VALTIO EXPO

Valtiokonttori
Statskontoret
State Treasury

Tekoälyn hallinta(malli)

Virpi Hotti, johtava asiantuntija
Valtiokonttori

Sisältö

Tekoälyn hallinta ja normatiiviset asiakirjat

- Pohjautuu 17.2.2025 alkaneeseen virastoyhteistyöhön tekoälyhallintamallirungon tekemiseksi
- Pohjautuu Gartnerin AI Playbookiin sekä EU ja Valtiovarainministeriön julkaisuihin

Tiedonhallintamalliin uusia näkymiä kuten automaatio ja AI-inventoinnit

- Pohjautuu Tiedonhallintalautakunnan suosituksiin ja VAHTI-työkalupohjiin

Alustakontrollit

- Pohjautuu Purview Regulations kehyskontrollitietoihin, jotka on poimittu yhteistyössä Microsoftin Jari Heleniuksen kanssa
- Havainnollistetaan PowerBI-työkalunäkymien avulla

Jatkoajatuksia


Terveyden ja
hyvinvoinnin laitos


PRH
PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN


Palkeet


VERO
SKATT


ork
OIKEUSREKISTERIKESKUS
RÄTTSREGISTERCENTRALEN


Valtori
Valtion tieto- ja
viestintätekniikkakeskus


Valtiokonttori
Statskontoret
State Treasury


Kela


TRAFICOM
Liikenne- ja viestintävirasto

Tekoälyn hallinta ja normatiiviset asiakirjat

Tekoälyn hallinnan osiot

Toimintamalli osiossa luodaan malli, joka määrittää, miten AI-hallinta toteutetaan käytännössä.

Politiikat ja kontrollit osiossa luodaan ja ylläpidetään sääntöjä ja ohjeita, jotka määrittävät, miten tekoälyä (AI) hallitaan ja valvotaan.

Valvontajärjestelmät osiossa kehitetään ja otetaan käyttöön järjestelmiä, jotka auttavat hallitsemaan ja valvomaan AI-järjestelmiä.

Lähde: Gartner (8 January 2025 - ID G00821275) "Executive AI Governance Playbook"

AI Governance Tekoälyn hallinta	**Governance Operating Model** Toimintamalli	**Responsible AI –** Vastuullinen tekoäly **Organization & Teams –** Organisaatio ja tiimit **Decision Rights –** Päätösoikeudet **People & Culture –** Ihmiset ja kulttuuri **Mandate & Scope –** Tekoälyn kehittämisen mandaatti ja laajuus **Communication** - Kommunikointi
	Policies & Controls Politiikat ja kontrollit	**AI Risk –** Tekoälyyn liittyvät riskit **Legal & Regulatory Compliance –** Lainsäädännön ja sääntelyn noudattaminen **AI Security –** Tekoälyn turvallisuus **AI Ethics –** Tekoälyn etiikka **Principles –** Periaatteet **Privacy –** Tietosuoja **Trustworthy AI –** Luotettava tekoäly **Sustainable AI –** Kestävä tekoäly
	Oversight Systems Valvontajärjestelmät	**AI Life Cycle –** Tekoälyn elinkaari **Monitoring & Compliance Reporting –** Seuranta ja vaatimustenmukaisuuden raportointi **Data Governance –** Tiedonhallinta **Testing & Validation –** Testaus ja validointi **Governance Systems & Tools –** Hallintajärjestelmät ja -työkalut **Vendor Coordination –** Toimittajayhteistyö

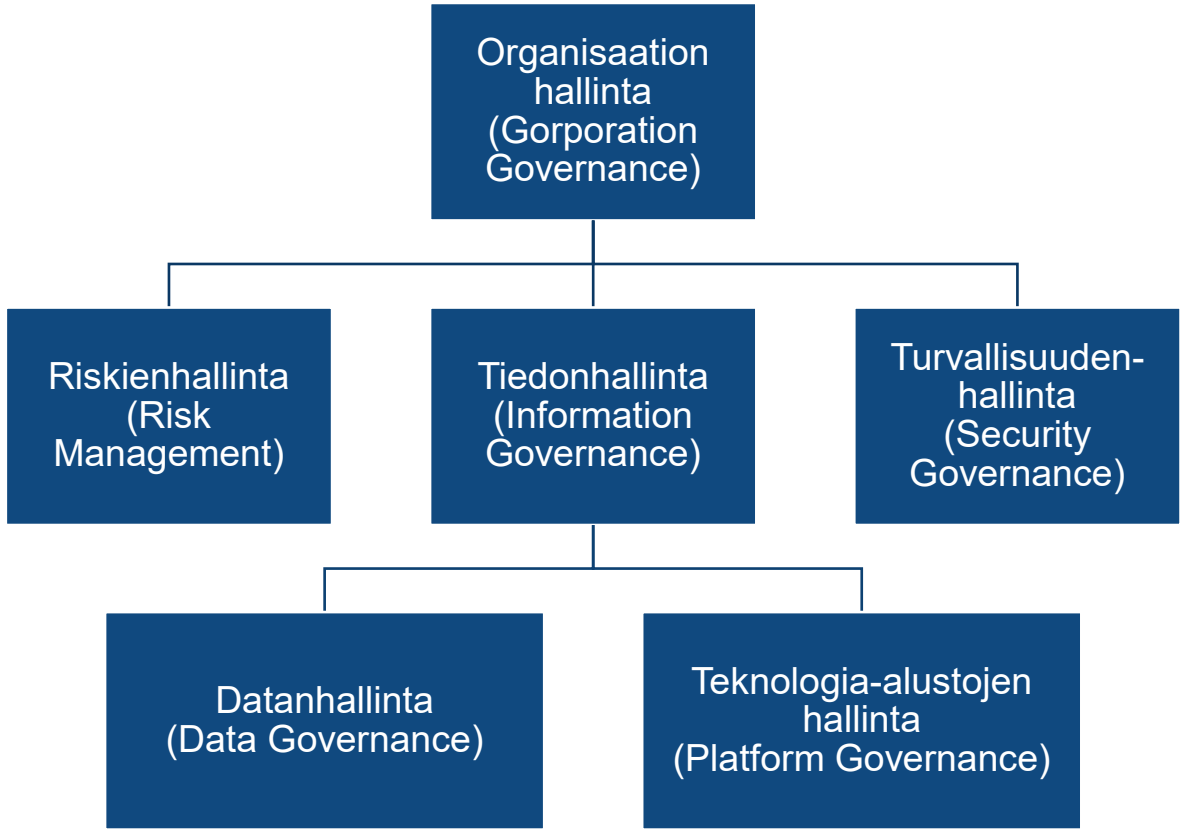
Lähde: Gartner (8 January 2025 - ID G00821275) "Executive AI Governance Playbook"

Tekoälyn hallinta

Tekoälyn hallinnassa otetaan huomioon organisaation olemassa olevat päätöksentekomallit ja hallintamallit.

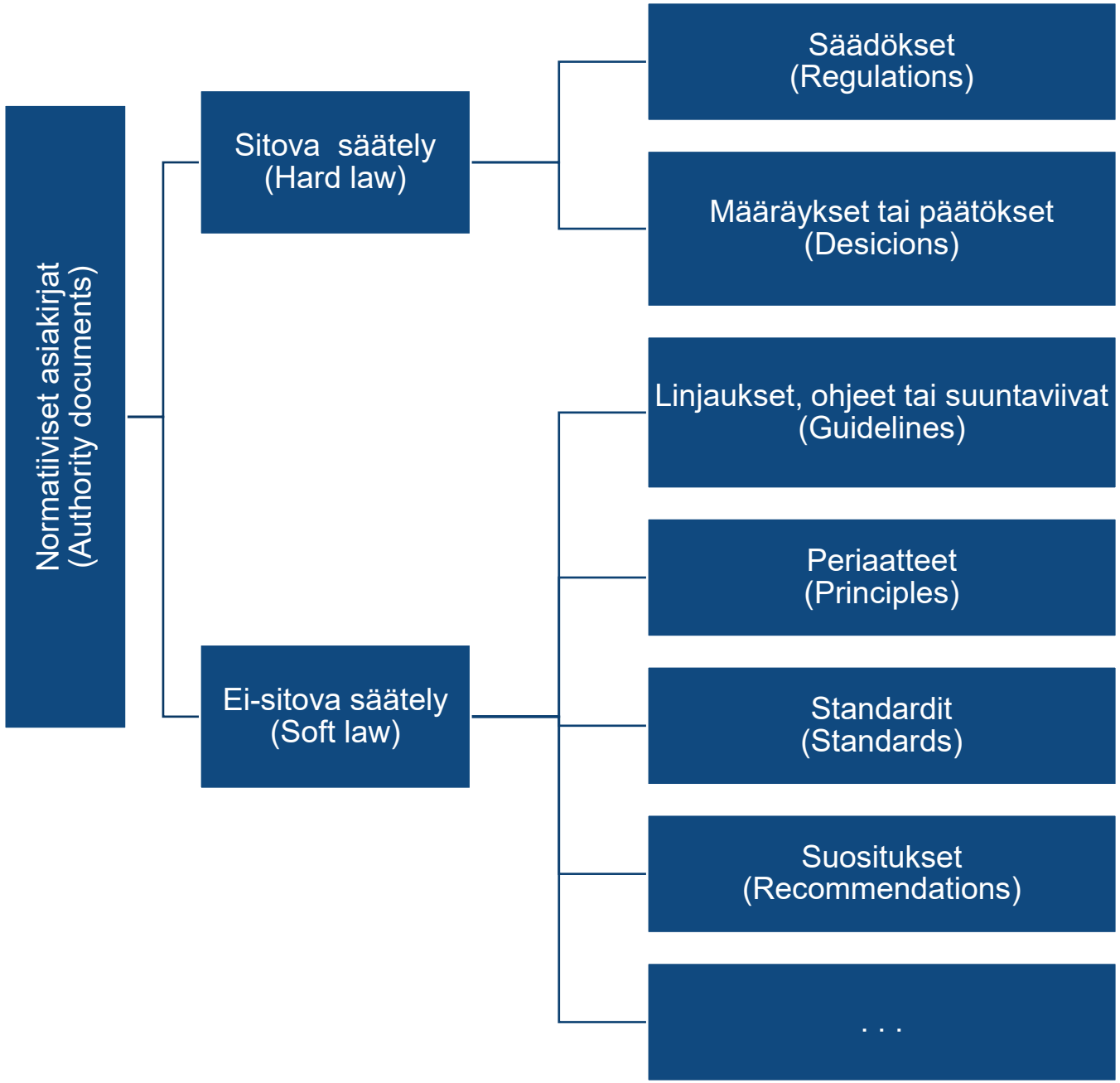
Tekoälyn hallinta on inventointi-, vaikutustenarviointi- ja valvontaprosessien muodostama kokonaisuus.

- Inventointiprosesseissa käydään läpi normatiiviset asiakirjat sekä tekoälyjärjestelmien ja mallien ominaisuudet, tehdään riskiarvioinnit ja määritellään mitigointikeinot.
- Vaikutustenarviointiprosessit kohdistuvat tarpeen mukaan tietosuojaan ja tietojen liikkumiseen sekä mahdollisesti perusoikeuksiin.
- Valvontaprosessit skannaavat tietoaineistoja ja seuraavat tietoteknisistä resursseja sekä arvioivat niiden komplianttiutta.

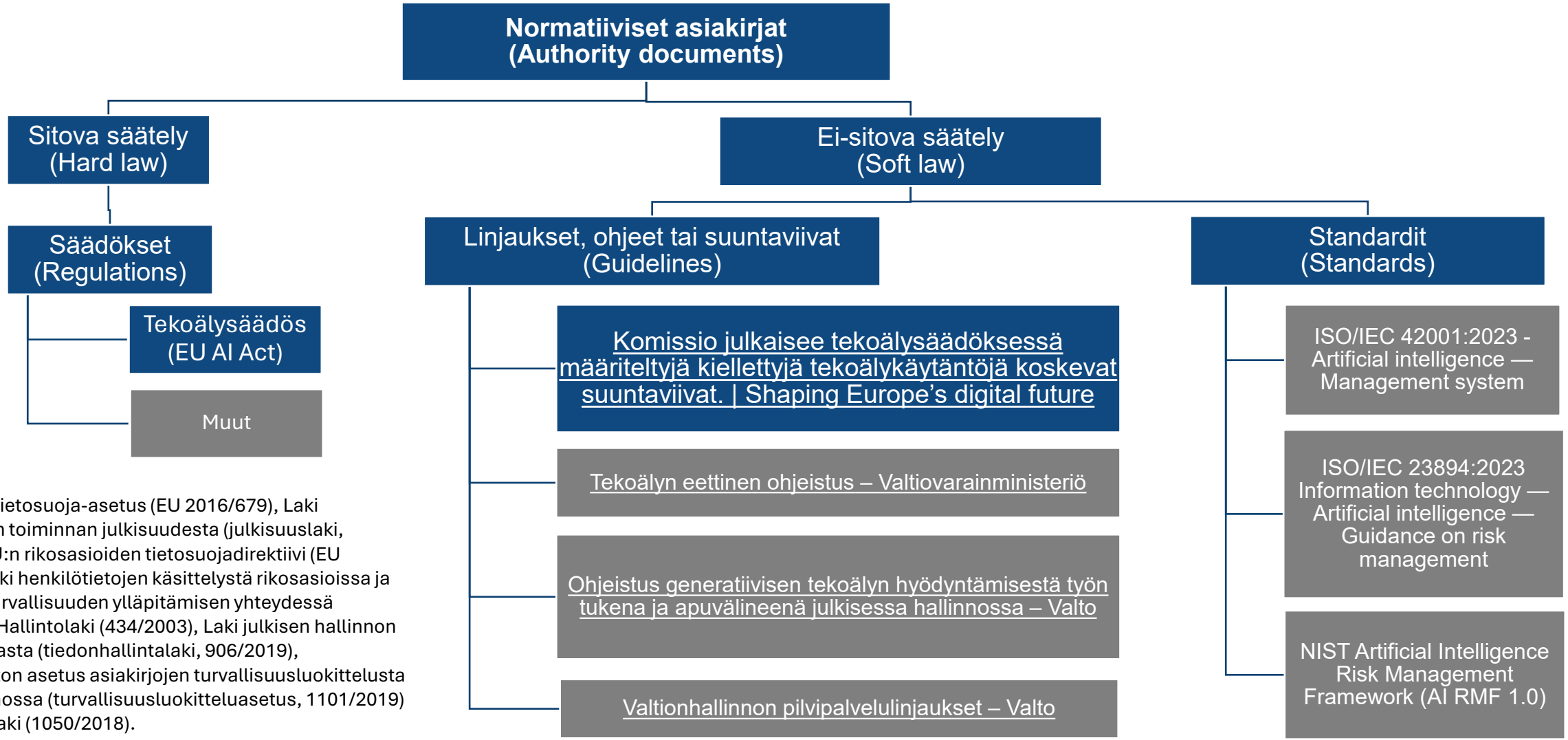


Normatiiviset asiakirjat

- Organisaatiota velvoittaa erilaiset säädökset sekä määräykset tai päätökset
- Organisaatio päättää, mitä muita normatiivisia asiakirjoja se noudattaa.
- Normatiivisten asiakirjojen perusteella muodostetaan politiikat, joita organisaatio noudattaa. Lisäksi normatiivisten asiakirjojen perusteella määritellään ja sanoitetaan asioita.
- Normatiivisten asiakirjojen valinta vaikuttaa teknologia-alustakontrolleihin.



Tekoälyn hallintaan tunnistettuja normatiivisia asiakirjoja



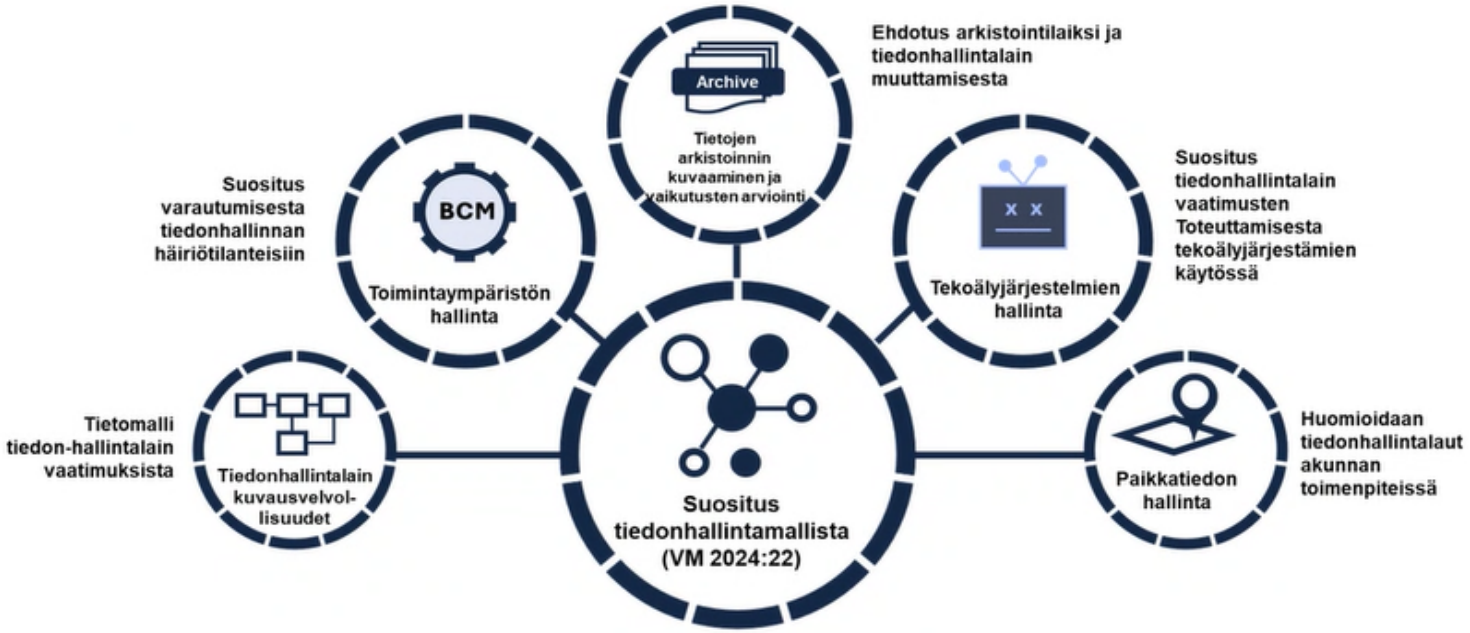
EU:n yleinen tietosuoja-asetus (EU 2016/679), Laki viranomaisten toiminnan julkisuudesta (julkisuuslaki, 621/1999), EU:n rikosasioiden tietosuojadirektiivi (EU 2016/680), Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018), Hallintolaki (434/2003), Laki julkisen hallinnon tiedonhallinnasta (tiedonhallintalaki, 906/2019), Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta Valtionhallinnossa (turvallisuusluokitteluasetus, 1101/2019) ja Tietosuojalaki (1050/2018).

Tiedonhallintamalli, jonka avulla ”määritetään ja ohjataan tiedon hallintaa”

Tiedonhallintamallin käyttäminen tiedonhallinnassa

Tiedonhallintalautakunnan toimenpiteitä 2025

- Suositus varautumisesta tiedonhallinnan häiriötilanteisiin (tiedonhallintamallin käyttö jatkuvuuden hallinnassa)
- Suositus tiedonhallintalain vaatimusten toteuttamisesta tekoälyjärjestelmien käytössä (tiedonhallintamallin käyttö tekoälyjärjestelmien hallinnassa)
- Paikkatietojen hallinta (tiedonhallintamallissa kuvattavat tiedot)
- Tiedonhallintalakiin tulevien muutosten päivittäminen lautakunnan suosituksiin (arkistointilaki)
- Tietomalli tiedonhallintalaissa säädetyistä vaatimuksista (tiedonhallintamalli, asiakirjajulkisuuskuvaus)

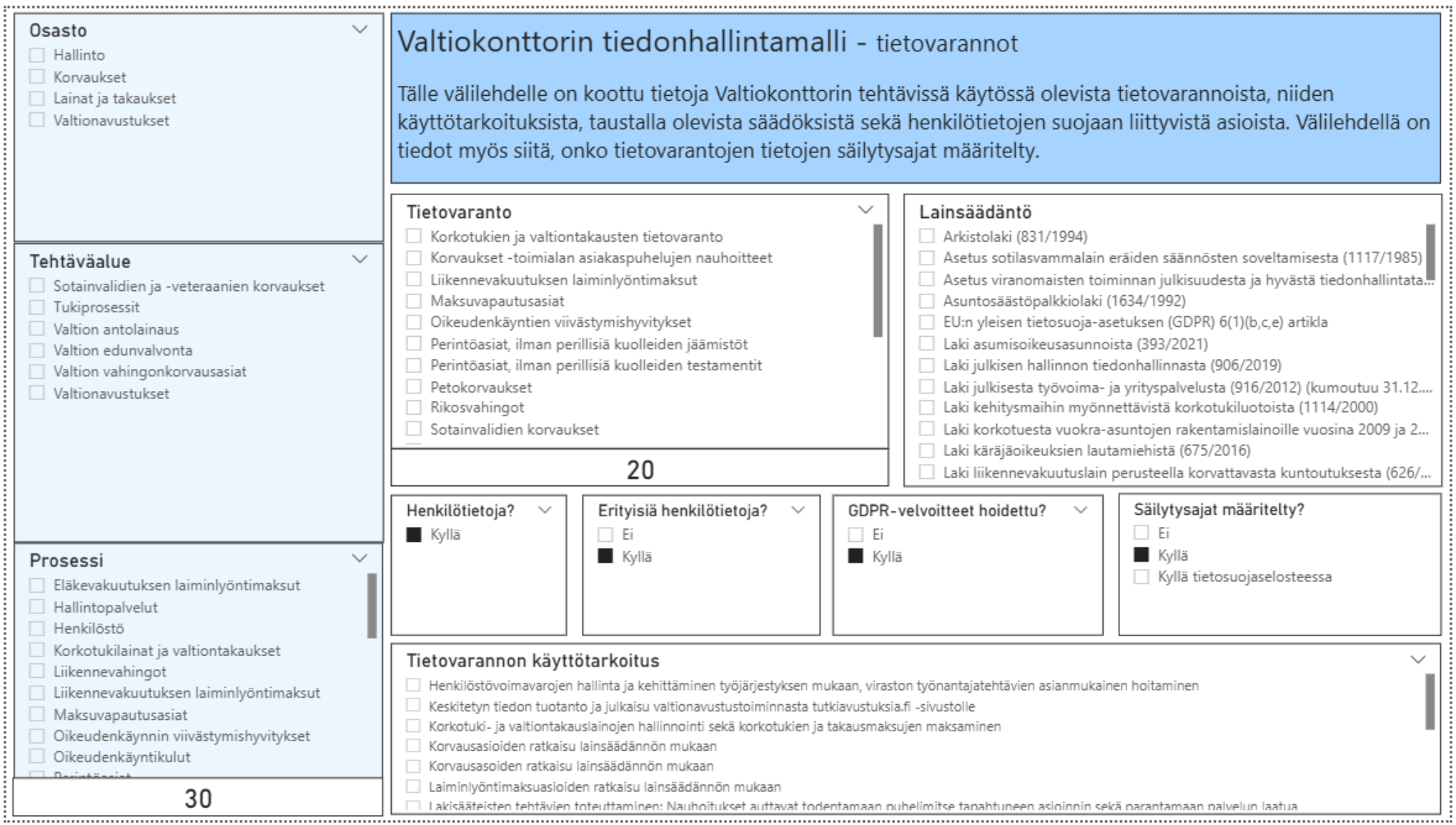


Tiedonhallintamallia ylläpidetään

- Palvelujen, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi
- Tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi,
- Moninkertaisen tietojen keruun vähentämiseksi,
- Tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteuttamiseksi
- Tietoturvallisuuden ylläpitämiseksi

Lähde: Tiedonhallintalautakunta, Oikarinen Tommi (3.4.2025) Arkkitehtuurikillan esitys.

Esimerkki säädösvelvotteiden huomioimisesta

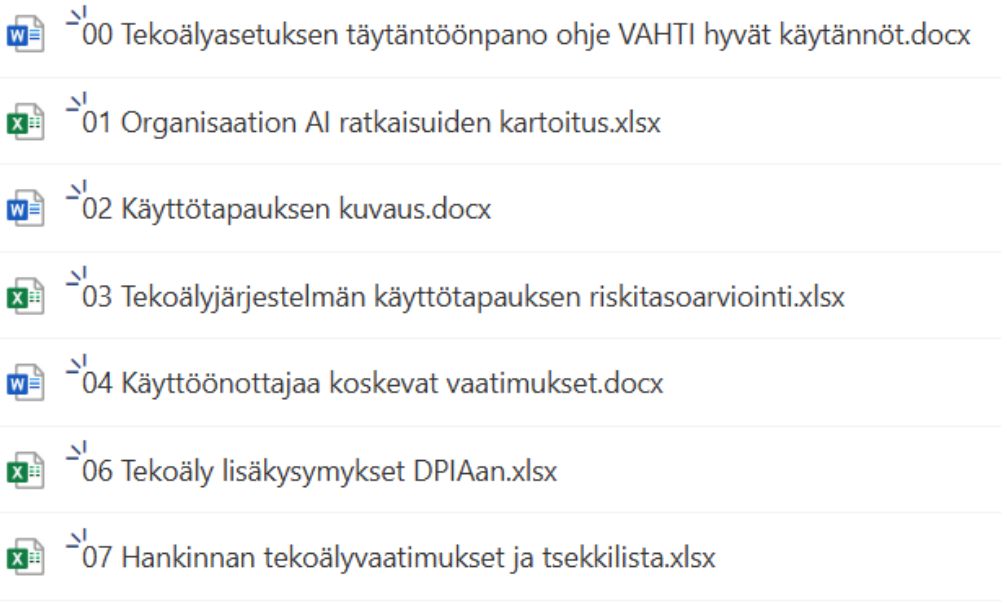


VAHTI-TIKE-työkaluesimerkkejä

Valtionhallinnon tietoturvan vastuuhenkilöiden verkoston (VAHTI) tietosuojan kehittämisen (TIKE) työryhmä on muodostanut työkaluja (Excel- ja Word-dokumentteja) tekoälyjärjestelmien kartoittamiseen ja käyttötapausten arviointiin.

Valtorin vanhempi juristi Päivi Kynkäänniemi on neuvonut työvälineiden käyttöön:

- Käyttöönottaja täyttää lomakkeet (01-04) – jollei johonkin kysymykseen osaa vastata, niin voi laittaa 03-lomakkeen osalta Valtorille tiketin
- Tarjoaja täyttää lomakkeen 07 yhdessä toimittajan kanssa
- Kun lomakkeet on täytetty, niin sitten tietosuoja-arviointi (huomioi lomake 06) ja tietoturva-arviointi
  - Tietoturva-arvioinnin yhteydessä käydään läpi tietojen salassapitoluokat



FRIA-työkalu mukaan, jos tehdään profilointia

Tiedonhallintamalli - automaatio- ja AI-inventoinnit

Osittajat eli suodattimet: osasto, tehtäväalue, prosessi, tietovaranto

Automaattisen ratkaisumenettely

- Menettelyn nimi ja lyhyt kuvaus
- Käsittelysäännöt kuvattu – K/E
- Suojatoimet kuvattu – K/E
- Käyttöönottopäätös tehty – K/E

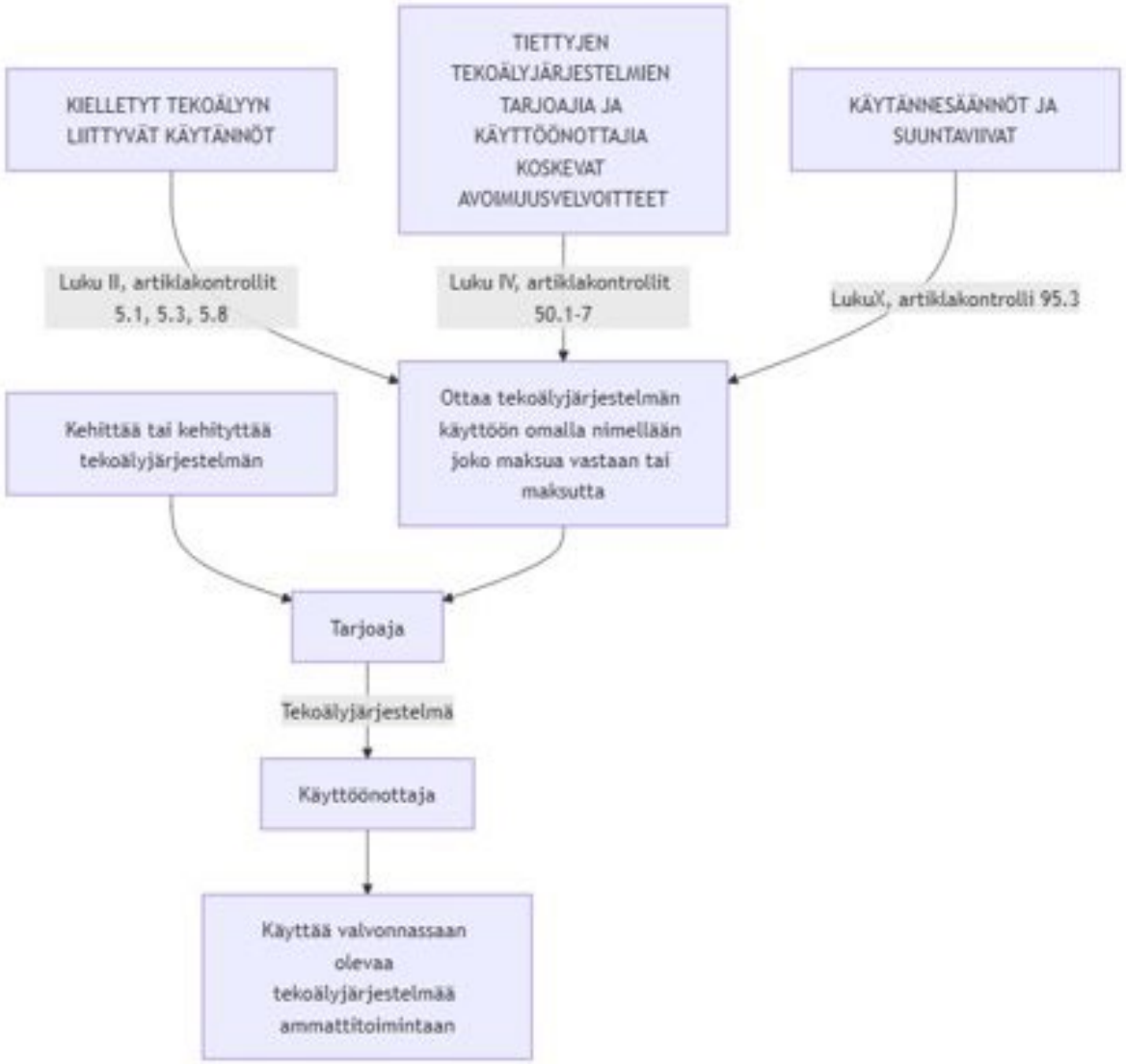
Tekoälyratkaisu

- Ratkaisun nimi ja lyhyt kuvaus
- Tekoälysäädöksen riskiluokka: Kielletyt Käytännöt, Korkea (turvallisuus), Korkea (profilointi), Erikoisryhmä 1 (yleiskäyttöiset tekoälymallit), Erikoisryhmä 2 (kommunikoivat), Vähäinen riski
- Tekoälysäädöksen toimijarooli(t): Toimittaja, Käyttöönottaja
- Täydennetty DPIA – K/E
- Perusoikeusvaikutustenarviointi (FRIA) – K/E
- Tiedot pysyvät EU Data Boundaryssä (TIA) – K/E
- Tietoturva-arviointi/-auditointi – K/E

Alustakontrollit

Kontrollit

- Säädöksistä ja muista kehyksistä (a.k.a., normatiiviset asiakirjat tai viranomaisasiakirjat) muodostuu teknologia-alustoilla huomioitavia kontrolleja, joihin liittyy yksi tai useampia toimia (actions).
- Toimikohtaisesti määritellään vastuurooli ja mahdollisesti työkalu, jonka avulla toimi voidaan hoitaa/raportoida automaattisesti tai manuaalisesti.



Kuvassa esimerkkinä EU AI Act -tarkastelu, kun organisaatioissa ei ole suurriskisiä tekoälyjärjestelmiä ja organisaatio kehityttää omia tekoälyjärjestelmiä

Kehyskontrollikokoelmaesimerkkejä

- **EU AI Act** eli tekoälysäädös
- **EU GDPR** eli General Data Protection Regulation, joka on tietosuoja-asetus
- **FI DP Act** eli Finland - Data Protection Act
- **NIST AI RMF** eli National Institute of Standards and Technology AI Risk Management Framework
- **ISO/IEC 23894** eli International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 23894 IT— AI — Guidance on risk management
- **ISO/IEC 42001** eli International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 42001 IT — AI — Management system
- **NIS2** eli Network and Information Security 2 direktiivi
- **DPB** eli Microsoft Data Protection Baseline, joka sisältyy tilauksiin (subscriptions) ja se sisältää kontrolleja seuraavista: NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) and ISO (International Organization for Standardization), FedRAMP (Federal Risk and Authorization Management Program) ja GDPR (General Data Protection Regulation of the European Union).

Kehyskontrollikokoelmien kenttiä

Framework	Kehyksen lyhenne
Control Family	Kontrollin kategoria kuten EU AI Act:n luku ja otsikko
Control	Kontrollin tunniste kuten EU AI Act:n artiklanumero
Control Title	Kontrollin nimi
Control Description	Kontrollin kuvaus
Action Title	Toimen otsikko, pääsääntöisesti muodossa verbi+kohde
Action Description	Toimen kuvaus
Action Type	Toimen tyyppi
Action Owner	Toimen omistaja, joka tulee nimetä
Compliance Score	Saa arvon 1-54 – mitä suurempi arvo, sitä enemmän vaikuttaa kompliantiusprosenttiin
Related Controls	Viittauksia muihin kontrollinimiin
Microsoft Solution Name	Microsoftin työkalusuositus toimen hoitamiseksi
Microsoft Implementation Details	Microsoftin toteutuskuvaus toimen suorittamiseksi

Overview

What's new? New Overview

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. Find guidance and documentation

Filter

Overall compliance score

Your compliance score: 74%

6447/8655 points achieved

Your points achieved
1/ 2,155

Microsoft managed points achieved
6,446/ 6,500

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Key improvement actions

Not completed	Completed	Out of scope
476	**1**	**0**

Improvement action	Impact	Test status	Group	Action type
Create and publish a retention label	+27 points	Failed high risk	Default Group	Technical
Control unmanaged device access	+27 points	None	Default Group	Technical
Disable 'Insecure guest logons' in Server Message Block (SMB)	+27 points	None	Default Group	Technical
Disable running or installing downloaded software with invalid sig...	+27 points	None	Default Group	Technical
Utilize sensitivity labels for data restriction	+27 points	None	Default Group	Technical
Manage endpoint security	+27 points	None	Default Group	Technical
Log off idle sessions	+27 points	None	Default Group	Technical
Create and apply a retention policy	+27 points	Failed high risk	Default Group	Technical
Detect and block malware and viruses	+27 points	None	Default Group	Technical
Provide privacy information for organizations	+27 points	None	Default Group	Technical

Luku ja jakso	Artikla	Kontrollien lkm	Toimien km
Kaikki	Kaikki	160	82
25	112		

Luku ja jakso	Artikla	Kontrolli	Toimi	Työväline
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	10 Data ja datanhallinta	Article 10.2 Data and data governance	Apply sensitivity labels to protect personal data	Purview
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	11 Tekninen dokumentaatio	Article 11.1 Technical documentation	Retain operational compliance supporting documentation	Purview
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	11 Tekninen dokumentaatio	Article 11.2 Technical documentation	Create and apply a retention policy	Purview
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	12 Tietojen säilyttäminen	Article 12.1 Record keeping	Configure automatic log upload	Defender
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	12 Tietojen säilyttäminen	Article 12.1 Record keeping	Monitor cloud activity log	Azure
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	12 Tietojen säilyttäminen	Article 12.2 Record keeping	Enable audit logging	Audit
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	12 Tietojen säilyttäminen	Article 12.3 Record keeping	Enable audit logging	Audit
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	13 Avoimuus ja tietojen antaminen käyttöönottajille	Article 13.2 Transparency and provision of information to deployers	Centralize AI app management with enhanced security	Purview
III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmiä koskevat vaatimukset	13 Avoimuus ja tietojen antaminen käyttöönottajille	Article 13.3 Transparency and provision of information to deployers	Create terms and conditions for user access	Intune

Luku ja jakso

Useita valintoja

3

Artikla

Useita valintoja

3

Kontrollien lkm

10

Toimien km

6

Luku ja jakso	Artikla	Kontrolli	Toimi	Työväline
II KIELLETYT TEKOÄLYYN LIITTYVÄT KÄYTÄNNÖT	5 Kielletyt tekoälyyn liittyvät käytännöt	Article 5.1 Prohibited AI Practices	Create customized DLP policies for personally identifiable information (PII)	Purview
II KIELLETYT TEKOÄLYYN LIITTYVÄT KÄYTÄNNÖT	5 Kielletyt tekoälyyn liittyvät käytännöt	Article 5.1 Prohibited AI Practices	Develop spillage response procedures	Purview
II KIELLETYT TEKOÄLYYN LIITTYVÄT KÄYTÄNNÖT	5 Kielletyt tekoälyyn liittyvät käytännöt	Article 5.1 Prohibited AI Practices	Enable security posture management for SaaS apps	Defender
II KIELLETYT TEKOÄLYYN LIITTYVÄT KÄYTÄNNÖT	5 Kielletyt tekoälyyn liittyvät käytännöt	Article 5.3 Prohibited AI Practices	Create data minimization policies to support privacy goals	Priva
II KIELLETYT TEKOÄLYYN LIITTYVÄT KÄYTÄNNÖT	5 Kielletyt tekoälyyn liittyvät käytännöt	Article 5.8 Prohibited AI Practices	Integrate third-party applications with compliance tools	Purview
IV TIETTYJEN TEKOÄLYJÄRJESTELMIEN TARJOAJIA JA KÄYTTÖÖNOTTAJIA KOSKEVAT AVOIMUUSVELVOITTEET	50 Tiettyjen tekoälyjärjestelmien tarjoajia ja käyttöönottajia koskevat avoimuusvelvoitteet	Article 50.1 Transparency obligations for providers and users of certain AI systems	Provide system use notifications to users at logon	Windows 10
IV TIETTYJEN TEKOÄLYJÄRJESTELMIEN TARJOAJIA JA KÄYTTÖÖNOTTAJIA KOSKEVAT AVOIMUUSVELVOITTEET	50 Tiettyjen tekoälyjärjestelmien tarjoajia ja käyttöönottajia koskevat avoimuusvelvoitteet	Article 50.2 Transparency obligations for providers and users of certain AI systems	Provide system use notifications to users at logon	Windows 10
IV TIETTYJEN TEKOÄLYJÄRJESTELMIEN TARJOAJIA JA KÄYTTÖÖNOTTAJIA KOSKEVAT AVOIMUUSVELVOITTEET	50 Tiettyjen tekoälyjärjestelmien tarjoajia ja käyttöönottajia koskevat avoimuusvelvoitteet	Article 50.3 Transparency obligations for providers and users of certain AI systems	Provide system use notifications to users at logon	Windows 10
IV TIETTYJEN TEKOÄLYJÄRJESTELMIEN TARJOAJIA JA KÄYTTÖÖNOTTAJIA KOSKEVAT AVOIMUUSVELVOITTEET	50 Tiettyjen tekoälyjärjestelmien tarjoajia ja käyttöönottajia koskevat avoimuusvelvoitteet	Article 50.4 Transparency obligations for providers and users of certain AI systems	Provide system use notifications to users at logon	Windows 10
IV TIETTYJEN TEKOÄLYJÄRJESTELMIEN TARJOAJIA JA KÄYTTÖÖNOTTAJIA KOSKEVAT AVOIMUUSVELVOITTEET	50 Tiettyjen tekoälyjärjestelmien tarjoajia ja käyttöönottajia koskevat avoimuusvelvoitteet	Article 50.5 Transparency obligations for providers and users of certain AI systems	Provide system use notifications to users at logon	Windows 10

Luku ja jakso

- [ ] I YLEISET SÄÄNNÖKSET
- [ ] II KIELLETYT TEKOÄLYYN LIITTYVÄT KÄYTÄNNÖT
- [ ] III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 1 Tekoälyjärjestelmien luokittel...
- [ ] III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmi...
- [ ] III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 3 Suurriskisten tekoälyjärjestel...
- [ ] III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 4 Ilmoittamisesta vastaavat vira...
- [ ] III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 5 Standardit, vaatimustenmukai...

25

Artikla

- [ ] 1 Kohde
- [ ] 10 Data ja datanhallinta
- [ ] 100 Unionin toimielimille, elimille, laitoksille ja vi...
- [ ] 101 Yleiskäyttöisten tekoälymalllien tarjoajille m...
- [ ] 102 Asetuksen(EY) N:o 300/2008 muuttaminen
- [ ] 103 Asetuksen(EU) N:o 167/2013 muuttaminen
- [ ] 104 Asetuksen(EU) N:o 168/2013 muuttaminen

112

Kontrollien lkm

160

Toimien km

82

Toimen tyyppi

- [ ] Documentation
- [ ] Operational
- [ ] Technical

Työväline

- [ ] Attack Simulation Tr...
- [ ] Audit
- [ ] Azure
- [ ] Defender
- [ ] Entra ID
- [ ] Exchange Online Pr...

Toimi	Toimen kuvaus
Review cloud traffic logs for ongoing visibility	Microsoft recommends that your organization admin review and analyze logs from your on-premise firewalls to provide visibility into cloud application usage and security posture.**How to Use Microsoft Solutions to Implement**Your organization can use **Microsoft Defender for Cloud Apps** through the "Microsoft 365 Defender" to create and review Cloud Discovery snapshot report for reviewing the logs from your on-premises firewalls. Select **Launch Now** to visit the portal, under "Cloud Apps", select "Cloud discovery". In the top-right corner, pull down "Actions", and select "Create Cloud Discovery snapshot report".[Launch Now](https://aka.ms/AAl3yig)**Learn More**[Set up cloud discovery](https://aka.ms/AA9xvyr)[Create snapshot Cloud Discovery reports](https://aka.ms/AA9ymof)
Control unmanaged device access	Microsoft recommends that your organization block or limit access to your organizational systems and/or data from unmanaged devices. Blocking access from unmanaged devices facilitates the protection of your systems/data and can facilitate regulatory compliance. As unmanaged devices may not have the configuration required by your organization and/or sufficient security controls, they may be more susceptible to be vectors and/or targets of cyber attacks and malicious use.**How to Use Microsoft Solutions to Implement**Your organization can use **SharePoint admin center** to block or limit access to SharePoir content from unmanaged devices. Select **Launch Now** to visit the portal. Select " Access control" in the new "SharePoint admin center" with with an account that has admin permissions for your organization. Select "Unmanaged devices" and then select "Allow limited", "web-only access", and then select "Save". [Launch Now](https://aka.ms/AAay46x)**Learn More**[Contro unmanaged device access](https://aka.ms/AAaxpd9)[Get started with the new SharePoint admin center](https://aka.ms/AA9ytw4)
Integrate compliance tool with	Microsoft recommends that your organization can integrate compliance tool in conjunction with AI application for better risk

Luku ja jakso

- [ ] II KIELLETYT TEKOÄLYYN LIITTYVÄT KÄYTÄNNÖT
- [ ] III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 1 Tekoälyjärjestelmien luokittel...
- [ ] III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 2 Suurriskisiä tekoälyjärjestelmi...
- [ ] III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 3 Suurriskisten tekoälyjärjestel...
- [ ] III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 4 Ilmoittamisesta vastaavat vira...
- [ ] III SUURIRISKISET TEKOÄLYJÄRJESTELMÄT 5 Standardit, vaatimustenmukai...
- [ ] IV TIETTYJEN TEKOÄLYJÄRJESTELMIEN TARJOAJIA JA KÄYTTÖÖNOTTAJIA ...

15

Artikla

- [ ] 10 Data ja datanhallinta
- [ ] 11 Tekninen dokumentaatio
- [ ] 13 Avoimuus ja tietojen antaminen käyttöönottaj...
- [ ] 14 Ihmisen suorittama valvonta
- [ ] 15 Tarkkuus vakaus ja kyberturvallisuus
- [ ] 16 Suuririskisten tekoälyjärjestelmien tarjoajien v...
- [ ] 17 Laadunhallintajärjestelmä

49

Kontrollien lkm

110

Toimien km

26

Toimen tyyppi

- [ ] Documentation
- [ ] Operational
- [ ] Technical

Työväline

- [ ] Microsoft 365 admi...
- [ ] Microsoft Teams
- [ ] Priva
- [x] Purview
- [ ] SharePoint Online
- [ ] Windows 10

Toimi	Toimen kuvaus
Apply sensitivity labels to protect personal data	Microsoft recommends that your organization classify and protect personal data through the use of sensitivity labels. When applying a sensitivity label to an email or document, any configured protection settings for that label are enforced on the content. Sensitivity labels can be used to automatically encrypt data in transit and create visual markings that include headers, footers, and watermarks. They can also help you categorize personal data so that you can protect it from illicit access, and it makes it easier to investigate discovered breaches.**How to Use Microsoft Solutions to Implement**Your organization can use **Microsoft Information Protection** within "Microsoft 365 Compliance Center" to classify and protect personal data. Select **Launch Now** to create and manage "sensitivity labels" and policies in the "Microsoft 365 Compliance Center". Select "Information protection" > "Labels" > "+Create a label" Configure the policy to your organization's specific needs. You can configure automatic classification policies for Office files (e.g., PowerPoint, Excel, Word, etc.) and Microsoft 365 services like OneDrive, SharePoint Online, and Exchange Online.Your organization can also use Powershell to create and configure sensitivity labels and policies.[PowerShell](https://docs.microsoft.com/microsoft-365/compliance/create-sensitivity-labels#use-powershell for-sensitivity-labels-and-their-policies)**Prerequisites and licensing requirements**[Subscription and licensing requirements fc sensitivity labels](https://aka.ms/AAa0fx0)[Launch Now](https://aka.ms/AA9z7c5)**Learn More**[Create and configure sensitivit labels and their policies] (https://aka.ms/AAncgwf)[Label priority (order matters)](https://aka.ms/AAnc9pd)[Learn about sensitivity labels](https://aka.ms/AAncn2w)
Configure filters for enhanced compliance monitoring	Microsoft recommends that your organization configure filters to help organizations detect and respond to potential compliance violations effectively. By setting up these filters, you can quickly identify and remediate issues such as the disclosur of sensitive information, the use of harassing or threatening language, and the sharing of inappropriate content. Filters allow

Kehystarkasteluyhteenvetoa

Normatiivisten vaatimusten tunnistaminen auttaa valitsemaan organisaatiolle sopivat kehyskontrollikokoelmat

- Kontrolleja ja toimia voi lisätä ja poistaa kehyskontrollikokoelmissa

Kontrollikokoelmat kannattaa käydä läpi risienhallinnasta, tietoturvasta- ja tietosuojasta vastaavien kanssa, jotta saadaan muodostettua yhteisymmärrys siitä, mitä teknologia-alustatasolla voidaan hallita

- Yksittäinen toimi voi vaikuttaa useaan komplianttiustarkasteluun (ks. kuvan portaalit)
- Jotkin toimet, kuten ”Apply sensitivity labels to protect personal [restricted] data”, ovat edellytyksiä muille toiminnallisuuksille kuten Data protection Lossille (DPL) ja Information Protectionille

Jatkoajatuksia

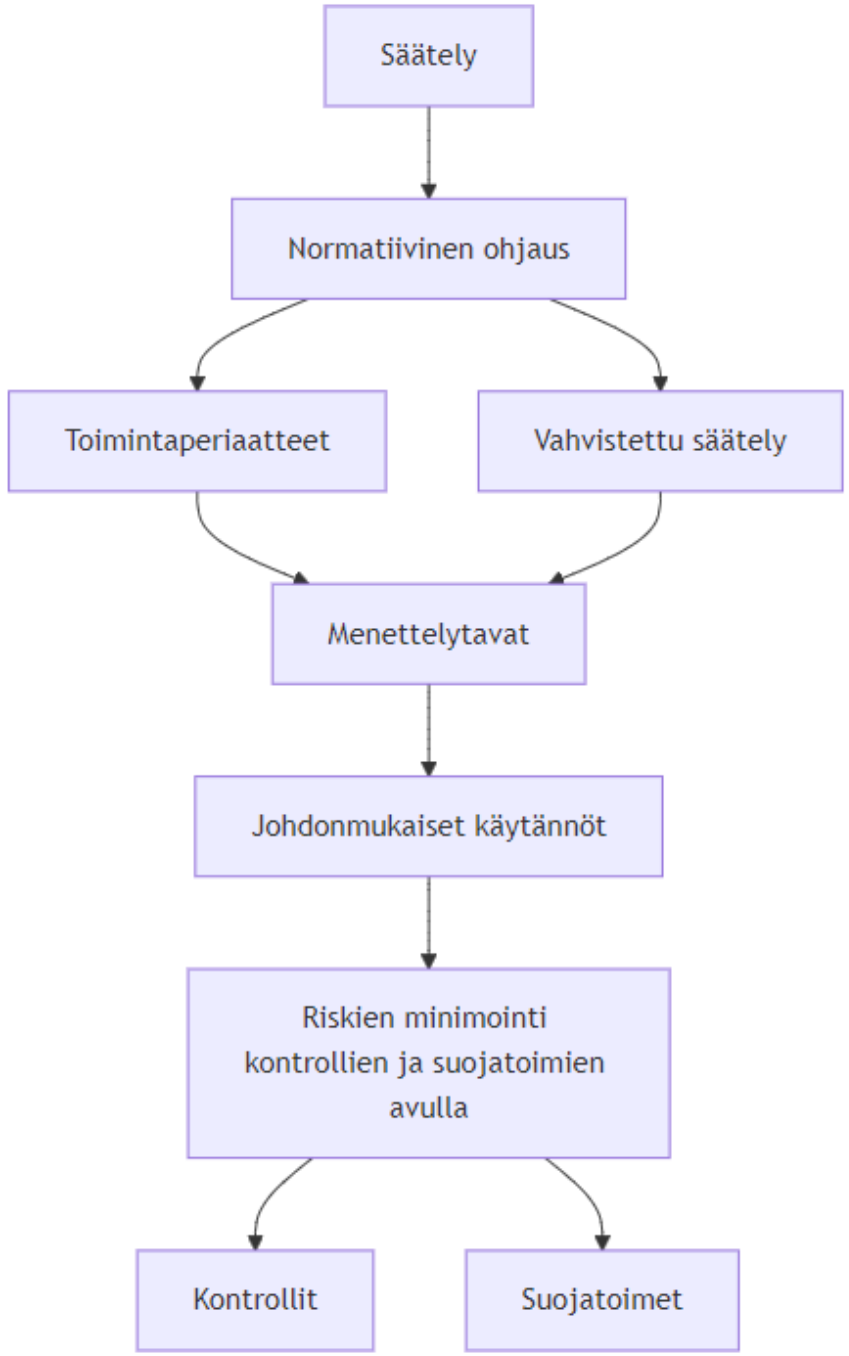
Jatkoajatuksia

- Päivitetään normatiivisten asiakirjojen joukkoa
- Tunnistetaan normatiivisia asiakirjoja vastaavat kehyskontrollit
  - Muodostetaan M365 kehysbaseline ja sitten Azure baseline
- Tunnistetaan riskit ja tiedostetaan, mitkä voidaan mitigoida alustakontrolleilla ja mitkä muiden suojatoimien avulla
- Hyödynnetään esimerkiksi VAHTI-työkaluja käyttötapausten ja erilaisten vaikutusarviointien tekemisessä sekä kehyskontrollivalinnoissa
- Täydennetään tiedonhallintamallia tekoälyratkaisutiedoilla ja huomioidaan Tiedonhallintalautakunnan suositukset
- Osallistutaan hallintamallityöhön muiden työryhmien ja virastojen kanssa

Luomalla selkeät toimintaperiaatteet (policies) ja menettelytavat (procedures) organisaatiot voivat muodostaa johdonmukaiset käytännöt (practices) ja minimoida riskit kontrollien ja suojatoimien avulla. Kontrolli vastaa usein kysymyksiin "mitä" ja "miksi”, ja niihin liittyy yksi tai useampi suojatoimi (safeguard), joka vastaa kysymykseen "miten".

Datan, tekoälyn ja muiden kohteiden voidaan lähestyä **kolmitasoisesti:**

- **Normatiivinen ohjaus**: sitovan säätelyn ja ei-sitovan säätelyn tunnistaminen sekä toimintaperiaatteiden luominen – linjataan toimintaa ja päätöksentekoa.
- **Vaatimustenmukaisuuden varmistaminen**: menettelytapojen luominen ja riskien minimointi – määritetään normatiivista ohjausta tukevat menettelytavat (ml. erilaiset vaikutusten arvioinnit) ja mekanismit, joiden avulla minimoidaan riskit kontrollien ja suojatoimien avulla
- **Vaatimustenmukaisuuden valvonta**: käytäntö tarkoittaa säännöllistä tapaa toimia eli esimerkiksi tehdään säätelypohjaisten kontrollien mukaiset toimet (actions) ja arvioidaan, voidaanko toimitodenteiden avulla todentaa vaatimustenmukaisuus.



Virpi Hotti

johtava asiantuntija, FT
Valtiokonttori
virpi.hotti@valtiokonttori.fi

Valtiokonttori
Statskontoret
State Treasury