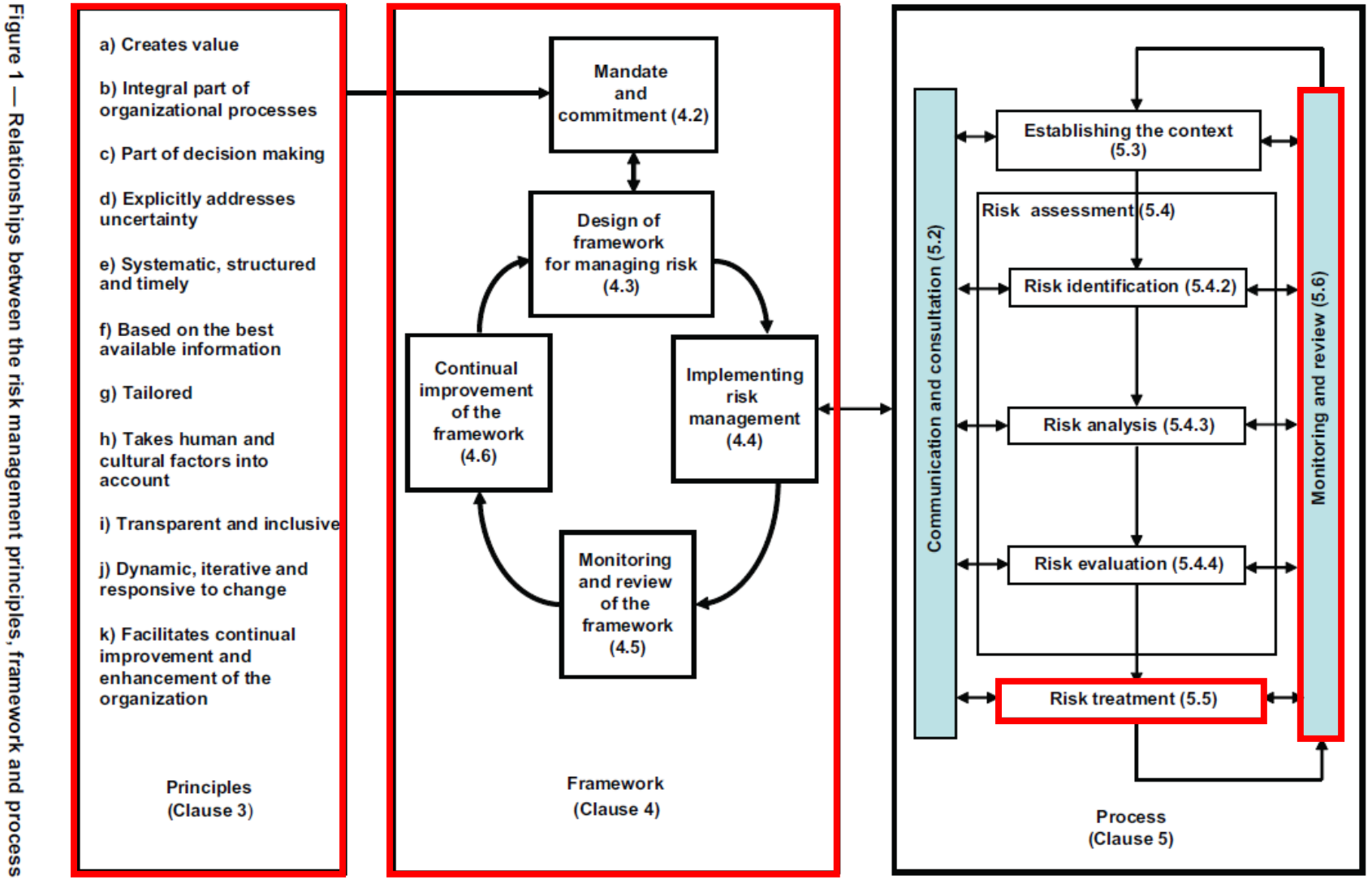


Figure 1 — Relationships between the risk management principles, framework and process

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

ISO 31000 kuva sivulta vii

Riskienhallinnan 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 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"

Vastuut, valtuutus ja sitouttaminen

Organisaation ylin johto on tilivelvollinen organisaation riskeistä ja riskienhallinnan järjestämisestä organisaatiossa. **Organisaation toimiva johto** on tilivelvollinen oman vastuualueensa riskeistä. **Organisaation riskienhallinnan kyvykkyydestä vastaava johtaja** on tilivelvollinen riskienhallinnan toimintamallin ja hallintaprosessin tuottavuudesta ja soveltuvuudesta organisaatioon (ei vastaa riskeistä).

#tuki2018 #stöd2018

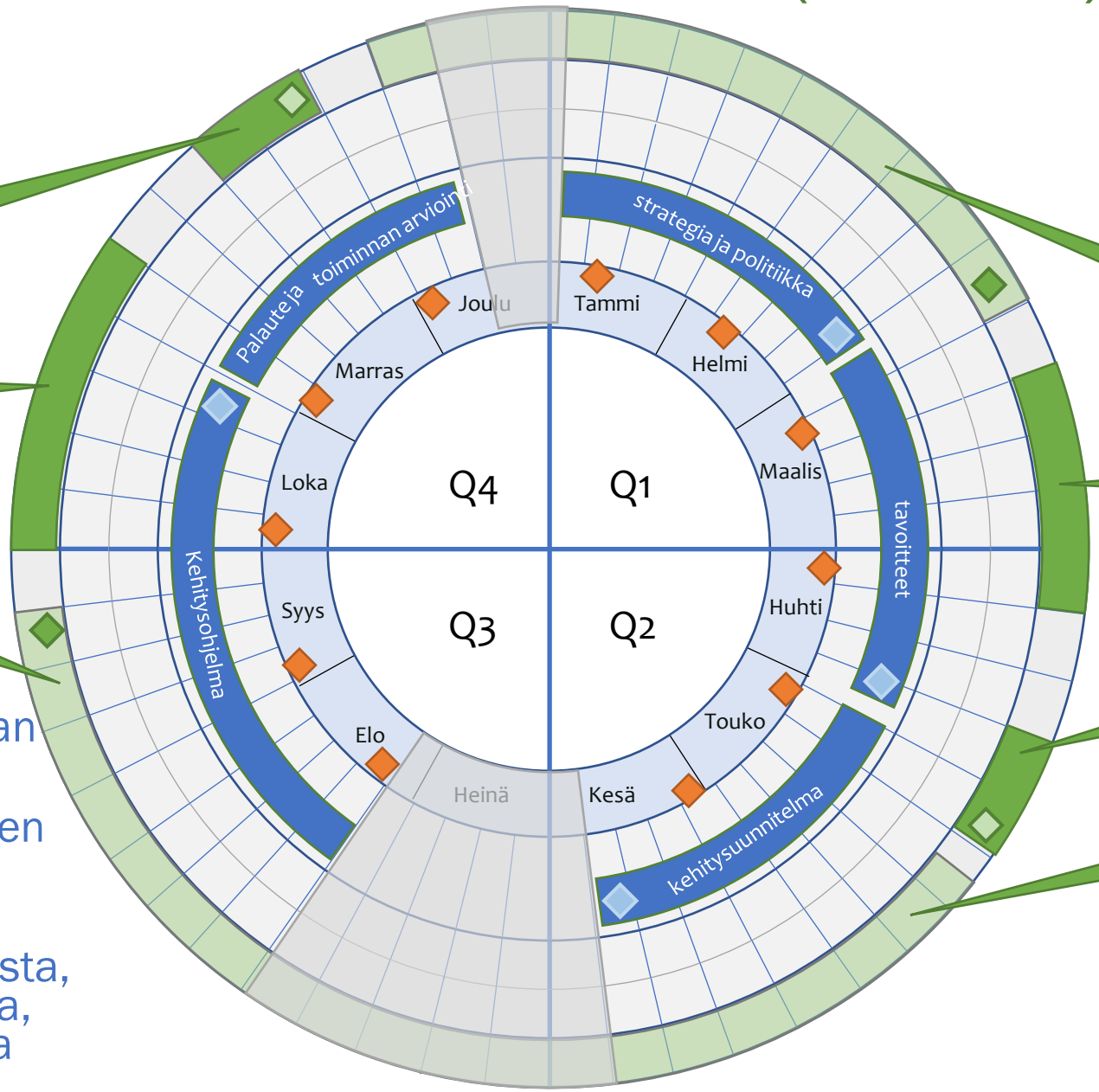
Hallinnan taso	Tehtävät	ARCI	Rooli
Riskienhallinnan toimintamalli (Governance)	Toimintamallin, politiikan, ohjeistuksen ja prosessin kehittäminen, suunnittelu, toteuttaminen, seuranta ja raportointi.	A	Organisaation ylin johto
		R	Organisaation riskienhallinnan kyvykkyydestä vastaava (riskienhallintajohtaja/-päällikkö)
		C	Organisaation johtoryhmä ja riskienhallinnan asiantuntijat
		I	Organisaatio
Riskien hallintaprosessi (Operations)	Organisaation riskien hallinta eli organisaation omaisuuden ja toiminnan riskien kartoitus, analysointi, päätökset, toimenpiteet ja raportointi.	A	Organisaation johtajat/päälliköt kukin omalla vastuualueellaan
		R	Organisaation ydintoimintojen päälliköt/vastaavat
		C	Ydintoimintojen henkilöstö ja riskienhallinnan asiantuntijat
		I	Koko organisaation / muiden ydintoimintojen päälliköt/vastaavat

Sovellettu VAHTI ohjeen liitteen taulukkoa sivulta 19

Lomake kohta 3.

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)

Riskienhallinnan vuosikellon tehtävät (esimerkki)

#tuki2018 #stöd2018

VAHTI

1.2.3 Organisaatiossa tehdään säännöllisesti tietoturvallisuuteen liittyvien riskien arviointia. Riskien arvioinnin perusteella parannetaan tietoturvallisuutta liian suurten riskien osalta johdon päättämillä toimenpiteillä.

2.4.1 Organisaatiolla on periaatteet, jotka kertovat, millaiset päivitykset tai muutokset asennetaan välittömästi ja millaisiin päivityksiin ja muutoksiin käytetään riskitason huomioon ottavaa tarveharkintaa.

2.13.1 Järjestelmään kohdistetaan riskianalyysi, jolla pyritään löytämään tietoturvavaatimukset tarjouspyyntöön, vaatimusmäärittelyyn tai uuden version asennuksen projektisuunnitelmaan.

1.2.3 Riskiarvioinnit ja –raportti (kk 3-5 ja 10-12)

Riskienhallintapäällikkö johtaa riskien arviointikierrokset yhdessä riskienhallinnan vastuuhenkilöiden kanssa kahdesti vuodessa organisaation suunnitteluprosessin tahdissa ja laatii johdon raportin riskeistä toimenpiteiden päättämiseksi

2.13 Jatkuva riskien hallinta

Johdon päättämiä tietoriskien toimenpiteitä edistetään yksiköiden päälliköiden toimesta.

Asiakasvastaavat koordinoivat toimialojen riskien hallintaa ja palveluvastaavat edistävät riskien toimenpiteitä.

Projektipäälliköt arvioivat projektin riskit kustannushyötyanalyysissa, suunnittelevat riskien toimenpiteet osaksi projektisuunnitelmaa ja edistävät toimenpiteitä projektin edetessä.

Riskienhallinnan vastuuhenkilöt tukevat organisaation riskienhallintaa.

Toimintaympäristön riskiavaruuden luokittelu

Lomake kohta 4.

Organisaation tulee valita riskien luokittelu organisaation toimintaympäristön luonteen mukaisesti

Strategiset riskit	Operatiiviset riskit
Pitkällä tähtäimellä menetyksiin tai mahdollisuuksien menettämiseen johtavat riskit. Esim. Väärät valinnat.	Päivittäisen toiminnan prosessien toimimattomuudesta tai ihmisten toiminnassa epäonnistuminen aiheuttaa välittömän vaikutuksen päivittäiseen toimintaan. Esim.
Taloudelliset riskit	**Vahinkoriskit**
Omaisuuden tai talouden hallinnassa epäonnistuminen aiheuttaa pääoman ja/tai omaisuuden menetyksen. Esim. Kavallus.	Vaaran tai vahingon toteutuessa menetetty inhimillinen menetys tai omaisuuden tuhoutuminen. Esim. Vesivahinko tai tulipalo.

Sovellettu riskien luokittelu VAHTI ohjeen liitteen sivulta 25

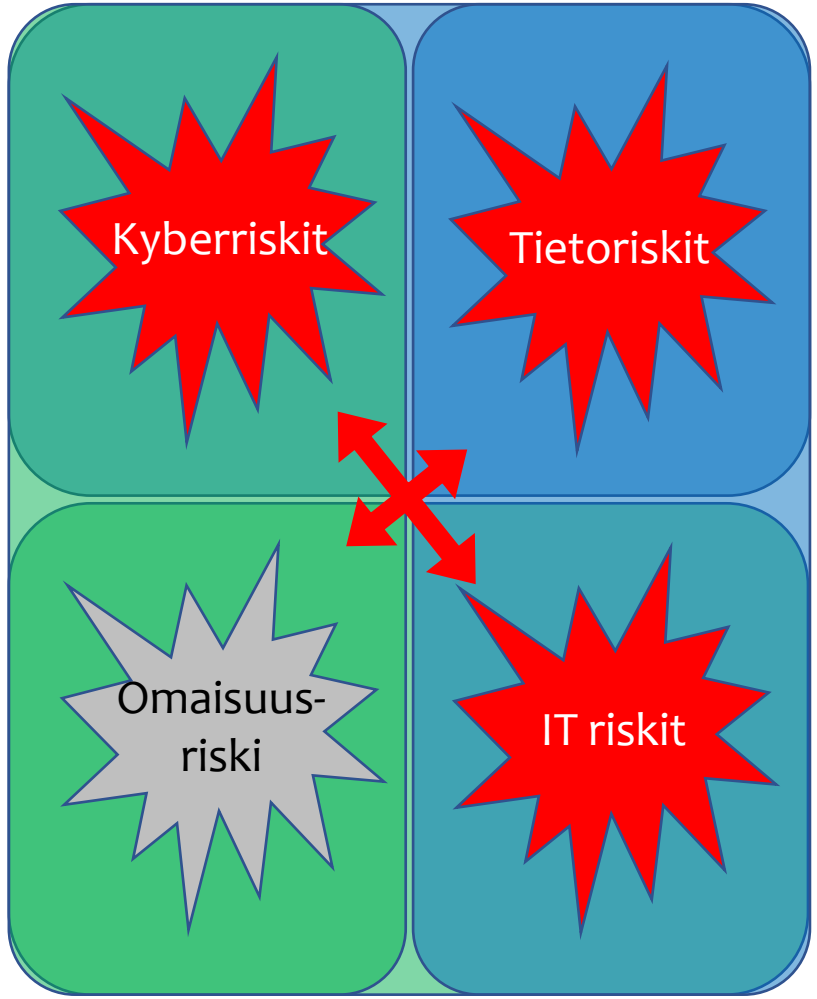
Muita mahdollisia luokkia organisaation toiminnan luonteen mukaisesti:
Asiakasriskit, henkilöriskit, johtamisriskit, toimintariskit, suunnitteluriskit, tietoriskit, IT riskit, teknologiariskit, sääntelyriskit, ympäristöriskit, turvallisuusriskit, tietoturvariskit, tietosuojariskit, sisäiset riskit, ulkoiset riskit, toimittajariskit, sopimusriskit, luottoriskit, maineriskit, ..

Riskiavaruuden luokat tulee valita koko organisaatiolle luontevasti, ymmärrettävästi ja tasapainossa, jotta riskien jakaminen ja viestintä helpottuisi ja hallinta tehostuisi.

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.



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?

Organisaation tietoriskien kartoituksen suunnittelu

#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

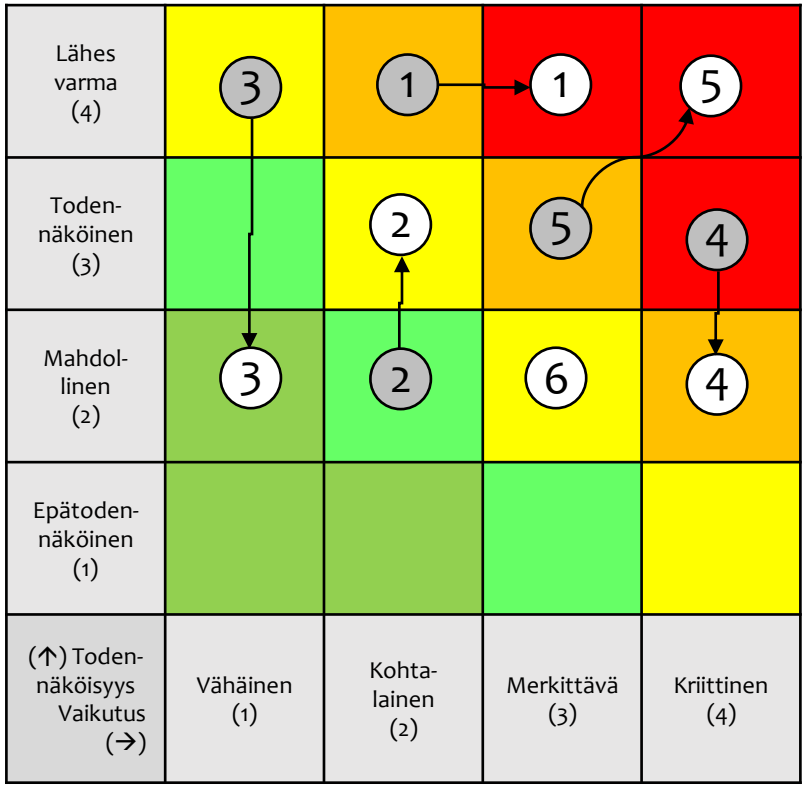
- **Tietoriskien omistajat**
  Organisaatiossa henkilö, joka kärsii riskin seurauksista, ja joka päättää mitä riskille tehdään
- **Riskipäätökset**
  Otetaan, seurataan, vältetään, siirretään tai hallitaan
- **Tietoriskien toimenpidesuunnitelmat ja vastuuhenkilöt**
  Syiden vähentäminen ja vaikutuksien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

Riskipäätökset (esimerkki)

Mitä riskipäätöksiä tekisit tällaisen riskikartan perusteella?

#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**



Lomake kohta 6.

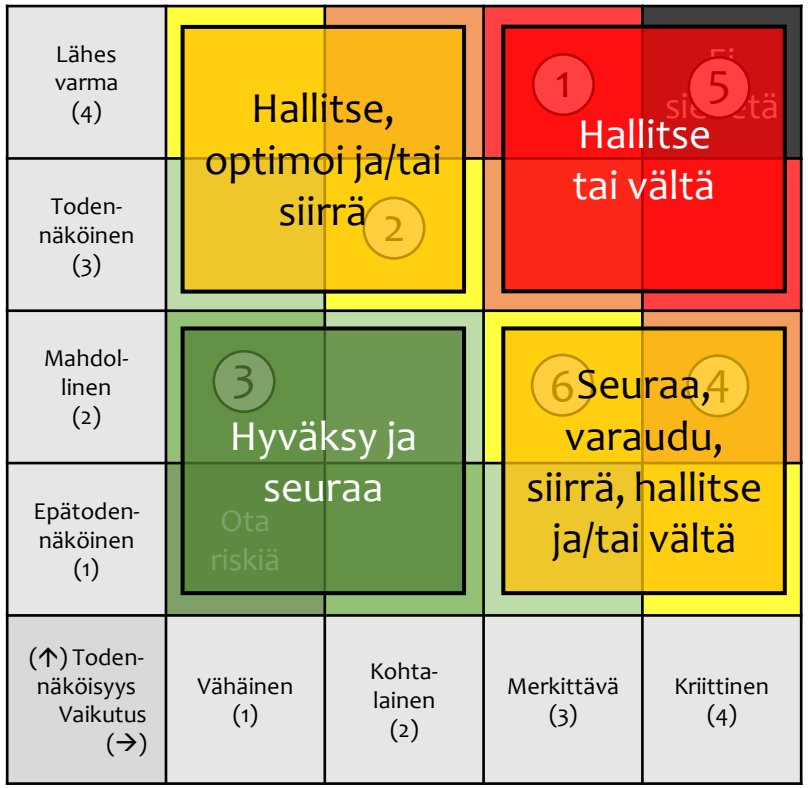
Kenen pitää/kuka saa päättää riskeistä?

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

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.

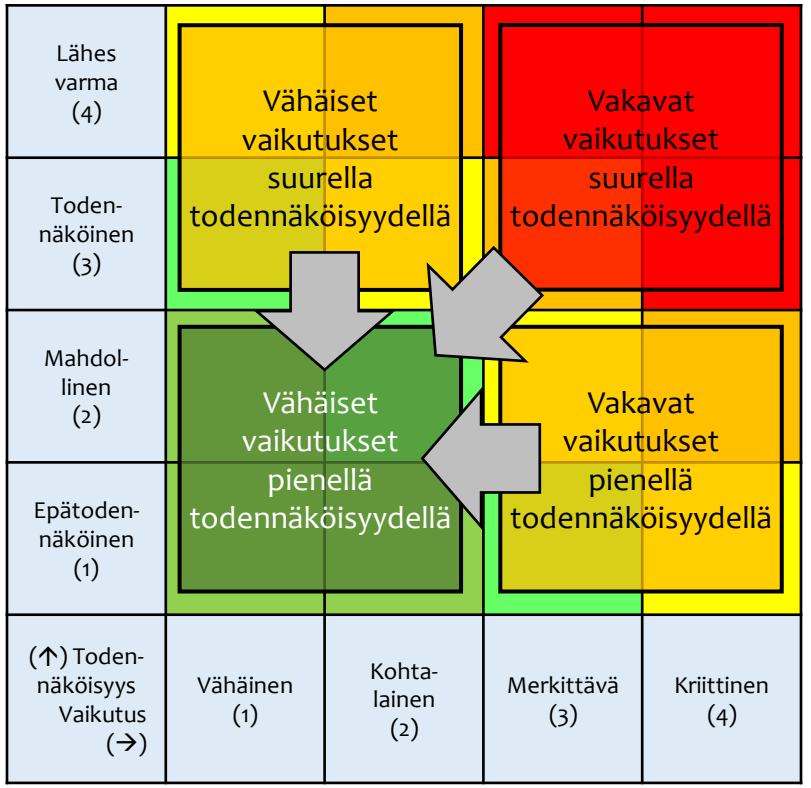
Lomake kohta 6.

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)



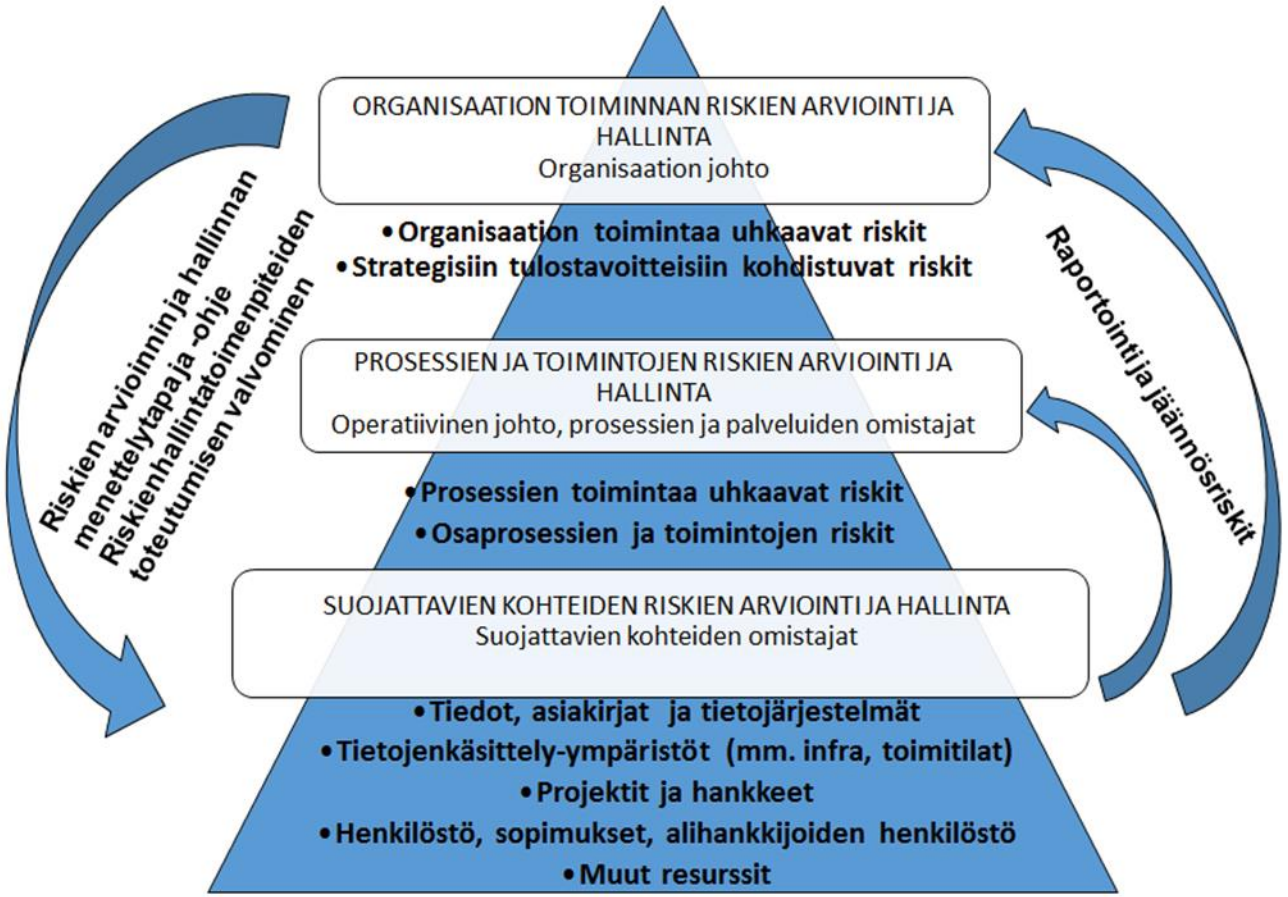
Lomake kohta 6.

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?

Ryhmätyö

#tuki2018 #stöd2018

Keskusteluaiheet

a) Miten vastuut riskeistä ja riskienhallinnan järjestämisestä tulee selkeästi kuvata ja jalkauttaa organisaatiossa?

b) Mitkä tekijät vaikuttavat riskienhallinnan saamiseksi osaksi organisaation ydintoimintoja?

c) Mitkä ovat julkishallinnon suurimmat tämän hetken riskit ?

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.

3. työpajan riskienhallinnan kotitehtävä

#tuki2018 #stöd2018

Riippuen työnkuvastasi ja roolistasi organisaatiossasi sekä organisaatiosi tarpeesta, valitse oikealla olevista kotitehtävistä 1-3 sopivin ja/tai mielenkiintoisin

Käytä lähteenä VAHTI 22/2017 ohje riskienhallintaan ja työpajojen materiaaleja

1. Laadi suunnitelma organisaatiosi riskienhallinnan kehittämiseksi tärkeimpien riskienhallinnan periaatteiden toteutumiseksi
2. Laadi suunnitelma ja toteuta tietoriskien arvioinnin työpaja organisaatiosi tärkeimpään kohteeseen
3. Täytä työpajan lomakkeen kohdan 6 sisältö oikealle suurimmalle riskille omalla vastuualueellasi. Voit käyttää toisessa työpajassa (18. elokuuta) arviomaasi riskiä ja keskittyä pohtimaan riskin toimenpiteitä.

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 viestintätekniikkakeskus

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto

pauli.wihuri@kpmg.fi
+358 60 62344

Lisäkalvot keskustelun perusteella →

Tiedon ja luulon miinakenttä

#tuki2018 #stöd2018

Tiedon ja luulon miinakenttä		Luulemme, että.. (↓)	
		..on riskitön	**..ei ole riskitön**
Tiedämme, että.. (→)	**..on riskitön**	Optimaalinen tilanne, kun tietää riskeistä ja suojauksista. Pitää panostaa palvelun laatuun ja helppokäyttöisyyteen, jotta käytettäisiin. (Esim. suojattu sähköposti)	Kun ei tiedetä tai uskota suojauksiin, ei käytetä. Menetetään mahdollisuus tuottavuuden kasvuun, kun ei käytetä hyödyllistä palvelua. (esim. pilvitoimisto)
	..ei ole riskitön	Ei ymmärretä arvioida riskejä ja suojautua vaikka pitäisi. Seurauksena ongelmia ja häiriöitä eli turhia kustannuksia. (Esim. sisäverkko)	Huomataan olla varovaisia ja pohtia riskejä etukäteen. Päätetään jättää käyttämättä tai suojautua, jotta voisi käyttää. (Esim. Internet)