#tuki2018 #stöd2018

Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet

Työpaja #1 – 12.6.2017

- **Tietosuoja-asetuksen osoitusvelvollisuus**
- **Riskienhallinta**

Kuntaliitto Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintätekniikkakeskus

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto

#tuki2018 #stöd2018

Tilaisuuden ohjelma

- 8.30 Kahvi
- 9.00 Tilaisuuden avaus – Tuula Seppo, Kuntaliitto & Kimmo Rousku, valtiovarainministeriö
- 9.30 KPMG:n työpajoista vastaavat konsultit esittäytyvät
- Tietosuoja-asetuksen osoitusvelvollisuus
- 10.30 Bio- ja jaloittelutauko
- 10.40 Työpaja jatkuu
- 12.15 Lounastauko (oma kustanne)
- 13.00 Tietosuojavaltuutettu Reijo Aarnion tervehdys
- 13.15 Riskienhallinta-osuus käynnistyy
- 14.30 Kahvitauko
- 14.45 Työpaja jatkuu
- 16.00 Yhteenveto – mitä ja miten organisaation tulisi työpajassa läpikäytyjä asioita omassa organisaatiossa edistää?
- 16.15 Työpaja päättyy

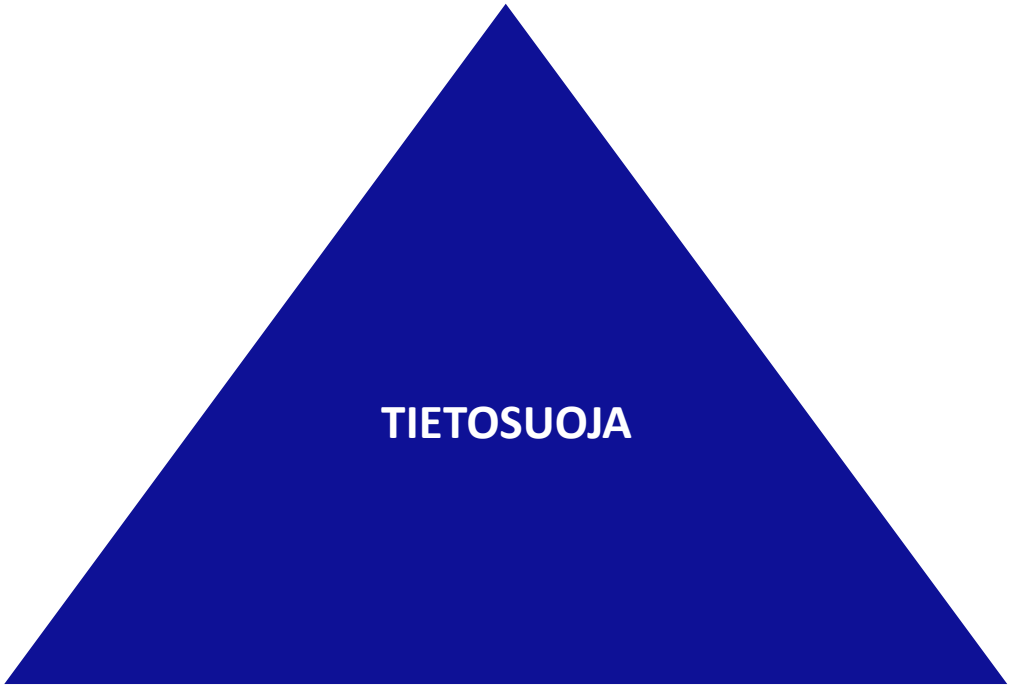
#tuki2018 #stöd2018

Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet

Tietosuojan perusteet

#tuki2018 #stöd2018

Tietosuoja – mitä se vaatii?



#tuki2018 #stöd2018

Tietosuoja vs. tietoturva

Tietosuojalainsäädäntö

#tuki2018 #stöd2018

- Henkilötietodirektiivi (95/46/EY)

→ Henkilötietolaki (523/1999)

- Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY)

→ Tietoyhteiskuntakaari (917/2014)

- Tulossa:
  - **EU:n yleinen tietosuoja-asetus (”GDPR”) ((EU) 2016/679)**
  - **Kansallinen ”tietosuojalaki”**
  - Tietosuojadirektiivi (EU)2016/680 (kansallinen sääntely puuttuu)
  - Tiedonhallintalaki ja se sisällä tietoturva-asetuksen korvaava lainsäädäntö
  - ePrivacy -asetus (luonnos)
- Huomioitava: Julkisuuslaki (621/1999), tietohallintolaki (634/2011)
- Alakohtaista erityissääntelyä, mm.
  - Laki yksityisyydensuojasta työelämässä (759/2004)
  - Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)

#tuki2018 #stöd2018

Tietosuojan peruskäsitteitä

- Henkilötieto
- Erityiset henkilötietoryhmät
- Rekisteröity
- Henkilötietojen käsittely
- Rekisterinpitäjä vs. henkilötietojen käsittelijä
- Asiakastieto vs. henkilöstöä koskeva tieto
- Järjestelmät vs. tietovarannot vs. henkilörekisterit (”looginen rekisteri”)
- ”In-house”-järjestelmät vs. ulkoistetut järjestelmät
- EU/ETA vs. non-EU/ETA

Osoitusvelvollisuus ja sen ulottuvuudet

Osoitusvelvollisuuden määritelmä

#tuki2018 #stöd2018

Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tietosuoja-asetusta. (24 art.)

Tarkemmin: Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että henkilötiedon käsittelyä koskevia periaatteita (art. 5) on noudatettu.

#tuki2018 #stöd2018

Tiedon elinkaaren hallinta – henkilötietojen käsittelyn periaatteet (5 art.)

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

- Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi;

Käyttötarkoitussidonnaisuus

- Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteen sopimattomalla tavalla;

#tuki2018 #stöd2018

Tiedon elinkaaren hallinta – henkilötietojen käsittelyn periaatteet (5 art.)

Tietojen minimointi

- Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään;

Täsmällisyys

- Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä;

#tuki2018 #stöd2018

Tiedon elinkaaren hallinta – henkilötietojen käsittelyn periaatteet (5 art.)

Säilytyksen rajoittaminen

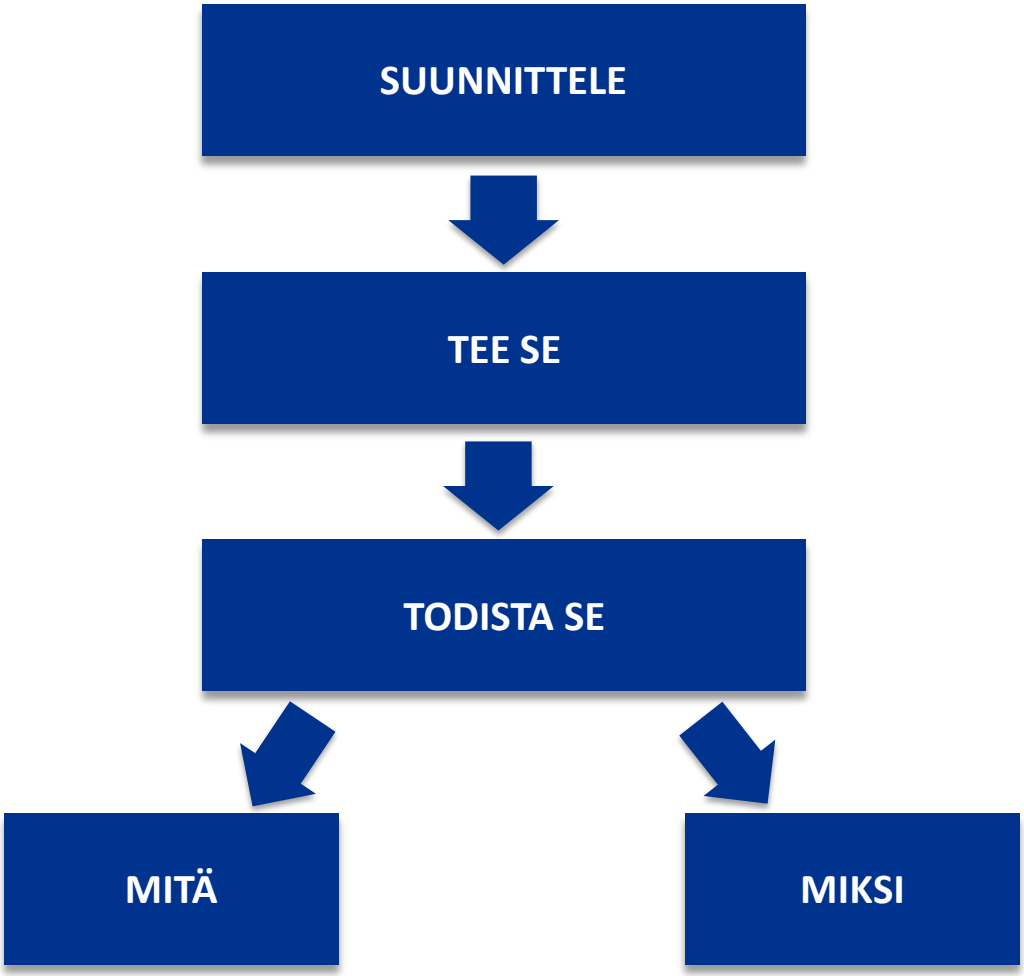
- Henkilötietoja on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten;

Eheys ja luottamuksellisuus

- Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia.

#tuki2018 #stöd2018

Osoitusvelvollisuus käytännössä



#tuki2018 #stöd2018

Osoitusvelvollisuus käytännössä

#tuki2018 #stöd2018

Riskilähtöisyys

- Osa asetuksen vaatimuksista jää melko yleiselle tasolle, jättäen tulkinnanvaraa esimerkiksi tietoturvan tason määrittelemisessä.
- Rekisterinpitäjän vastuulle jää viime kädessä päättää esim. tiedon suojaamiseen käytettävien kontrollien järeydestä ja arvioida niiden riittävyys.

→ Vaatii tulkintaa mutta tuo myös joustavuutta

- Valittavien kontrollien sekä resurssien käytön tulee perustua mm.
  - riskiarvioon,
  - käsiteltävien henkilötietojen luonteeseen,
  - käytettävissä oleviin resursseihin, sekä
  - teknologian tasoon päätöksentekohetkellä.
- Osoitusvelvollisuus täydentää asetuksen vaatimuksia, mitoittaa kontrolleja ja ohjaa toimimaan riskilähtöisesti.
- Päätösten ja niiden perusteiden dokumentointi on osa osoitusvelvollisuuden toteuttamista.

Case: Pilvipalvelu

Hankinnan tietosuoja- ja tietoturvaratkaisuihin vaikuttavat mm.

- siirrettävän tiedon arkaluonteisuus
- tietoon kohdistuvat uhat
- tietomassan kokoluokka
- tietojen sijainti
- palveluntoimittajan rooli tietojenkäsittelyssä
- alihankintaketju

#tuki2018 #stöd2018

Ryhmätehtävä

- Jaetaan osallistujat n. 10 hengen ryhmiin.
- Tehtävä: **Mitkä osoitusvelvollisuuden osa-alueet tulevat vaatimaan organisaatiossasi eniten kehitystyötä?**
- Aikaa: 10 min

Tietosuojan hallinnointi

#tuki2018 #stöd2018

- Rekisterinpitäjän tietosuojavelvollisuudet koskettavat kaikkia organisaation käsittelemiä henkilötietoja, olipa kyseessä yksityishenkilöiden, yhteistyökumppaneiden, asiakkaiden tai organisaation henkilöstön tiedot.
- Jotta tietosuojasta voidaan huolehtia organisaation laajuisesti huomioiden kaikki käsiteltävät tiedot, tulee tietosuojan hallinnointi vastuuttaa organisaatiossa sekä varata riittävästi resursseja koko organisaation tietosuojatehtävien toteuttamiseen.

Tietosuojan hallinnointiin kuuluu mm.

Johdon tuki
Vastuiden ja raportointiketjujen määrittely
Tietosuojavastaava/tietosuojaorganisaatio
Politiikat ja ohjeistukset sekä niiden jalkautus
Riskienhallinta
Sopimusten ja alihankkijoiden hallinta
Henkilöstön koulutus
Valvonta ja seuranta
Vuosikello
Jatkuva kehittäminen
Auditoinnit ja sertifioinnit

#tuki2018 #stöd2018

Politiikat ja dokumentointivelvoite

Tietosuoja-periaatteet	Seloste henkilötietojen käsittelytoimista	Rekisteriselosteet / tietosuojaselosteet
Sopimukset	Henkilötietojen käsittelyn ohjeistus henkilöstölle sekä tietojenkäsittelijöille	Prosessien, analyysien ja toimenpiteiden dokumentointi
Riskienhallinta-periaatteet	Tietoturvapolitiikka	Käyttövaltuus- ja pääsynhallinta-periaatteet

#tuki2018 #stöd2018

Politiikat ja dokumentointivelvoite

Tietotilinpäätös	Alihankkijoiden valintaa ohjaavat periaatteet	Prosessikuvaukset rekisteröidyn oikeuksien toteuttamiseksi
Kuvaus tietovirroista	Tiedon luokittelun periaatteet	Prosessikuvaus tietoturvaloukkausten ilmoittamiseksi
Lokituksen periaatteet	Tiedon varmistus-periaatteet	Tietosuojan vuosikello

#tuki2018 #stöd2018

Riskienhallinnasta yleisesti

- Rekisterinpitäjä ja henkilötietojen käsittelijä ovat velvollisia arvioimaan henkilötietojen käsittelyyn liittyviä riskejä ja valitsemaan arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet.
- Tietosuojariskien hallinta on syytä liittää osaksi organisaation riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka.
- Jos tietosuojavastaava on nimetty, hänen tulee tukea organisaation eri yksiköitä, jotta tietosuojariskejä tunnistettaisiin paremmin sekä olla mukana määrittelemässä tunnistetuille, hallintaan otettaville riskeille tarvittavia hallintakeinoja.

Riskiprofiiliin vaikuttavia tekijöitä ovat mm.

- Henkilötietojen arkaluonteisuus
- Henkilötietojen lukumäärä
- Käyttäjien lukumäärä
- Järjestelmän luonne (web-applikaatiot ym.)
- Tietojenkäsittelyn ulkoistuksen luonne
- Rekisteröidyn oikeudet
- Resurssien kohdentaminen
- Henkilöstön osaaminen

#tuki2018 #stöd2018

Tietosuojan vaikutustenarviointi (”DPIA”/”PIA”) (35 art.)

- Suoritettava koskien sellaisia henkilötietojen käsittelytoimia, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä.
- Tietosuojavastaava osallistettava.
- Tuloksia tulee käyttää niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään riskitasoa, sekä varmistumaan asetuksen vaatimusten toteutumisesta.
- Jos vaikutustenarvioinnin perusteella riskitaso on suuri, eikä rekisterinpitäjä pysty sitä pienentämään, on otettava yhteyttä valvontaviranomaiseen (”ennakkokuuleminen”).
- Valvontaviranomainen tulee julkaisemaan luettelon käsittelytoimista, jotka vaativat vaikutustenarvioinnin laatimisen.

Vaikutustenarviointi mahdollisesti suoritettava mm. seuraavissa:

- Profilointi ja pisteyttäminen
- Automatisoitu päätöksenteko
- Järjestelmällinen seuranta
- Arkaluonteisten tietojen käsittely
- Suurten tietomassojen käsittely
- Heikossa asemassa olevien henkilötietojen käsittely (mm. lapset)
- Edistykselliset tietojenkäsittelytavat
- Henkilötietojen siirto EU:n/ETA:n ulkopuolelle
- Yleisölle avoimen alueen järjestelmällinen valvonta laajamittaisesti

Lähde: Art. 29 WP 248

#tuki2018 #stöd2018

Henkilötietoinventaario

- Tärkeänä osana nykytila-analyysia tulee selvittää organisaation keräämien ja käsittelemien henkilötietojen kokonaiskuva.
- Tiedot palvelevat suoraan osoitusvelvollisuuden täyttämistä sekä avustavat yleisesti rekisterinpitäjän velvollisuuksien täyttämisessä.
- Ks. myös osio ”tietotilinpäätös”.

Kartoitettava:

- Käsiteltävät henkilötietovarannot (→ henkilörekisterit)
- Henkilötietoluokat
- Henkilötietojen käsittelyperusteet
- Henkilötietojen säilytysajat
- Henkilötietovirrat
- Henkilötietojen käsittelyyn käytetyt järjestelmät
- Henkilötietojen maantieteellinen sijainti
- Palveluntoimittajat

#tuki2018 #stöd2018

Sisäänrakennettu ja oletusarvoinen tietosuoja (”Privacy by Design” ja ”Privacy by Default”) (25 art.)

Tietosuojan sekä tietoturvan huomiointi ja sisäänrakentaminen prosessien sekä järjestelmien suunnittelussa

- ✓ Henkilötiedon keruun ja käsittelyn minimointi
- ✓ Käyttäjäpiirin tehokas rajaaminen (käyttövaltuudet ja pääsynvalvonta)
- ✓ Säilytysaikojen määrittely ja vanhentuneen tiedon poistaminen
- ✓ Pseudonymisointi
- ✓ Anonymisointi
- ✓ Tiedon salaaminen (kryptaus)
- ✓ Tietoturva
- ✓ Rekisteröidyn oikeuksien toteuttaminen
- ✓ Käyttäjäystävälliset asetukset
- ✓ Tietosuojavastaavan rooli
- ✓ Vaikutustenarvioinnit

#tuki2018 #stöd2018

Tietosuojavastaavan nimittäminen (37 art.)

- Asetus velvoittaa viranomaiset ja julkishallinnon elimet (pl. tuomioistuimet) nimeämään tietosuojavastaavan.
- Tietosuojavastaavan nimeäminen on ollut vaatimuksena nykysääntelyssäkin esimerkiksi terveydenhuollon alalla.
- Yksi tietosuojavastaava voidaan nimittää useampaa viranomaista tai julkishallinnon elintä varten.
- Pätevyysvaatimukset:
  - tietosuojalainsäädännön tuntemus,
  - lain vaatimusten soveltamisosaaminen,
  - alan käytäntöjen tuntemus, sekä
  - valmiudet suorittaa 39 artiklassa tarkoitetut tehtävät.

#tuki2018 #stöd2018

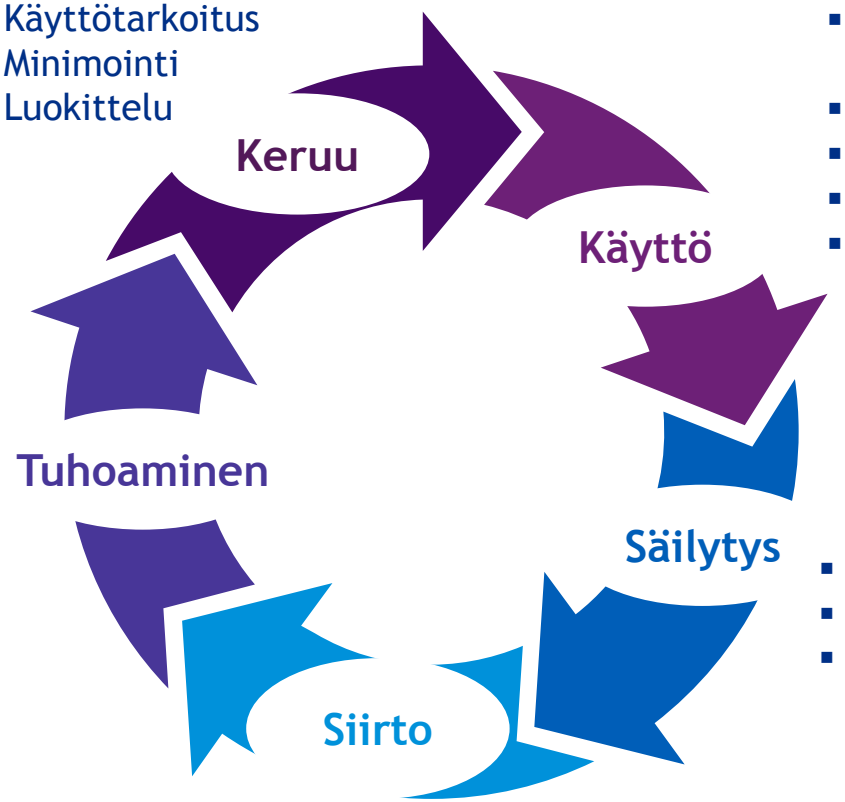
Tietosuojavastaavan asema (38 art.)

- Riippumaton asema organisaatiossa
- Ei kokonaisvastuuta tietosuojan toteutumisesta organisaatiossa
- Raportoi suoraan rekisterinpitäjän tai käsittelijän ylimmälle johdolle
- Otetaan asianmukaisesti ja riittävän ajoissa mukaan kaikkiin tietosuojaan liittyviin kysymyksiin
- Salassapitovelvollisuus
- Ei saa erottaa tai rangaista tietosuojavastaavan tehtävien hoitamisen vuoksi
- Voi suorittaa muitakin tehtäviä tietosuojavastaavan tehtävien ohella kuitenkin niin, ettei niistä aiheudu eturistiriitoja.

#tuki2018 #stöd2018

Tiedon elinkaari

- Oikeudellinen peruste
- Käyttötarkoitus
- Minimointi
- Luokittelu



- Käyttötarkoitus-sidonnaisuus
- Tarpeellisuus
- Tiedon laatu
- Jalostaminen
- Käyttäjienhallinta

- Säilytysajat
- Turvallisuus
- Siivousoperaatiot

- Pseudonymisointi
- Anonymisointi
- Tiedon salaaminen

- Siirtoperusteet
- Sopimukset
- Tiedonsiirtojen turvallisuus

Tietoturvallisuus – mitä asetus vaatii? (32 art.)

- Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten

  a) henkilötietojen pseudonymisointi ja salaus;

  b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;

  c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;

  d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

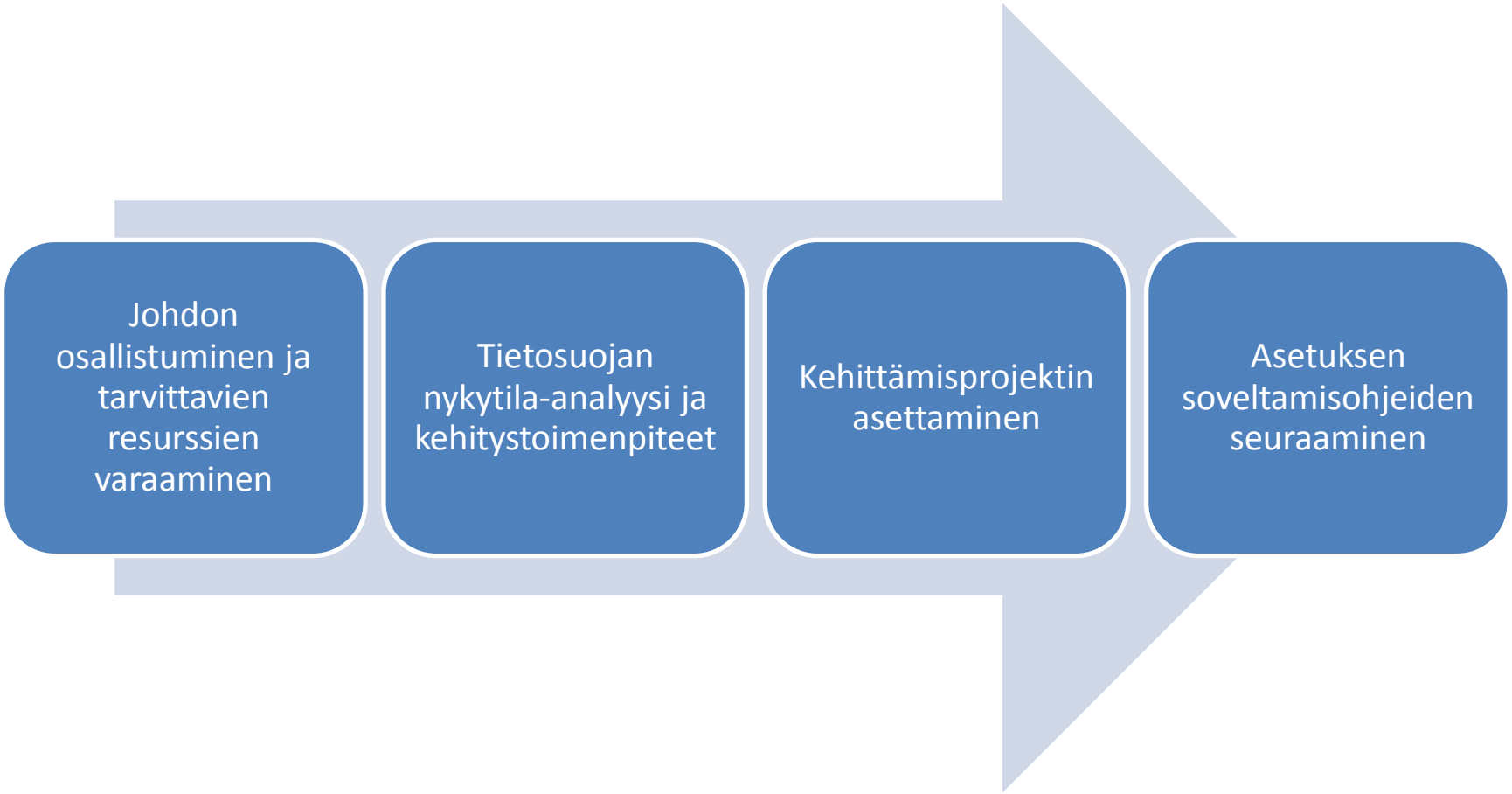
Tietoturvallisuuden elementtejä

- Riskianalyysit
- Turva-arkkitehtuuri
- Tietojärjestelmien hankinta, kehitys ja ylläpito
- Pääsynhallinta
- Omaisuuden ja tiedon hallinta
- Päivitysten ja muutosten hallinta
- Fyysinen turvallisuus
- Henkilöstöturvallisuus
- Toimittajien ja sopimusten hallinta
- Toiminnan jatkuvuuden hallinta
- Käsittelyn valvonta ja seuranta
- Tietoturvallisuuden hallinta

Sopimuskumppania ja sopimusta koskevat vaatimukset (mm. 28 art.)

- Rekisterinpitäjän velvollisuuksiin kuuluu valita vain sellaisia henkilötietojen käsittelijöitä, jotka
  - noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla; sekä
  - täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta.
- Rekisterinpitäjän ja henkilötietojen käsittelijän välillä on oltava kirjallinen sopimus.
- Sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto, sopia käsiteltävät henkilötiedot sekä tietojenkäsittelijälle asetettavat muut vaatimukset.
- Rekisterinpitäjän tulee varmistaa, että henkilötietojen siirroille (fyysinen lokaatio/pääsy tietoihin) EU:n/ETA:n ulkopuolelle on riittävät siirtoperusteet.

Arviointi ja kehittäminen – GDPR kehityshanke



Kriittisiä teemoja tietosuojan kehittämisessä

- Riskien arviointi
- Tietosuojan hallinnointi ja politiikkojen luonti / jalkautus
- Rekisterinpidon perusedellytysten varmistaminen
- Henkilötietojen ja tietovirtojen kartoittaminen
- Prosessit ja tiedon elinkaaren hallinta
- Sopimukset: Alihankinta ja henkilötietojen luovutukset
- Rekisteröityjen oikeuksien toteuttaminen
- Tietosuoja-asetuksen vaatimukset ICT:lle ja sen hallinnoinnille
- Valvonta ja tietoturva

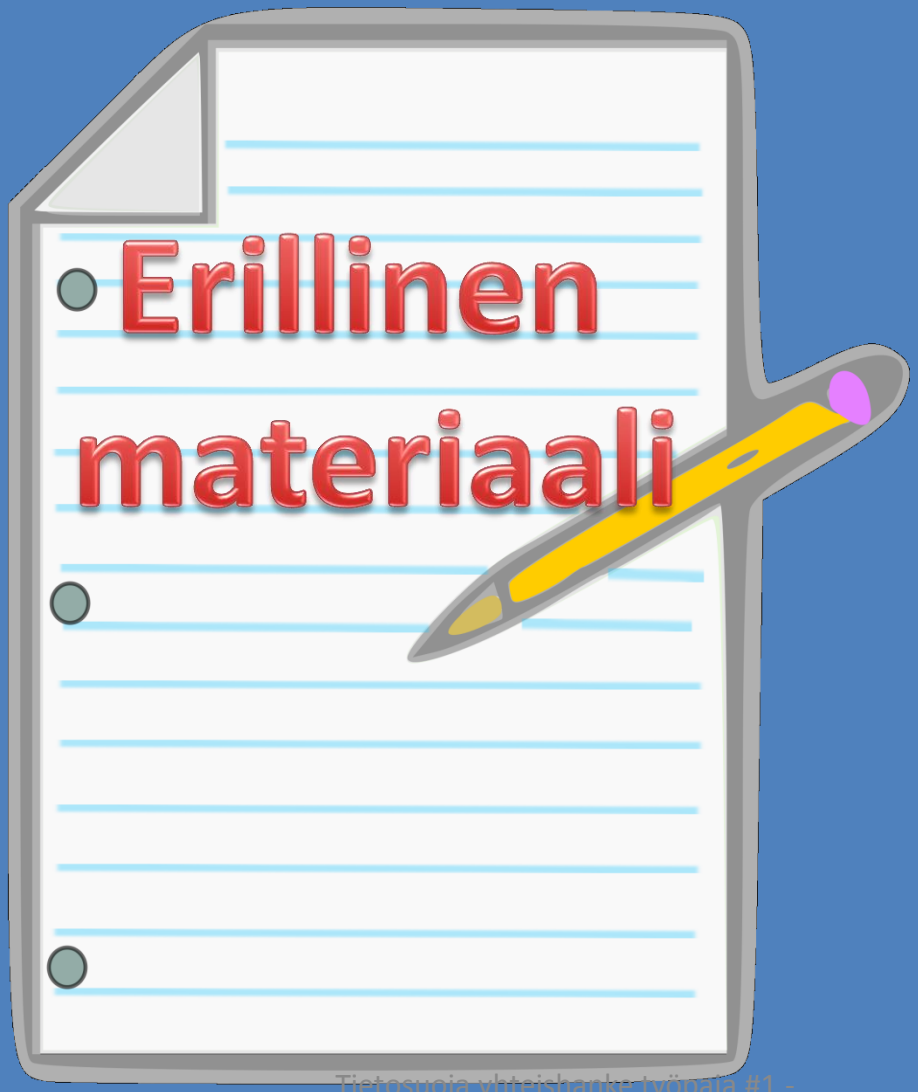
Seuranta ja raportointi

- Johdon tietoisuus organisaation tietosuojan nykytilasta on tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.
- Säännöllisen raportoinnin tulee sisältää tärkeimmät tietosuojaan ja henkilötietojen käsittelyyn liittyvät asiat.
- Niitä voivat olla esimerkiksi
  - tietosuojamittarit sisältäen niiden käytön raportointikauden aikana,
  - tietosuojan kehityshankkeet ja niiden tilanne,
  - havaitut puutteet ja tarpeet,
  - merkittävimmät tietoturvaloukkaukset, joilla on ollut tietosuojavaikutuksia,
  - tehdyt riski- ja vaikutustenarvioinnit sekä niiden merkittävimmät löydökset hallintakeinoineen sekä
  - rekisteröityjen oikeuksiin ja yhteistyöhön valvontaviranomaisen kanssa liittyvät tarpeelliset tiedot.
- Johdon vuosiraportti voi olla esimerkiksi tietotilinpäätös.

Tietotilinpäätös

- Tietotilinpäätös antaa kokonaiskuvan organisaation henkilötietojen käsittelyn ja tietosuojan nykytilasta.
- Sen avulla johto voi valvoa ja arvioida nykytilaa sekä ohjata resursseja sen kehittämiseen.
- Tietotilinpäätöksestä ja sen laatimisesta löytyy lisätietoja tietosuojavaltuutetun sivuilla: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf

Kotitehtävä 12.6.2017



Hyödyllisiä linkkejä

Hyödyllisiä linkkejä

EU:n yleinen tietosuoja-asetus

VAHTI-raportti 1/2016: EU-tietosuojan kokonaisuudistus

Tietosuojavaltuutetun opas tietosuoja-asetukseen valmistautumiseen

Kuntaliiton ohje: Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja

WP29:

WP29 guidelines on the Data Protection Officer requirement in the GDPR

WP29 guidelines on the right to data portability in the GDPR

The WP29 Guidelines on the Lead Supervisory Authority

Riskienhallinta – yleinen osa

Riskienhallinnan lähtökohtia

Riskienhallinnan lähtökohtia

Ymmärtääkseen nykypäivän tarkastusvaliokunnan haasteita, KPMG Audit Committee Institute toteutti tutkimuksen, johon osallistui yli 800 tarkastusvaliokunnan jäsentä ympäri maailmaa.

Tutkimuksen päähavainnot – Riskienhallinta on yksi organisaation hallituksen pääprioriteeteista

Risk management is a top concern for audit committees.	Internal audit can maximize its value to the organization by focusing on key areas of risk and the adequacy of the company's risk management processes generally.	Tone at the top, culture, and short-termism are major challenges—and may need more attention.
CFO succession planning and bench strength in the finance organization continue to be weak spots.	Two key financial reporting issues may need a more prominent place on audit committee agendas: Implementation of new accounting standards and non-GAAP financial measures.	Audit committee effectiveness hinges on understanding the business.

Lähde: 2017 Global Audit Committee Pulse Survey, KPMG

Riskienhallinnan lähtökohtia

Riskienhallintaa, taloudellista raportointia, vaatimusten mukaisuutta ja sisäistä valvontaa testataan myös vuonna 2017 hitaan ja epävarman taloudellisen kasvun, teknologian kehittymisen, kyberriskien, regulaation tarkemman tarkastelun ja investoijien kasvavien läpinäkyvyysvaatimusten sekä poliittisten muutosten vuoksi. Ohessa on seitsemän teemaa, joita tutkimuksen tulosten mukaan tarkastusvaliokuntien tulee huomioida työssään.

Tutkimuksen päähavainnot – Riskienhallinta on yksi organisaation hallituksen pääprioriteeteista

Give non-GAAP financial measures a prominent place on the audit committee agenda.

Monitor implementation plans and activities for major accounting changes on the horizon—particularly the new revenue recognition and lease accounting standards.

Redouble the company's focus on ethics, compliance, and culture.

Focus internal audit on key areas of risk and the adequacy of the company's risk management *processes* generally.

Monitor key regulatory initiatives to enhance transparency of the audit process.

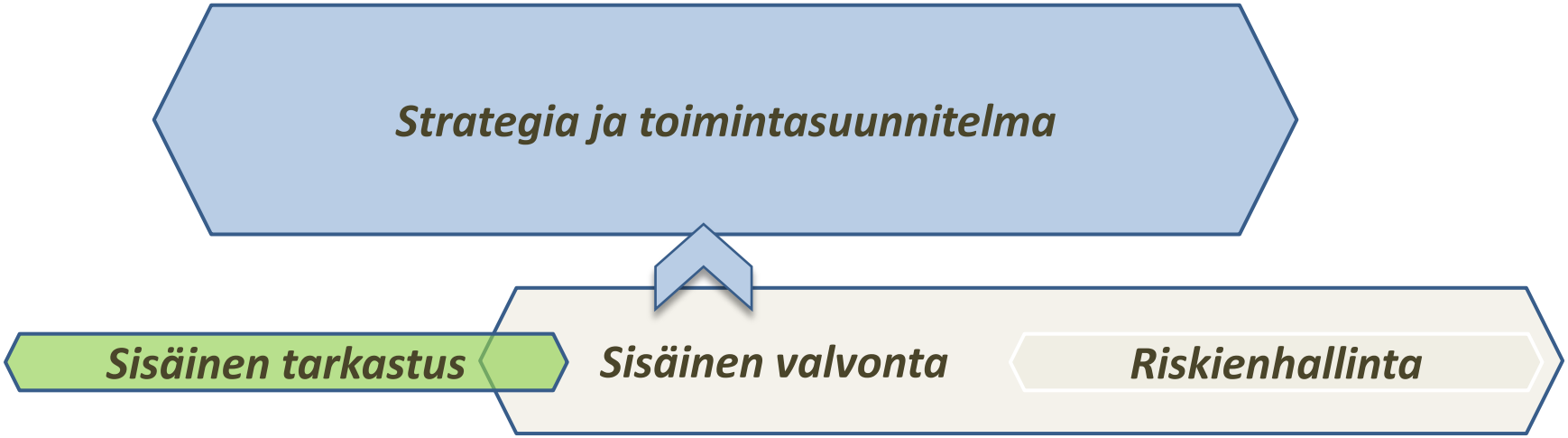
Quality financial reporting starts with the CFO and finance organization; maintain a sharp focus on leadership and bench strength.

Make the most of the audit committee's time together—inside and outside the boardroom.

Lähde: 2017 Global Audit Committee Pulse Survey, KPMG

Riskienhallinnan perusteet

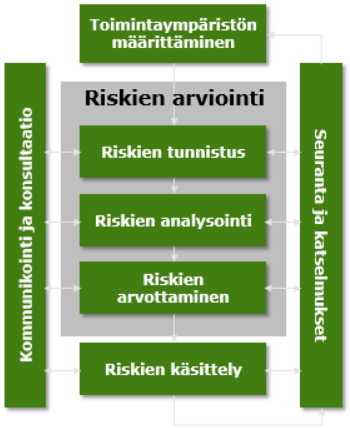
Riskienhallinta ja GRC

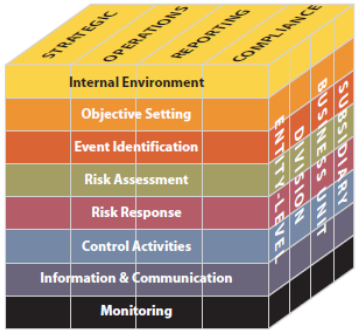


Riskienhallinta koostuu riskien johtamisen ja hallinnan koordinoiduista toimenpiteistä. Se tukee organisaation strategiaa ja toimintasuunnitelmia auttaen organisaatiota saavuttamaan asettamansa tavoitteet ja tekemään hallittuja päätöksiä. Riskienhallinnan perusta määritellään yleisesti organisaation riskienhallintapolitiikkaan, joka ohjaa riskienhallinnan toteuttamista.

Riskienhallinnan määritelmä

- Riskienhallinta on joukko prosesseja ja toimenpiteitä organisaation liiketoiminnassaan kohtaamien riskien tunnistamiseksi, analysoimiseksi, arvioimiseksi ja vähentämiseksi
- Tehokas riskienhallinta tukee organisaatiota vähentämään riskiä kriittisillä liiketoiminnan alueilla ja varmistaa, että tunnistetut liiketoimintamahdollisuudet hyödynnetään organisaation suorituskyvyn parantamiseksi
- Luodakseen arvoa, riskienhallinnan tulee olla systemaattista, jatkuvaa, kokonaisvaltaista sekä proaktiivista





ISO 31000 ja COSO ERM riskienhallinnan viitekehykset.

Riskienhallinnan määritelmät johtavissa riskienhallinnan viitekehyksissä:

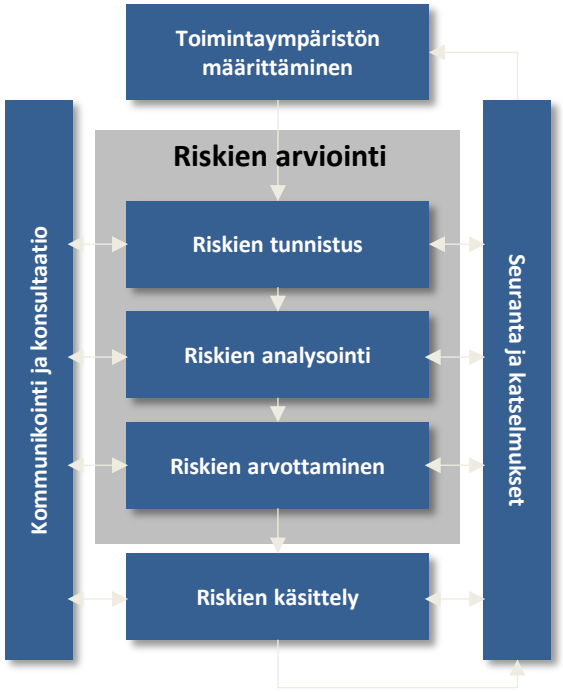
"Risk management consists of coordinated activities to direct and control an organization with regard to risk"

Lähde: *ISO 31000 – Risk management - Principles and guidelines, 2009, definition of risk management*

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"

Lähde: Committee of Sponsoring Organization of the Treadway Committee (COSO), Enterprise Risk Management – Integrated Framework

ISO 31000 -viitekehys

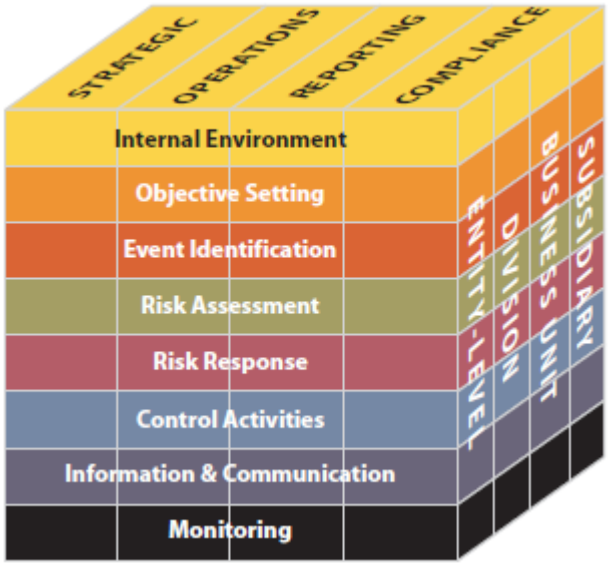


ISO 31000 riskienhallinnan prosessi.

ISO 31000 pääelementit:

- ISO 31000 on ensimmäisen kerran vuonna 2009 International Standard Organizationin julkaisema riskienhallinnan viitekehys. ISO 31000 on riskienhallinnan ammattilaisten suosima ja laajalti käytetty standardi. Ensimmäistä versiota ollaan paraikaa päivittämässä ja uusin versio tullaan todennäköisesti julkaisemaan viimeistään alkuvuodesta 2018.
- ISO 31000 standardi koostuu riskienhallinnan periaatteiden määrittämisestä ja riskienhallinnan kehikosta sekä ylätason riskienhallinnan prosessista (kuvattu vasemmalla)
- ISO 31000 standardi keskittyy määrittelemään mitä riskienhallinta on ja mitä organisaation tulee sisällyttää riskienhallinnan kehikkoon ja prosesseihin
- ISO 31000 standardi keskittyy siihen, mitä riskienhallinnassa tulisi tehdä, ei niinkään miten riskienhallinta toteutetaan

COSO ERM -viitekehys

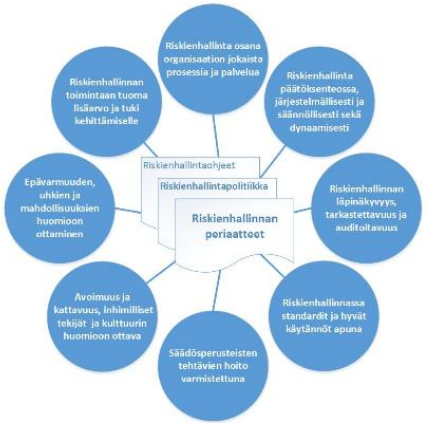


COSO ERM riskienhallinnan viitekehyksen elementit.

COSO ERM pääelementit:

- COSO ERM on Commission of Sponsoring Organization of the Treadway Commissionin (COSO) vuonna 2004 julkaisema riskienhallinnan viitekehys. COSO ERM on laajalti käytetty riskienhallinnan viitekehys, jota on hyödynnetty toimialasta riippumatta määrittelemään organisaation riskienhallinnan kehystä
- COSO ERM on COSO:n sisäisen valvonnan viitekehyksestä erillinen, riskienhallintaan keskittyvä viitekehys. Viitekehyksen tavoitteena on tarjota organisaatioille pääperiaatteet, yhteisen kielen sekä selkeät suuntaviivat riskienhallinnalle
- COSO riskienhallinnan viitekehys keskittyy integroimaan riskienhallinnan osaksi organisaation johtamisprosesseja. Lisäksi viitekehys painottaa organisaation strategian ja tavoitteiden saavuttamisen edistämistä riskienhallinnan avulla

Riskienhallinnan lähtökohdat julkishallinnon organisaatioissa



Kuvankaappauksia VAHTI-ohjeesta.

Kokonaisvaltainen riskienhallinta

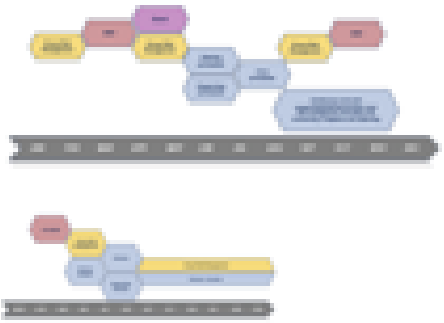
- **Vaatimukset riskienhallinnan järjestämiselle julkishallinnossa**
- **Miten riskienhallintapolitiikka toimii riskienhallinnan ohjauksessa?**
- **Riskienhallinta osana johtamista**
- **Riskienhallinta toiminnan kehittämisen ja kehittämistoimenpiteiden seurannan tukena**
- **Riskienhallinta sisäisen tarkastuksen tukena**

Riskienhallinnan organisointi

Riskienhallinnan roolit ja resursointi

- **Riskienhallintafunktio ja sen toimenkuva**
- **Vastuu riskienhallinnasta johdolla**
- **Riskienhallinnan osaaminen organisaatiossa**
- **Riskikulttuuri ja riskiajattelun jalkauttaminen koko organisaatioon**

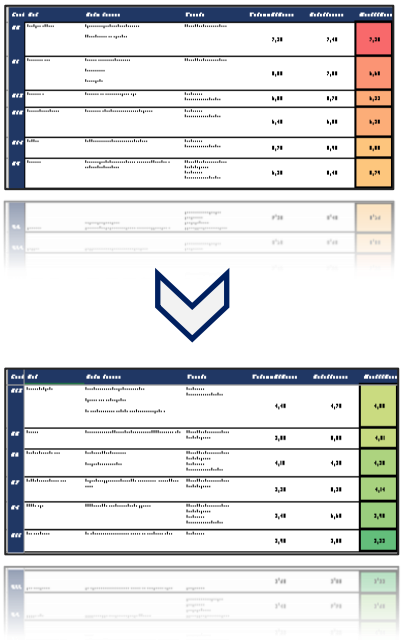
Kokonaisvaltaiset riskienhallinnan prosessin rajapinnat



Riskienhallinnan rajapinnat

- **Rajapinnat esim. Compliance-, Kyber-, Ympäristö-, Laatu- tai Tietosuojariskien kanssa avainasemassa kokonaisvaltaisen riskienhallinnan prosessia määritellessä**
- **Yhteistyö ydintoiminnan ja tukiyksiköiden välillä**
- **Yhteistyö eri tukiyksiköiden välillä**

Riskienhallintatoimenpiteiden integrointi osaksi toiminnan johtamista



Integrointi osaksi johtamista

- **Lähtee toiminnan suunnitteluprosessista**
- **Toimenpiteiden määrittely ja seuranta avainasemassa**
- **Mahdollinen keskittyminen vain avainriskeihin**
- **Johdon raportointi sekä riskiraportointi**

Esimerkkejä riskeistä

Esimerkkejä organisaatioiden riskeistä, riskienhallintatoimenpiteistä ja riskienhallinnan työkaluista

Riskienhallinnan työkalut

- **Riskirekisteri**
- **Muita riskienhallinnan työkaluja, kuten työpajoissa hyödynnettävät äänestyslaitteistot**
- **Erilaiset riskienhallintaa tukevat analyysit ja mallinnukset (esim. Monte Carlo)**
- **Riskienhallinnan järjestelmät**

Esimerkkejä organisaatioiden riskeistä, riskienhallintatoimenpiteistä ja riskienhallinnan työkaluista
Esimerkkiriski 1

	Riskilaji	Riski	Riskin kuvaus	Riskin merkittävyys Asteikko: 1-9	Riskin trendi	Hallintakeino, aikataulu ja hallintakeinon vastuuhenkilö	Hallinta-keinon tila
Riski 1	Strateginen	Prosessikuvausten puute	Organisaation pääprosesseja ei ole tunnistettu. Prosessikuvauksia ei ole tai ne eivät ole ajan tasalla. Kuvausten puute voi johtaa esimerkiksi: -Epäselvyyksiin vastuualueissa, aiheuttaen virheitä päivittäisessä työssä -Päällekkäiseen työhön -Toiminnan jatkuvuuden vaarantumiseen poikkeuksellisissa tilanteissa	8,0	→	Järjestetään johdon työpaja, jossa pääprosessit tunnistetaan ja prosessien tahtotila selkeytetään. Työpajan tuloksien perusteella pääprosessit sekä kriittiset alaprosessit kuvataan. Prosessikuvauksen lopputuotteena syntyy uimaratakaaviotyyliset prosessikaaviot ja tarvittavat työohjeet. Aikataulu: Marraskuu 2015 mennessä Vastuuhenkilö: Matti Meikäläinen, toimitusjohtaja	

Esimerkkejä organisaatioiden riskeistä, riskienhallintatoimenpiteistä ja riskienhallinnan työkaluista
Esimerkkiriski 2

	Riskilaji	*Riski*	*Riskin kuvaus*	*Riskin merkittävyys Asteikko: 1-9*	*Riskin trendi*	*Hallintakeino, aikataulu ja hallintakeinon vastuuhenkilö*	*Hallinta-keinon tila*
Riski 2	Taloudellinen	Talousraportointi	Organisaation sisäinen talousraportointi ei tue johdon päätöksentekoa. Raporttien sisältö, esitystapa ja/tai ulkoasu ei palvele päätöksentekoa. Riski voi johtaa esimerkiksi: -Epäoptimaalisiin päätöksiin -Virheelliseen ulkoiseen raportointiin -Organisaation tehottomaan suoriutumiseen	**7,0**	-	Arvioidaan talousraportoinnin nykytila, ja kartoitetaan määriteltyjen tahojen tarpeet talousraportointiin liittyen. Kartoituksen pohjalta suunnitellaan tarvittavat toimenpiteet, jotka esitetään johtoryhmälle 1.12.2015. Aikataulu: 1.12.2015 mennessä Omistaja: Matti Meikäläinen, talousjohtaja	

Esimerkkejä organisaatioiden riskeistä, riskienhallintatoimenpiteistä ja riskienhallinnan työkaluista
Esimerkkiriski 3

	Riskilaji	*Riski*	*Riskin kuvaus*	*Riskin merkittävyys Asteikko: 1-9*	*Riskin trendi*	*Hallintakeino, aikataulu ja hallintakeinon vastuuhenkilö*	*Hallinta-keinon tila*
Riski 3	Tietoturva	Tietoturvaosaaminen	Organisaation henkilökunnan tietoturvaosaaminen ei ole riittävän hyvällä tasolla. Puutteet osaamisessa voivat johtaa esimerkiksi: -Tietojen menetyksiin vahingon seurauksena -Tahallisina tietomurtoina -Organisaation resursseja hyödyntävinä väärinkäytöksinä	2,0		Järjestetään tietoturvakoulutuksia koko organisaation henkilökunnalle. Sisällytetään tietoturvakoulutus uusien henkilöiden perehdyttämiseen. Aikataulu: Marraskuu 2015 mennessä Omistaja: Matti Meikäläinen, IT-johtaja	

Esimerkkejä organisaatioiden riskeistä, riskienhallintatoimenpiteistä ja riskienhallinnan työkaluista
Esimerkkiriski 4

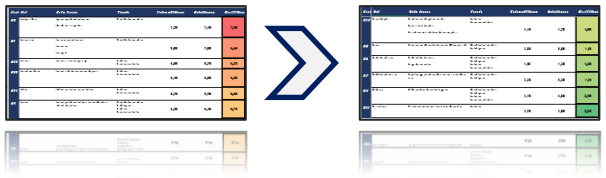
	Riskilaji	*Riski*	*Riskin kuvaus*	*Riskin merkittävyys Asteikko: 1-9*	*Riskin trendi*	*Hallintakeino, aikataulu ja hallintakeinon vastuuhenkilö*	*Hallinta-keinon tila*
Riski 4	Hyvä hallinto	Riskienhallintaprosessi	Organisaation riskiprofiilia ei päivitetä eikä uusia riskejä tunnisteta säännöllisesti. Organisaation riskienhallintatoimenpiteitä ei ole vastuutettu. Puutteet riskienhallinnassa voivat johtaa esimerkiksi: -Riskien tunnistamatta jäämiseen -Tilanteeseen, että riskienhallintatoimenpiteiden toimeenpanoa ei seurata aktiivisesti	**6,0**	-	Määritellään riskienhallinnan vuosisuunnitelma, joka myötäilee organisaation vuosikelloa ja aikataulutuksellaan tukee esim. strategiaprosessia. Käydään organisaation riskirekisteri läpi ja määritellään jokaiselle riskille omistaja. Riskin omistaja on ensisijaisesti johtajatasolla oleva henkilö. Aikataulu: Marraskuu 2015 mennessä Omistaja: Matti Meikäläinen, toimitusjohtaja	

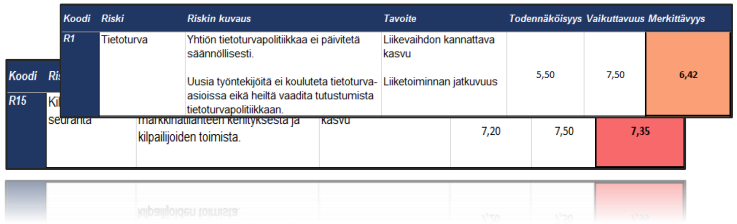
Esimerkkejä organisaatioiden riskeistä, riskienhallintatoimenpiteistä ja riskienhallinnan työkaluista
Esimerkkiriski 5

	Riskilaji	*Riski*	*Riskin kuvaus*	*Riskin merkittävyys Asteikko: 1-9*	*Riskin trendi*	*Hallintakeino, aikataulu ja hallintakeinon vastuuhenkilö*	*Hallinta-keinon tila*
Riski 5	Hallinto	Avainhenkilöriski	Organisaation avainhenkilö tai avainhenkilöitä lähtee palveluksesta, vaarantaen organisaation häiriöttömän toiminnan.	7,4		Tarkistetaan, että organisaation jokaisella henkilöllä on tarvittavat varahenkilöjärjestelyt. Lisäksi tarkistetaan, että organisaation pääprosessien kaikista työvaiheista on riittävät kuvaukset ja niihin on ajan tasalla olevat työohjeet. Aikataulu: Joulukuu 2015 mennessä Omistaja: Matti Meikäläinen, hallintojohtaja	

Esimerkkiriskien tunnistaminen

Ryhmätyö - esimerkkiriskien tunnistaminen





Organisaation TOP 3 riskit

- **Tunnista organisaatioon kohdistuvat merkittävimmät Top 3 -riskit**
- **Riski on tapahtuma, jolla voi olla negatiivinen ja/tai positiivinen vaikutus organisaation tavoitteiden saavuttamiseen**
- **Dokumentoi riski konkreettisesti ja määrittele sille alustava hallintatoimenpide, jolla hallitaan riskin todennäköisyyttä tai vaikutusta**

Riskienhallinnan kypsyystasot

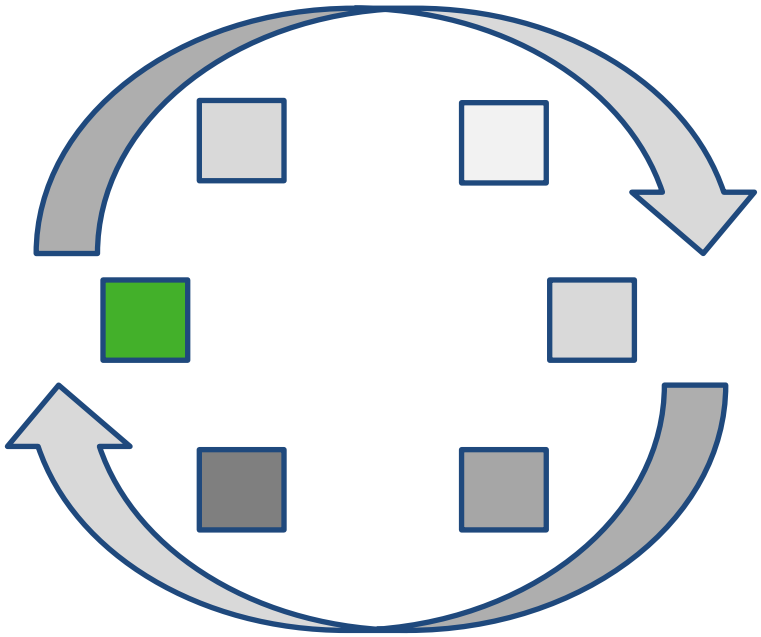
Riskienhallinnan kypsyystasot

Riskienhallinnan kypsyystasot

- **Riskienhallinnan tahtotilan määrittäminen**
- **Kypsyystasojen arviointi riskienhallinnan käynnistämisessä**
- **Riskienhallinnan kypsyyden arviointi osana riskienhallinnan suunnittelua ja kehittämistä**

Riskienhallinnan kehityskohteita

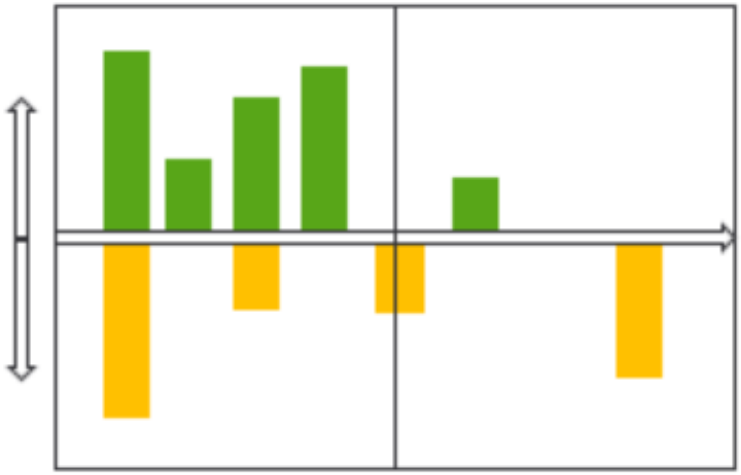
Dynaaminen riskienhallinta



Dynaaminen riskienhallinta

- **Riskien tunnistaminen dynaamisesti organisaation prosesseissa**
- **Dynaamisesti tunnistettujen riskien integrointi osaksi kokonaisvaltaista riskienhallintaa**

Positiiviset riskit



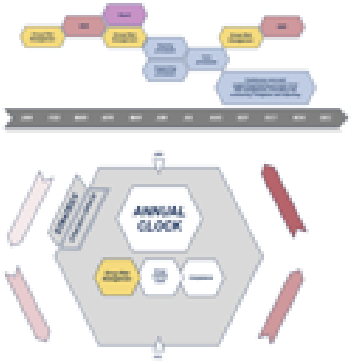
Positiiviset riskit

- **Riskien positiivisten vaikutusten sekä mahdollisuuksien tunnistaminen voi tuoda uusia näkökulmia sekä lisäarvoa kun se on toimivasti yhdistetty riskikartoitusprosessiin.**

- **Riskien positiivisten vaikutusten arviointi vaatii toimiakseen riittävän riskienhallinnan maturiteetin sekä riskienarviointiasteikon kehitystä**

Yhteenveto

Riskityöpajan yhteenveto



Yhteenveto

- **Riskienhallinta yleisesti**
- **Riskien tunnistaminen ja hallinta**
- **Riskienhallinta ja johtaminen**
- **Merkittävimmät riskit**
- **Riskienhallinnan kehittäminen organisaatiossa**

Kotitehtävä 12.6.2017

Tämän jälkeen - kertaus

- 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-video 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
  - JUHTA / VAHTI toimittaa tästä lisää ohjeita kesän aikana videon ja nettitestien julkaisun jälkeen