

Tekoöilyn hallintamalli

Astu Labsin suositukset organisaatioille

Tässä suosituksessa

1. Hallintamallin taustoitus
2. Hallintamallin rakenne
3. Strateginen ohjaus ja vastuut
4. Tekoälyn koordinaatioryhmä
5. Tekoälylähettiläät (champions, muutosagentit)
6. Käyttö- ja kehitysmalli
7. Riskienhallinta ja eettiset periaatteet
8. Tekninen ja operatiivinen hallinta
9. Viestintä, koulutus ja muutosjohtaminen
10. Hallintamallin jatkuva kehittäminen

1. Hallintamallin taustoitus



Hallintamallin taustoitus

Tekoäly ja erityisesti generatiiviset tekoälytyökalut ja erilaiset tekoälyagentit ovat siirtymässä yksittäisistä kokeiluista osaksi organisaatioiden päivittäistä toimintaa. Niiden avulla parannetaan tehokkuutta, päätöksenteon laatua ja asiakaskokemusta, mutta samalla ne tuovat mukanaan uuden hallinnan tason, joka poikkeaa perinteisestä IT- ja tietohallintamallista.

Tekoäly muuttaa vastuunjakoa ja toimintalogiikkaa

Perinteinen ohjelmisto on deterministinen: se toimii ennalta määritetyllä tavalla. Tekoäly sen sijaan luo sisältöä, tekee tulkintoja ja ehdottaa päätöksiä, mikä tarkoittaa, että:

- virheiden luonne on erilainen ("hallusinaatiot", väärät tulkinnot),
- tietosuoja- ja tietoturvariskit voivat syntyä huomaamatta, ja
- vastuu ei ole yksiselitteisesti kehittäjällä, IT:llä tai käyttäjällä.

Ilman selkeitä pelisääntöjä tekoäly voi toimia "harmaalla alueella" — ei tahallisesti väärin, mutta ilman valvontaa tai jäljitettävyyttä. Hallintamalli tekee näkyväksi, kuka vastaa mistäkin, millä periaatteilla ja missä rajoissa.

Hallintamallin taustoitus

Johtoryhmälle: hallintamalli on väline strategiseen ohjaukseen ja riskien hallintaan

Tekoälyyn liittyvät riskit eivät ole vain teknisiä, vaan myös maineeseen liittyviä, sekä eettisiä ja juridisia. EU:n AI Act edellyttää, että tekoälyn käyttö on riskiperusteisesti hallittua ja dokumentoitua. Samalla generatiiviset tekoälytyökalut ja tekoälyagentit vaikuttavat suoraan työn tekemisen tapoihin, päätöksentekoon ja tietovirtoihin.

Johtoryhmän näkökulmasta hallintamalli:

- luo läpinäkyvyyden siihen, missä tekoälyä käytetään ja millä vaikutuksilla,
- varmistaa, että tekoäly tukee strategisia tavoitteita (esim. tuottavuus, asiakaskokemus, vastuullisuus),
- mahdollistaa ennakoivan riskienhallinnan ennen kuin ongelmia syntyy,
- auttaa viestimään sidosryhmille (asiakkaat, viranomaiset, työntekijät), että tekoälyä käytetään vastuullisesti ja hallitusti.

Hallintamalli on siis johtamisen väline, ei pelkkä IT-dokumentti. Se luo perustan sille, että tekoälyinvestoinnit ovat hallittuja, mitattavia ja yhteensopivia yhtiön arvojen ja sääntelyn kanssa.

Tietohallinnolle: hallintamalli mahdollistaa kestäväen ja turvallisen skaalaamisen

IT- ja tietohallintoympäristössä Copilotin ja muiden tekoälyratkaisujen myötä tapahtuu merkittävä muutos:

- käyttäjät voivat itse rakentaa ja julkaista omaa tekoälylogiikkaa (esim. agentteja, automaatioita),
- tekoälyn "toimintakoodi" voi olla osittain näkymätöntä ja muuttuvaa,
- tietolähteiden, käyttöoikeuksien ja auditointien hallinta on entistä kriittisempää.

Kun tekoälyratkaisut lisääntyvät, hallintamalli varmistaa, että kaikki agentit toimivat yhteisten periaatteiden ja tietoturvakontrollien puitteissa.

Hallintamallin taustoitus

Tavoitteena vastuullinen, turvallinen ja arvoa tuottava tekoälyekosysteemi

Hallintamallin avulla rakennetaan organisaation oma tekoälyekosysteemi, jossa:

- yksilöt voivat kehittää omia henkilökohtaisia agentejaan hallitusti,
- parhaat agentit voidaan nostaa koko organisaation käyttöön,
- autonomiset ja prosessitason agentit voidaan hyväksyä turvallisesti osaksi liiketoimintaprosesseja,
- kaikki tekoälyn muodot tukevat yhteisiä eettisiä ja tietoturvaperiaatteita.

Tavoitteena ei ole rajoittaa innovointia, vaan mahdollistaa laaja ja turvallinen tekoälyn hyödyntäminen koko organisaatiossa – tavalla, joka lisää tuottavuutta ja luottamusta samanaikaisesti.

2. Hallintamallin rakenne



Hallintamallin rakenne

Tekoälyn ja tekoälyagenttien hallintamalli rakentaa yhtenäisen kehyksen sille, miten tekoälyä suunnitellaan, toteutetaan, valvotaan ja kehitetään organisaation sisällä. Sen tehtävänä on yhdistää strateginen ohjaus, riskienhallinta, eettiset periaatteet ja tekninen toteutus yhdeksi kokonaisuudeksi, joka ohjaa niin päivittäistä käyttöä kuin pitkän aikavälin kehitystä.

Hallintamalli koostuu neljästä toisiinsa kytkeytyvästä osa-alueesta:

1. Strateginen ohjaus ja vastuut

Tämä osa määrittelee päätöksenteon rakenteet, vastuut ja roolit: kuka omistaa tekoälyn kehittämisen, kuka hyväksyy uudet agentit ja kuka vastaa eettisistä, tietoturvallisista ja liiketoiminnallisista linjauksista. Strateginen ohjaus varmistaa, että tekoälytoiminta etenee yhteisen vision mukaisesti ja tukee yhtiön pitkän aikavälin tavoitteita.

2. Käyttö- ja kehitysmalli

Tämä määrittää, miten tekoälyratkaisuja ja agentteja kehitetään, testataan, hyväksytään, julkaistaan ja ylläpidetään. Käyttömalli tekee näkyväksi koko agentin elinkaaren ideasta käytännön tuotantoon – ja luo yhteisen prosessin niin henkilökohtaisten kuin organisaatiotason agenttien kehittämiseksi. Sen avulla voidaan varmistaa, että innovaatiot syntyvät hallitusti ja että parhaat käytännöt ja oppimiset leviävät läpi organisaation.

3. Riskienhallinta ja eettiset periaatteet

Tämä osa kytkee tekoälyn käyttöön liittyvät sääntely- ja vastuukysymykset (esim. EU AI Act, GDPR) osaksi käytännön toimintaa. Sen tavoitteena on varmistaa, että jokainen agentti toimii läpinäkyvästi, oikeudenmukaisesti ja turvallisesti. Malliin sisältyy riskiluokitus, hyväksymisprosessit ja eettinen viitekehys, joka ohjaa päätöksentekoa ja priorisointia.

Hallintamallin rakenne

4. Tekninen ja operatiivinen hallinta

Tämä osa määrittelee alustat, tietolähteet, kontrollit ja valvontamekanismit, joiden avulla tekoälyratkaisuja ylläpidetään ja seurataan. Se varmistaa, että tekoäly toimii osana M365- ja Azure-ympäristöä turvallisesti, että datan käyttö on hallittua ja että kaikista toiminnoista jää auditointikelpoinen jälki. Tekninen hallinta tukee myös skaalaamista – se luo perustan agenttien kasvavalle määrälle ja monimutkaisuudelle ilman, että hallittavuus kärsii.

Yhdessä nämä neljä osa-aluetta muodostavat kokonaisuuden, jossa strateginen tahtotila, käytännön toiminta ja tekninen toteutus kulkevat käsi kädessä. Hallintamallin tehtävä ei ole rajoittaa tekoälyn käyttöä, vaan varmistaa, että se tapahtuu yhteisesti sovituin säännöin, vastuullisesti ja organisaation arvojen mukaisesti.

3. Strateginen ohjaus ja vastuut



Strateginen ohjaus ja vastuut

Pääroolit ja vastuut

Rooli	Vastuu
Johtoryhmä	Päättää tekoälyn linjauksista ja sen nivomisesta strategiaan, hyväksyy periaatteet, seuraa riskejä ja vaikutuksia. Omistaa tekoälyn roadmapin. Astu Labs tukee työtä tarvittaessa ja voi auttaa esimerkiksi osallistumalla roadmapin luomiseen tai hallintamallin rakentamiseen.
Tekoälyn koordinaatioryhmä (Centre of Excellence, tekoälypumppu)	Vastaa tekoälytoiminnan koordinoinnista, raportoinnista ja yhteisistä periaatteista. On vastuussa kustannuksista, osaamisesta ja roadmapin toteutuksesta. Suosittelemme koostuvan IT:n, HR:n ja liiketoiminnan puolelta kootuista henkilöistä. Hyvä koko on 3-6 henkeä. Astu Labsin edustaja voi osallistua toimintaan kuukausittain tai kvartaaleittain.
Tietoturva ja tietosuoja (CISO/DPO), legal	Valvoo lainmukaisuutta, turvallisuus- ja tietosuoja-asioita, hyväksyy agenttien käyttöön liittyvät riskianalyysit. Tukee tekoälyn koordinaatioryhmän työtä ja konsultoi esimerkiksi ohjeistuksien luomista. Myös Astu Labs voi tarjota konsultointia.
Liiketoimintayksiköt	Ehdottavat tekoälyn käyttökohteita, sekä ehdottavat ja ylläpitävät omia agenttejaan, huolehtivat toiminnallisesta jatkuvuudesta. Astu Labs voi auttaa työnkulkujen suunnittelussa ja käytötapausten luomisessa sekä osaamisen kehittämisessä.
Tekoälylähettiläät (champion, muutoslähettiläs)	Tukevat, kannustavat ja inspiroivat tekoälytyökalujen käyttöä ja uuden työnteon tavan opettelua organisaatiossa. Astu Labsilla on tuotteistettu palvelu tekoälylähettiläiden jatkuvaan tukemiseen, mutta oman organisaation johdon esimerkki ja tuki ovat heidän työssään onnistumisen edellytys.
Käyttäjät	Ovat vastuussa henkilökohtaisten Copilotien ja agenttien vastuullisesta käytöstä. Astu Labs auttaa osaamisen kehittämisessä esimerkiksi AI-viikkokahveilla tai säännöllisin koulutuksin.

Strateginen ohjaus ja vastuut

Strategiset periaatteet

Astu Labs suosittelee, että hallintamallia ohjaavat alla kuvatut neljä strategista periaatetta, jotka määrittävät, millä tavoin tekoälyä ja tekoälyagentteja suunnitellaan, käytetään ja kehitetään. Periaatteet luovat yhteisen arvopohjan tekoälylle ja varmistavat, että sen hyödyntäminen on linjassa sekä organisaation strategian että sääntelyn vaatimusten kanssa.

- **"Human-in-control"** – ihminen säilyttää päätösvallan.
Tekoäly toimii tukena, ei itsenäisenä päätöksentekijänä. Tämä periaate korostaa, että ihmisellä on aina viimeinen sana tekoälyn tuottamien tulosten tulkinnassa ja hyödyntämisessä. Periaate ohjaa koulutusta, käyttöohjeita ja valvontaa siten, että tekoäly nähdään kumppanina, ei korvaajana.
- **Läpinäkyvyys ja auditointi** – jokainen agentti on jäljitettävissä ja dokumentoitu.
Läpinäkyvyys tarkoittaa, että tekoälyn käyttötarkoitus, tietolähteet, päätöksentekoperusteet ja vastuut ovat dokumentoituja ja todennettavissa. Käytännössä tämä toteutuu mm. agenttirekisterillä, hyväksymisprosessilla ja audit traililla, joka tallentaa agentin version, datalähteet ja käyttöhistorian.
- **Arvo- ja sääntelyperustaisuus** – noudatetaan EU AI Actin riskitasoja ja organisaation eettisiä linjauksia.
Tekoälyn tulee olla linjassa sekä organisaation arvojen että yhteiskunnallisten ja oikeudellisten velvoitteiden kanssa. Tämä tarkoittaa, että tekoälyä ei oteta käyttöön vain teknologian mahdollisuuksien perusteella, vaan sen vaikutukset arvioidaan eettisesti, liiketoiminnallisesti ja juridisesti. Tavoitteena on, että tekoälyratkaisut lisäävät luottamusta eivätkä vaaranna sitä.
- **Strateginen integraatio** – tekoäly tukee liiketoimintastrategiaa ja sen tavoitteita.
Tekoäly ei ole erillinen teknologiahanke, vaan olennainen osa liiketoiminnan uudistumista ja strategian toteuttamista. Sen kehittäminen, käyttöönotto ja mittaaminen sidotaan samoihin tavoitteisiin kuin muutkin liiketoimintainvestoinnit. Ilman tätä periaatetta tekoäly jää helposti irralliseksi kokeiluksi – sen sijaan tavoitteena on, että se vie liiketoimintastrategiaa eteenpäin konkreettisesti ja mitattavasti.

4. Tekoöilyn koordinaatioryhmä



Tekoällyn koordinaatioryhmä

Todennäköisesti olet törmännyt muuallakin termiin tai termeihin tekoällyn koordinaatioryhmä, Center of Excellence, tekoälypumppu... Rakkaalla lapsella kun on monta nimeä. Jotta puhumme samaa kieltä, kerromme tässä, mitä termillä tarkoitamme.

Käytämme termiä tekoälyryhmä tarkoittamaan ryhmää, joka varmistaa, että tekoälyhankkeet kytkeytyvät aidosti liiketoimintatavoitteisiin ja tuottavat mitattavaa arvoa. Ryhmä huolehtii tietoturvan, tietosuojan ja vastuullisuuden peruslinjoista, kokoaa yhteen IT:n, HR:n, liiketoiminnan ja kumppaneiden osaamisen sekä estää päällekkäiset hankinnat ja yllättävät kulupiikit.

Ydinryhmän koko voi yrityksessä olla pienikin, tyypillisesti 3–6 henkilöä, mutta sen toimivallan tulee olla suora: se raportoi johtoryhmälle ja kutsuu tarvittaessa asiantuntijoita, kuten tietosuojavastaavan, juristin tai vastuullisuusasiantuntijan.

Mandaatin ydin on koordinoida ja vauhdittaa tekoällyn turvallista, vastuullista ja tuottavaa hyödyntämistä organisaatiossa. Ryhmä priorisoi aloitteet liiketoiminta-arvon ja riskin perusteella, hyväksyy minimitason tietoturva- ja tietosuojavaatimukset, ohjaa käyttöönottoa piloteista tuotantoon sekä seuraa vaikutuksia ja kustannuksia raportointia varten.

Kokoonpanossa kannattaa huomioida se, että liiketoiminta- ja IT-osaaminen yhdistyvät. Tietohallintojohtaja tai liiketoimintajohto johtaa työtä ja raportointia, IT huolehtii työkaluista ja integraatioista, liiketoiminta tuo käyttötapaukset ja ROI-näkökulman, HR tukee muutosta ja koulutusta, ja HR tai talous seuraa kustannuksia.

Niin haluttaessa johtoryhmäkin voi pienemmässä organisaatiossa toimia tekoälyryhmän roolissa. Riippumatta ryhmän kokoonpanosta suosittelemme, että se raportoi suoraan toimitusjohtajalle tai johtoryhmälle. Astu Labsin edustaja voi tarvittaessa tulla tekoällyn koordinaatioryhmän jäseneksi tuomaan ulkopuolista näkemystä ja esittämään niitä kysymyksiä, joita muutoin ehkä tulisi kysytyksi.

5. Tekoälylähettäät (champions, muutosagentit)



Tekoälylähettiläät

Tekoälylähettiläiden tehtävä, jonka kaltaiseen rooliin voit törmätä Microsoftin materiaaleissa termillä Champion, on olla tekoälyn tuomassa murroksessa ja muutoksessa tekoälyn käytön lähettiläs, viestijä, sitouttaja ja käytännön esteiden raivaaja.

Tekoälylähettiläiden toimintaa koskevissa käytännöissä kannattaa painottaa verkostoa, selkeää tukea, valmennusta ja jatkuvaa vuorovaikutusta, jotta työ ei jää yksittäisen henkilön harteille vaan muodostaa organisaation laajuisen muutoksen moottorin.

Jokainen organisaatio sopii itselleen sopivat käytännöt, mutta vakiintuneiden viitekehysten opit kannattaa huomioida. Kun tarkastellaan Kotterin, Proscin ja Bridgesin malleja, jotka muodostavat Astu Labsin kokemusten mukaan hyvän perustan, voidaan tunnistaa suositeltaviksi käytännöiksi:

- Selkeä mandaatti ja tuki: Tekoälylähettiläs tarvitsee johdon selkänöjan ja selkeän roolin määrittelyn - ilman sitä rooli jää helposti epämääräiseksi.
- Verkostoituminen: Muutoslähettiläät toimivat parhaiten verkostona, jossa he voivat jakaa kokemuksia ja vinkkejä. Tämä luo yhteistä linjaa ja vähentää yksinäisyyden tunnetta.
- Säännölliset kohtaamiset: Esim. kuukausittaiset tapaamiset, joissa jaetaan tilannekuvaa, onnistumisia ja haasteita.
- Viestinnän työkalut ja tuki: Käyttöön annetaan valmiita viestintämateriaaleja (FAQ, esityspohjat, tarinat), joita he voivat sovittaa omalle tiimilleen.
- Valmennus ja koulutus: Lähettiläät hyötyvät muutosjohtamisen peruskoulutuksesta (esim. ADKAR, Kotter), jotta heillä on kieltä ja työkaluja muutoksen fasilitointiin.
- Palaute- ja raportointikäytännöt: Kevyt, mutta systemaattinen tapa koota havaintoja johdolle (esim. kerran kuussa "kolme onnistumista, kolme haastetta").
- Palkitseminen ja arvostus: Muutoslähettilään työ on usein näkymätöntä – siksi sen huomioiminen ja palkitseminen lisää motivaatiota.

Astu Labsiltä voi tarvittaessa hankkia tekoälylähettiläsverkostoille vahvaa tukea, osaamisen kehittämistä ja toiminnan määrämuotoisuutta jatkuvan kuukausipalvelun kautta.

6. Käyttö- ja kehitysmalli



Käyttö- ja kehitysmalli

Tekoälyagenttien hallittu elinkaari varmistaa, että jokainen agentti – oli se sitten henkilökohtainen Copilot-apuri tai autonomisempi prosessiagentti – kehitetään, julkaistaan ja ylläpidetään turvallisesti, vastuullisesti ja liiketoimintaa tukevalla tavalla. Elinkaari toimii yhteisenä ”kehysprosessina” kaikille yksiköille ja kehittäjille, ja se on samalla väline tekoälyn riskienhallintaan, laadunvarmistukseen ja jatkuvaan kehittämiseen.

Elinkaari jakautuu viiteen päävaiheeseen:

1. Ideointi ja määrittely
2. Suunnittelu ja kehitys
3. Hyväksyntä ja julkaisu
4. Käyttö ja valvonta
5. Ylläpito, kehittäminen ja poistaminen

Kun kyse on yksinkertaisesta käytöstä, esimerkiksi siitä, että organisaatiossa on tavoitteena helpottaa kiireen tunnetta ja vapauttaa aikaa sälältä ja silpulta laadukkaalle ajattelutyölle kouluttamalla ja luvittamalla käyttäjät luomaan henkilökohtaisia agenteja, ei käyttö- ja kehitysmallista kannata tehdä liian raskasta.

Esimerkiksi Microsoft 365 -ympäristössä agentit noudattavat olemassa olevia käyttöoikeuksia ja ne ovat tekniseltä luonteeltaan melko riskittömiä. Tällöin agentteihin voi suhtautua tapana kerätä käyttäjiltä ideoita ja ratkaisuja arjen rutiineihin ja julkaista parhaat agentit koko organisaation käyttöön.

Laajempi käyttö- ja kehitysmalli tulee kuitenkin luoda viimeistään siinä vaiheessa, kun agenteille siirretään vaativampia tehtäviä tai niiden hoidettavaksi annetaan kokonaisia prosessien työvaiheita.

Käyttö- ja kehitysmalli: Ideointi ja määrittely

Tässä vaiheessa tunnistetaan tarve tekoälyratkaisulle – mitä ongelmaa agentti ratkaisee ja mitä liiketoiminta-arvoa se tuottaa. Ehdotuksen voi tehdä yksittäinen työntekijä, tiimi tai liiketoimintayksikkö.

Tavoite: muuttaa idea hallituksi käyttötapaukseksi.

Keskeiset tehtävät:

- Kuvaillaan agentin tarkoitus, käyttäjät, tietolähteet ja odotettu hyöty.
- Määritellään alustavasti riskitaso (esim. käsitteleekö henkilötietoja tai arkaluontoista dataa).
- Ideat kirjataan agenttirekisteriin (esim. M365 List tai Power BI -näkymä).
- Tekoälyn koordinaatioryhmä arvioi, onko idea liiketoimintastrategian mukainen ja mitä hyväksyntäpolkua se seuraa. Alustavasti ryhmä arvioi myös kustannukset ja riskit.

Kannattaa kuitenkin huomioda se, että kaikki ymmärtävät termit samalla tavalla. Esimerkiksi Microsoft käyttää termiä AI-agentti laveasti tarkoittaen myös sellaisia työtä avustavia tekoälyavustajia, jotka eivät tee autonomisia päätöksiä, eivätkä muodosta suuria riskejä tai kustannuksia. Esimerkiksi Microsoft 365 Copilotin Tutkija ja Avustaja ovat turvallisia käyttää aina tarvittaessa ja ilman erillistä prosessia hyväksyntää varten, kunhan ihminen tarkistaa niiden työn tulokset ja vastaa työstä kuin omastaan.

Kannattaa myös suhtautua henkilökohtaisiin agentteihin oivana keinona kerätä organisaatiossa tietoa siitä, mitä rutiinitehtäviä kannattaa automatisoida. Kannustamme vahvasti jakamaan kokemuksia ja oivalluksia koko tiimin tai organisaation kesken.

Käyttö- ja kehitysmalli: Suunnittelu ja kehitys

Kun idea on hyväksytty, agentti siirtyy kehitysvaiheeseen, jossa se rakennetaan valituilla työkaluilla (esim. Microsoft Copilot Studio, Power Automate, Azure AI Services).

Tavoite: rakentaa toimiva, testattu ja dokumentoitu agentti.

Keskeiset tehtävät:

- Kuvaillaan tietovirrat ja käyttöoikeudet.
- Dokumentoidaan lähdedata, integraatiot ja mallin rajaukset.
- Toteutetaan kehittäjien testaus ja validointi (tarkkuus, tietosuoja, luotettavuus). Tekoälyn koordinaatioryhmä tai sen nimeämä vastuhenkilö tarkistaa, että riskiluokitus ja eettiset periaatteet on huomioitu.

Kehitysvaiheen lopuksi agentilla on oltava:

- kuvattu toiminnallinen ja tekninen rakenne,
- riskinarviointilomake ja DPIA täytettynä,
- ja vastuhenkilö määriteltynä (omistaja).

Käyttö- ja kehitysmalli: Hyväksyntä ja julkaisu

Ennen käyttöönottoa agentti käy läpi hyväksyntäprosessin, joka riippuu sen luokasta (henkilökohtainen, tiimi-, organisaatio- tai autonominen agentti). Tämä vaihe varmistaa, että agentti täyttää tekniset, tietoturvalliset ja eettiset vaatimukset.

Tavoite: julkaista vain hallitusti arvioituja ja hyväksytyjä agentteja.

Keskeiset tehtävät:

- Koordinaatioryhmä tai liiketoimintayksikkö hyväksyy agentin käyttöönoton.
- Tietoturva, tietosuoja ja legal osallistuvat arviointiin tarvittaessa (etenkin organisaatio- ja autonomisissa agenteissa).
- Agentti rekisteröidään ja julkaistaan viralliseen agenttikatalogiin (esim. Copilot-hakemisto tai intranet).
- Käyttäjille viestitään käyttötarkoitus, ohjeet ja vastuukysymykset.

Käyttö- ja kehitysmalli: Käyttö ja valvonta

Julkaisun jälkeen agentti on aktiivisessa käytössä, mutta sitä valvotaan ja mitataan jatkuvasti. Elinkaaren pisin vaihe keskittyy vaikuttavuuden ja turvallisuuden seurantaan.

Tavoite: varmistaa, että agentti toimii oikein, tuottaa arvoa ja pysyy turvallisena.

Keskeiset tehtävät:

- Lokitus ja audit trail: kaikki agentin toiminnot ja versiot tallennetaan.
- Mittarit (esim. käyttömäärät, palautteet, virheiden määrä) kerätään ja analysoidaan.
- Säännöllinen uudelleenarviointi (esim. 6–12 kk välein): tarkistetaan riskit, datalähteet ja toimivuus.
- Käyttäjät voivat antaa palautetta ja ehdottaa parannuksia suoraan rekisterin tai Copilot-katalogin kautta.

Käyttö- ja kehitysmalli: Ylläpito, kehittäminen ja poistaminen

Elinkaaren viimeisessä vaiheessa varmistetaan, että agentti pysyy ajan tasalla tai poistetaan hallitusti, kun sen käyttötarkoitus päättyy.

Tavoite: ylläpitää vain hyödyllisiä, ajantasaisia ja turvallisia agentteja.

Keskeiset tehtävät:

- Päivitykset ja jatkokehitys (uudet datalähteet, parannettu logiikka).
- Versiohallinta ja muutosten dokumentointi.
- Autonomisten agenttien osalta myös toiminnallinen valvonta (esim. ettei tee päätöksiä itsenäisesti väärissä tilanteissa).
- Poistoprosessi: vanhat tai riskialttiit agentit poistetaan käytöstä, ja niiden lokit arkistoidaan.

7. Riskienhallinta ja eettiset periaatteet



Riskienhallinta ja eettiset periaatteet

Tekoälyagenttien riskienhallinnan tavoitteena on varmistaa, että jokainen agentti toimii turvallisesti, läpinäkyvästi ja eettisesti hyväksyttävällä tavalla, riippumatta sen käyttötarkoituksesta tai teknisestä monimutkaisuudesta. Koska tekoäly kykenee oppimaan, tulkitsemaan ja toimimaan itsenäisesti, sen hallinta ei voi perustua pelkästään teknisiin kontrollipisteisiin. Tarvitaan myös eettinen ja vastuuperustainen viitekehys, joka ulottuu suunnittelusta päivittäiseen käyttöön.

Tekoälyagenttien riskienhallinnan perusta on ihmisen vastuussa, läpinäkyvyydessä ja jatkuvassa arvioinnissa. Riskiluokittelu mahdollistaa joustavan mutta turvallisen tavan hyödyntää tekoälyä eri tasoilla aina arkisista avustajista strategisesti tärkeisiin autonomisiin agentteihin. Tämä lähestymistapa tukee organisaation tavoitetta rakentaa luotettava, eettinen ja hallittu tekoälyekosysteemi, joka tuottaa arvoa liiketoiminnalle ilman, että turvallisuus tai vastuu vaarantuvat.

Jokaisen organisaation tulee rakentaa itselleen ja toimintaympäristöönsä soveltuva riskienhallintakäytäntö. Kannattaa kuitenkin huomioida, että riskienhallinta ei pääty hyväksyntään, vaan on jatkuva prosessi, jossa agenttien käyttöä seurataan mittareilla ja auditoinneilla, riskiluokitus tarkistetaan, jos agentin toimintaa muutetaan, ja koordinaatioryhmä raportoi vuosittain tekoälytoiminnan riskiprofiilista johtoryhmälle. Näin organisaatio varmistaa, että tekoälyn käyttö pysyy hallittuna myös sen kehittyessä kohti autonomisempia ja liiketoimintakriittisempiä rooleja.

Pääperiaatteena tulee pitää sitä, että agentin riskitaso kasvaa sen autonomisuuden ja toimintavapauden myötä. Toisin sanoen: mitä enemmän agentti tekee päätöksiä, suorittaa tehtäviä tai käsittelee arkaluonteista dataa ilman ihmisen välitöntä ohjausta, sitä suurempi on riski vääristä tulkinnoista, virheistä tai tietoturvaepoikkeamista.

Tämän vuoksi agentit kannattaa luokitella eri riskiluokkaan, joihin sovelletaan eritasoisia hallintakäytäntöjä, hyväksyntää ja valvontaa. Riskiluokittelun tulee toimia ohjausmekanismina koko agenttien elinkaaren ajan: sen pitää määrittää, millaisia testaus-, hyväksyntä- ja valvontaprosesseja agentti edellyttää, ja miten vastuut jakautuvat.

Seuraavalla sivulla on kuvattu esimerkinomaisesti kolmiluokkainen malli, joka kokemuksemme mukaan soveltuu isolle osalle agenteja käyttävistä organisaatioista.

Riskienhallinta ja eettiset periaatteet

Riskiluokka	Kuvaus	Hallintakäytännöt	Hyväksyntä / Valvonta
1. Low risk – Avustavat agentit	Agentit, jotka eivät tee päätöksiä tai toimenpiteitä, vaan tukevat käyttäjää esimerkiksi tiivistämällä tekstejä, ehdottamalla vastauksia, hakemalla tietoa tai kääntämällä tekstejä.	Automaattiset tietoturva- ja tietosuojakontrollit (DLP, datarajaukset), käyttäjän oma vastuu ja organisaation yleiset tekoälyn käyttöohjeet.	Ei erillistä hyväksyntää. Valvonta esimerkiksi osana normaalia M365 Copilot -käyttövalvontaa.
2. Medium risk – Toimeenpanevat agentit	Agentit, jotka tekevät yksinkertaisia toimintoja (esim. laativat raportteja, siirtävät tietoja, luovat dokumentteja tai käynnistävät prosesseja), mutta aina ihmisen vahvistuksella.	Testaus ja validointi ennen tuotantoa. Logiikan, datalähteiden ja rajojen dokumentointi. Käyttöoikeuksien hallinta ja audit trail -tallennus.	Hyväksyntä tekoälyn koordinaatioryhmältä ennen käyttöönottoa. Jatkuva seuranta käyttö- ja virhelokeista.
3. High risk – Autonomiset agentit	Agentit, jotka toimivat itsenäisesti tai suorittavat monivaiheisia tehtäviä ilman jatkuvaa ihmisen valvontaa (esim. tietojen yhdistäminen, päätöksentekoehdotukset, raportointisilmukat).	Tiukka hyväksymismenettely, riskianalyysi ja eettinen arviointi ennen tuotantoa. Reaaliaikainen valvonta, toimintalokit, hälytykset poikkeavista toiminnoista. Säännöllinen auditointi ja toiminnallinen tarkastus.	Pakollinen hyväksyntä koordinaatioryhmältä, tietoturvalta, tietosuojalta ja legalilta. Reaaliaikainen monitorointi ja raportointi hallintajärjestelmään.

8. Tekninen ja operatiivinen hallinta



Tekninen ja operatiivinen hallinta

Tekoälyn ja tekoälyagenttien tekninen ja operatiivinen hallinta varmistaa, että koko ekosysteemi toimii turvallisesti, valvotusti ja ennustettavasti osana organisaation IT-infrastruktuuria. Tämä osa hallintamallia tuo tekoälyn samalle hallinnan tasolle kuin muutkin kriittiset järjestelmät, mutta tunnistaa myös sen erityispiirteet: jatkuvasti kehittyvät mallit, avoimet rajapinnat ja käyttäjien mahdollisuus luoda omia agentejaan.

Tekninen ja operatiivinen hallinta rakentuu neljästä kokonaisuudesta:

1. arkkitehtuuri ja alustat,
2. tietolähteet ja datan hallinta,
3. turvallisuus- ja valvontamekanismit,
4. sekä operatiiviset prosessit ja jatkuva kehittäminen.

Tekninen ja operatiivinen hallinta muodostavat tekoälyn hallintamallin selkärangan: ne tuovat rakenteen, turvallisuuden ja jatkuvuuden siihen, että agentit voivat toimia luotettavasti osana organisaation arkea. Ne mahdollistavat sen, että, kehitys ja käyttö tapahtuvat hallitussa infrastruktuurissa ja data pysyy sekä suojattuna että jäljitettävänä. Lisäksi valvonta varmistaa, että tekoäly toimii aina ihmisen ohjauksessa ja liiketoiminnan tavoitteiden mukaisesti.

Kukin yllä mainitusta neljästä osa-alueesta on kuvattu lyhyesti seuraavilla sivuilla, mutta hallinta kannattaa rakentaa omaa organisaatiota ja sen tavoitteita tukemaan. Seuraavien sivujen esimerkissä organisaation oletetaan käyttävän Microsoft 365 –ekosysteemiä, koska se on Suomessa de facto standardi. Tarvittaessa Astu Labsin konsultit auttavat hallinnan rakentamisessa myös muissa teknisissä ympäristöissä.

Tekninen ja operatiivinen hallinta

1. Arkkitehtuuri ja alustat

Tekoäly- ja agenttiratkaisut toimivat osana Microsoft 365 -ekosysteemiä, jonka päälle rakentuu laajennuksia ja integraatioita Azure-ympäristön palveluista. Tavoitteena on keskittää kehitys ja käyttö hallittuihin, turvallisiin ja yhteensopiviin alustoihin, jotta kokonaisuus säilyy läpinäkyvänä ja hallittuna.

Keskeiset periaatteet:

- Pääalusta: Microsoft Copilot ja Copilot Studio henkilökohtaisille ja tiimiagenteille.
- Laajennusalustat: Azure OpenAI Service, Cognitive Search, Power Platform ja M365 Graph.
- Kehitysympäristö: vain hyväksytyt ja auditoidut ympäristöt, ei avoimia tai ulkoisia LLM-rajapintoja ilman arviointia.
- Yhtenäinen identiteetti: agentit käyttävät organisaation tunnistautumista (Azure AD / Entra ID).
- Yhteentoimivuus: agentit toimivat M365:n natiivien työkalujen (Teams, Outlook, SharePoint, OneDrive) sisällä ilman erillisiä datareplikointeja.

Tämä arkkitehtuurinen ratkaisu takaa, että tekoälyratkaisut ovat osa organisaation tietoturvatua pilvikokonaisuutta ja hyödyntävät Microsoftin jatkuvasti päivittyviä suojamekanismeja.

Tekninen ja operatiivinen hallinta

2. Tietolähteet ja datan hallinta

Koska tekoälyn laatu riippuu sen käyttämästä datasta, datan hallinta on teknisen hallinnan kriittisin osa.

Tavoitteena on, että agentit käyttävät vain sellaisia tietolähteitä, joiden käyttö on hyväksytty, hallittu ja tietoturvallinen.

Keskeiset periaatteet:

- Sallitut tietolähteet: M365:n natiivit datavarannot (SharePoint, OneDrive, Teams) ja muut erikseen hyväksytyt sisäiset järjestelmät.
- DLP (Data Loss Prevention) -säännöt estävät arkaluonteisen tiedon siirron ja varmistavat, että henkilötiedot pysyvät organisaation rajojen sisällä.
- Tietoluokittelu ja tagitus: dokumentit ja datalähteet luokitellaan luottamustason mukaan (esim. Julkinen / Sisäinen / Luottamuksellinen / Henkilötieto).
- Metatiedot ja jäljitettävyys: kaikki agenttien käyttämät tietolähteet kirjataan agentin dokumentaatioon ja rekisteriin.

Näin varmistetaan, että tekoälyn käyttö pysyy läpinäkyvänä ja että riskiluokituksen mukaiset agentit toimivat vain niille hyväksytyissä tietoympäristöissä.

Tekninen ja operatiivinen hallinta

3. Turvallisuus ja valvonta

Tekninen hallinta ei ole pelkästään infrastruktuuria, vaan se on ennen kaikkea toiminnan jatkuvaa valvontaa ja kontrollia.

Jokaiselle agentille määritetään sen riskiluokkaa vastaavat tekniset valvontamekanismit, jotka suojaavat väärinkäytöksiltä, virheiltä ja luvattomalta datankäytöltä.

Keskeiset mekanismit:

- Käyttölokitus ja audit trail: kaikki agentin suorittamat toiminnot, päätökset ja tiedonhaut tallennetaan automaattisesti.
- Reaaliaikainen valvonta (monitorointi): etenkin autonomisille agenteille – hälytykset poikkeavista toiminnoista, kuten suurista tiedonsiirroista tai epätyypillisestä ajastetusta toiminnasta.
- Tietoturvainventointi: agentit sisällytetään organisaation tietoturva-arkkitehtuuriin ja säännölliseen riskikartoitukseen.
- Autentikointi ja käyttöoikeudet: agentit eivät koskaan toimi laajemmilla oikeuksilla kuin niiden käyttötarkoitus edellyttää ("least privilege" -periaate).
- Automaattiset suojausmekanismit: DLP, Defender for Cloud Apps, sekä M365 Purview -säännöt tietovuotojen ja väärinkäytösten havaitsemiseksi.

Näiden avulla varmistetaan, että tekoälytoiminta pysyy hallinnassa myös silloin, kun agenttien määrä ja autonomia kasvavat.

Tekninen ja operatiivinen hallinta

4. Operatiiviset prosessit ja jatkuva kehittäminen

Tekninen hallinta kytkeytyy päivittäiseen operatiiviseen tekemiseen. Tekoälyratkaisut eivät ole kertaluonteisia projekteja, vaan jatkuvasti elävä osa organisaation digitaalisia prosesseja. Siksi operatiivinen hallinta rakentuu jatkuvuuden ja parantamisen periaatteelle.

Keskeiset käytännöt:

- Säännöllinen valvonta ja raportointi: koordinaatioryhmä tarkastelee agenttien käyttö- ja valvontaraportteja säännöllisesti (esim. kvartaalittain).
- Versiohallinta ja dokumentointi: kaikki muutokset agentin logiikkaan tai käyttöoikeuksiin dokumentoidaan.
- Red Team -testaus ja stressitestit: erityisesti autonomiset agentit altistetaan hallituille simulaatioille, joilla arvioidaan niiden reagointia poikkeustilanteissa.
- Poikkeamien hallinta: tietoturva-, tietosuoja- ja toiminnalliset poikkeamat käsitellään osana normaalia incident management -prosessia.
- Deprekoiminen ja poistaminen: käytöstä poistettavat agentit arkistoidaan hallitusti ja niiden lokit säilytetään määrääjän.

Jatkuva seuranta, palaute ja auditoinnit varmistavat, että tekoälyratkaisut pysyvät ajan tasalla, turvallisina ja linjassa liiketoiminnan tavoitteiden kanssa.

9. Viestintä, koulutus ja muutosjohtaminen



Viestintä, koulutus, muutosjohtaminen

Tekoälyn ja tekoälyagenttien hallintamallissa ei kyse ole pelkästä ohjeistuksesta tai käytännöistä. Oikein rakennettu ja mitoitettu hallintamalli on muutoksen johtamisen väline. Tekoäly muuttaa työn tekemisen tapoja, rooleja ja päätöksentekoa, ja siksi hallintamallin onnistuminen riippuu siitä, miten hyvin koko organisaatio ymmärtää, hyväksyy ja omaksuu uuden toimintatavan. Viestintä, koulutus ja muutosjohtaminen muodostavat tämän muutoksen inhimillisen perustan: ne rakentavat luottamusta, osaamista ja yhteistä kieltä tekoälyn ympärille.

Tekoälyn käyttöönotossa viestintä on yhtä tärkeää kuin tekninen toteutus. Sen tehtävänä on varmistaa, että kaikki organisaation tasot ymmärtävät, miksi tekoälyä otetaan käyttöön, miten se toimii ja mitä vastuita siihen liittyy. Viestinnällä hallitaan odotuksia, ehkäistään pelkoja ja luodaan luottamusta uuden teknologian käyttöön.

Viestinnän ja muutosjohtamisen eskeiset periaatteet ja toimenpiteet:

- Yhteinen narratiivi: tekoäly ei ole uhka vaan väline, joka vapauttaa aikaa ja vahvistaa osaamista.
- Johdon näkyvä sitoutuminen: hallitus, johtoryhmä ja esihenkilöt viestivät johdonmukaisesti tekoälyn merkityksestä osana strategiaa.
- Säännöllinen sisäinen viestintä: intranet, uutiskirjeet ja Teams-kanavat kertovat uusista agenteista, parhaista käytännöistä ja onnistumisista.
- Avoimuus ja palautekanavat: työntekijöillä on matala kynnys kysyä, raportoida huolia tai ehdottaa parannuksia tekoälyn käyttöön liittyen.

Hyvä viestintä tekee tekoälystä yhteisen asian, ei IT-projektin.

Viestinnän lisäksi tärkeässä osassa on osaamisen kehittäminen ja turvallinen kokeilukulttuuri. Tekoälyn vastuullinen käyttö edellyttää, että käyttäjillä on ymmärrys sekä mahdollisuuksista että rajoista. Koulutusten tarkoituksena on varmistaa, että jokainen työntekijä osaa käyttää tekoälyä turvallisesti, eettisesti ja tuottavasti omassa roolissaan. Astu Labsin kokemuksen perusteella kaikille on hyvä tarjota yleinen tekoälykoulutus, joka kattaa myös EU:n AI Actin edellyttämän tekoälyn lukutaidon, mutta mitattavat hyödyt saadaan aikaan roolipohjaisilla koulutuksilla.

Viestintä, koulutus, muutosjohtaminen

Tekoälyn käyttöönotto muuttaa työtä, mutta sen on tapahduttava ihmislähtöisesti ja hallitusti. Muutosjohtamisen tavoitteena on tukea työntekijöitä sopeutumaan uuteen rooliin, jossa tekoäly on osa päätöksentekoa, viestintää ja tiedonhallintaa.

Keskeiset painopisteet:

- Osallistaminen: työntekijät ja tiimit otetaan mukaan kehitykseen jo varhaisessa vaiheessa. Näin syntyy omistajuutta ja luottamusta.
- Kokeilukulttuuri: hallittu "sandbox" –ympäristö, jossa voidaan testata uusia agentteja ja oppia turvallisesti.
- Tukirakenteet: tekoälyn koordinaatioryhmä ja tekoälylähettiläs-verkosto tarjoavat jatkuvaa tukea, ohjeistusta ja sparrausta.
- Psykologinen turvallisuus: korostetaan, että virheet ovat osa oppimista – tärkeintä on, että ne havaitaan, ja niistä opitaan.

Tekoälyyn liittyvä muutos on organisaatiokulttuurin muutos, jossa työ, oppiminen ja johtaminen kehittyvät rinnakkain uuden teknologian kanssa.

Jotta viestinnän, koulutuksen ja muutosjohtamisen vaikutuksia voidaan arvioida, niiden tueksi määritellään selkeät mittarit ja seurantamekanismit. Esimerkkejä mittareista ovat koulutusten osallistumisaste ja palautteet, henkilöstön tekoälyosaamisen itsearvioinnit, Copilotin ja agenttien käyttöasteet eri yksiköissä ja raportoidut riskit tai tietoturvapoikkeamat. Kokemuksemme perusteella kannattaa myös seurata tunnetaitojen, psykologisen turvallisuuden ja johtoa kohtaan koetun luottamuksen kehittymistä.

Viestintä, koulutus ja muutosjohtaminen varmistavat, että tekoälyn hallintamalli ei jää ohjeistukseksi paperilla, vaan muuttuu osaksi organisaation toimintakulttuuria. Ne tekevät tekoälystä hallitun, ymmärretyn ja hyväksytyn osan arkea – ja mahdollistavat sen, että jokainen työntekijä voi toimia vastuullisesti ja luottavaisesti tekoäly rinnallaan.

Astu Labs on erikoistunut todellisen muutoksen aikaansaamiseen tekoälyn käyttöä tuotaessa osaksi organisaation arkea. Tekoälyssä on kyse enemmän uudesta työnteon tavasta kuin ohjelmistosta tai teknisestä ratkaisusta. Koska aihealue on laaja, suosittelemme tutustumaan Tekoälykyvykäs henkilöstö –palveluumme oheisen QR-koodin kautta.



10. Hallintamallin jatkuva kehittäminen



Hallintamallin jatkuva kehittäminen

Tekoälyn ja tekoälyagenttien hallintamalli ei ole staattinen asiakirja, vaan elävä ohjausjärjestelmä, joka kehittyy teknologian, lainsäädännön ja organisaation omien kokemusten mukana. Sen tarkoitus on mahdollistaa hallittu oppiminen ja jatkuva parantaminen, jotta tekoälyn käyttö pysyy turvallisena, tehokkaana ja strategisesti merkityksellisenä myös tulevaisuudessa.

Tekoälyn kehitystahti on poikkeuksellisen nopea, olemme siirtymässä lineaarisesta kehityksestä eksponentiaaliseen. Microsoft Copilotin, Azure AI -palveluiden ja muiden tekoälyratkaisujen ominaisuudet muuttuvat kuukausitasolla, ja samalla EU:n tekoäylainsäädäntö (AI Act) ja viranomaisohjeet täsmentyvät jatkuvasti.

Siksi hallintamallin on oltava iteratiivinen eli rakenteeltaan sellainen, että sitä voidaan päivittää säännöllisesti ilman raskaita muutosprosesseja. Sen tulee olla oppiva ja pohjautua käytännön kokemuksiin ja palautteeseen. Lisäksi kannustamme luomaan mallista yhteistyöhön perustuvan, jolloin kehitys tapahtuu liiketoiminnan, IT:n, HR:n, tietoturvan ja legalin yhteisenä työnä. Tämä varmistaa, että hallintamalli pysyy relevanttina sekä liiketoiminnan että sääntelyn näkökulmasta.

Hallintamallin ylläpidosta ja kehittämisestä vastaa tekoälyn koordinaatioryhmä, joka toimii jatkuvana ohjaus- ja kehitysfoorumina. Ryhmä kokoontuu säännöllisesti (esim. neljännesvuosittain) tarkastelemaan mallin toimivuutta ja tunnistamaan kehitystarpeita. Ryhmän keskeiset tehtävät ovat: seurata teknologian, riskien ja sääntelyn muutoksia, arvioida agenttien käyttödataa, riskejä ja palautetta, päivittää prosesseja, rooleja ja vastuuta tarvittaessa, sekä raportoida hallintamallin tilasta ja kehityksestä johtoryhmälle säännöllisesti.

Kehitys tulee perustua faktapohjaiseen arviointiin eli mallia ei muuteta mielipiteiden, vaan havaittujen tarpeiden ja mittarien perusteella. Suosittelemme noudattamaan esimerkiksi PDCA-mallia, jossa tarvittava muutos suunnitellaan, toteutetaan, tarkistetaan ja tarvittaessa korjataan. Suosittelemme myös, että hallintamallin ja tekoälyn koordinaatioryhmän toiminnan tarkastelu asetetaan osaksi organisaation vuosikelloa ja tuodaan osaksi muuta määrämuotoista johtamista.

Hallintamallin jatkuva kehittäminen varmistaa, että tekoälytoiminta ei jähmety, vaan kehittyy rinnakkain organisaation strategian ja toimintaympäristön kanssa. Se tekee hallinnasta elävän prosessin — ei valvontamekanismia, vaan oppimisen ja sopeutumisen järjestelmän, joka mahdollistaa vastuullisen, tehokkaan ja ihmislähtöisen tekoälyn hyödyntämisen pitkällä aikavälillä.

Olemme täällä sinua varten!

sales@astulabs.fi

045 279 2794



*AI isn't only about technology - it's a new way of working.
It calls for new skills, fresh thinking, and
a culture that embraces change.*



"Astu Labs was founded because the true power of AI lies not in technology, but in a culture built on employees' daily choices."



Lenni Laukkanen



- Runner, cyclist, adventurer.
- Professional in business management and technology. I have developed the operations and competitiveness of companies with the help of technology over three different decades.
- Keywords of my competence: ISO 9001, ISO 27001, ISO 27701, NIS2, DORA, Lean, ITIL.



How do we do it?

Kasvuohjelma

Ongoing Partnership

- AI-enabled staff
- AI-enabled governance
- AI-capable management team

Kiihdyttämö

On-Demand Expertise

- AI consulting incl. processes and automation, training, responsible artificial intelligence, strategies, management systems and regulation
- Workshops and studies

With experience spanning dozens of organizations, we've driven impactful technology and transformation projects across industries — from forestry to financial services.



References from our experts

"Lenni sees artificial intelligence as an enabler and an opportunity to free up working time for creative work: humans act as masters, artificial intelligence as servants. Lenni is able to help with ideas and views and, above all, spar with things moving forward."

ANDERS DAHLQVIST, Chief Information Officer

"In dealing with Janne, clarity and solution-orientation stood out. Cooperation has always been nice and smooth, and we have also been able to trust that the promised work will be carried out as agreed and on time."

JULIA MAUNOLA, IT Manager

"Jouni is a reliable, professional and highly competent person who has always been trusted. Regardless of the situation, he is always ready to help you find the right solution."

JONATHAN GASKIN, Head of IT

References from our experts

"As a customer, I have worked with Lenni for several years (IT matters). Lenni knows how to listen and genuinely looks for suitable solutions for the customer's needs. In particular, I have also remembered the good service attitude when the situation requires stretching. He is uncomplicated and easy to work with."

JANNE ELO, CEO

"Lenni has been an important partner for me for years and I can warmly recommend him: Lenni is a very competent and reliable professional who brings significant value to all cooperation situations. His expertise and commitment to understanding and solving the customer's needs is exemplary. Lenni is always ready to help and find the best solutions, which makes cooperation with him smooth and productive."

TUUKKA SOINI, Director of Development

Company Type	Main activity	Nature of the product	The role of AI	Examples
ISV/Consulting	Software development as a service	Customer-specific projects	Possible part of projects	 SOLITA  vincit  tietoenvy
SaaS company	Development of your own SaaS products	Finished products, not customized	AI as an additional feature	 salesforce  HubSpot
AI company	Develop AI models and AI products	AI technology is a core product	AI is strategy and business	 OpenAI ANTHROPIC  AMD AI SILO
IT partner	Supports in technical deployment, licenses and infrastructure	Work and bearing investments and risks on behalf of the customer	AI included in licenses sold, support for AI tools	 TIETOKESKUS  Dustin  TAHTO
AI partner	Helps with implementation, culture and competence development	Changes in working methods and operating culture	AI is an "object of scrutiny" or a strategic tool	 astu twoday

astu



AI CAPABILITY BUILDER, WORK-LIFE FIXER