Tampereen yliopisto

Sara Heimola

VAKUUTUSYHTIÖIDEN JA PANKKIEN RISKIENHALLINTA EU:N TEKOÄLYASETUKSEN (AI ACT) NÄKÖKULMASTA

Johtamisen ja talouden tiedekunta

Pro Gradu -tutkielma

Toukokuu 2026

TIIVISTELMÄ

Sara Heimola: Vakuutusyhtiöiden ja pankkien riskienhallinta EU:n tekoälyasetuksen (AI Act) näkökulmasta
Ohjaaja: Lasse Koskinen
Pro gradu -tutkielma
Tampereen yliopisto
Kauppatieteiden tutkinto-ohjelma, Vakuutustiede

Toukokuu, 2026

Tekoäly on nostanut suosiotaan viime vuosina ja se tuottaa monenlaisia taloudellisia, ympäristöön liittyviä ja yhteiskunnallisia hyötyjä kaikilla teollisuudenaloilla ja kaikessa sosiaalisessa toiminnassa. Tekoäly tulee mullistamaan eri toimialojen toimintaympäristöjä ja tuoden mukanaan merkittäviä lainsäädäntömuutoksia. EU on tunnistanut tekoälyn nopean kehityksen ja nähnyt tarpeelliseksi luoda sitä koskevaa sääntelyä.

Finanssisektori on koko talouden vakauden kannalta keskeinen, ja tekoälyn vastuullinen käyttö on ratkaisevaa kuluttajansuojan sekä luottamuksen säilyttämiseksi. Vaikka pankit ja vakuutusyhtiöt toimivat samalla sektorilla, niiden riskienhallintajärjestelmät poikkeavat toisistaan. Vakuutusyhtiöiden riskienhallinta keskittyy perinteisesti aktuaarisiin ja vakuutusteknisiin riskeihin sekä asiakasdatan hyödyntämiseen, kun taas pankeilla painopiste on luottoriskeissä, markkinariskeissä ja vakavaraisuusvaatimuksissa. EU:n tekoälyasetus (AI Act) voi korostaa näitä eroja entisestään: vakuutusyhtiöissä tekoäly liittyy erityisesti riskien arviointiin, hinnoitteluun ja vahinkojen käsittelyyn, kun taas pankeissa sen rooli korostuu luotonmyönnössä, petosten havaitsemisessa ja asiakasprofiloinnissa.

Tutkielman tavoitteena on tutkia, miten uusi tekoälyasetus AI Act suhteutuu pankki- ja vakuutussektorin olemassa olevaan sektorikohtaiseen sääntelyyn sekä millaisia eroavaisuuksia sektoreiden välille syntyy asetuksen käyttöönoton yhteydessä. Tutkielma on laadullinen ja analysoitava aineisto perustuu primääri- ja sekundääriaineistoon. Aineisto analysoidaan teoriaohjaavan sisällönanalyysin avulla.

Tutkimustulokset osoittavat, että finanssisektori tällä hetkellä suosii matalan riskin käyttötapauksia, mutta korkean riskin käyttötapauksia on käytössä ja niiden käyttö tulevaisuudessa lisääntyy. AI Actin velvoitteet sulautuvat luonnollisesti nykyiseen sääntely-ympäristöön ja täydentää olemassa olevaa säädäntöä. Riskienhallinnan näkökulmasta näkyvimpiä muutoksia ovat olleet erilaisten toimintamallien päivitys tekoälyjärjestelmien kohdalla.

Avainsanat: AI Act, riskienhallinta, tekoäly,

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

TEKOÄLYN KÄYTTÖ OPINNÄYTTEESSÄ

Opinnäytteessäni on käytetty tekoälysovelluksia:

☐ Ei
☒ Kyllä

Ilmoitukseni mukaan olen käyttänyt opinnäytteessäni tutkielmaprosessin aikana seuraavia tekoälysovelluksia:

Tekoälysovellusten nimet ja versiot: ChatGPT -5.4 ja ChatGPT 5.5

Käyttötarkoitus: Tekoälyä on käytetty lähteiden etsimiseen ja niiden sisällön tulkitsemineen, lähteiden kääntämiseen ja tekstin kieliopilliseen tarkastamiseen

Osiot, joissa tekoälyä on käytetty: Tekoälyä on käytetty teoriaosuudessa lähteiden etsimiseen ja näiden kääntämiseen, koko tekstin osalta kirjoitusasun tarkastukseen

Olen tietoinen siitä, että olen täysin vastuussa koko opinnäytteeni sisällöstä, mukaan lukien osat, joissa on hyödynnetty tekoälyä, ja hyväksyn vastuun mahdollisista eettisten ohjeiden rikkomuksista.

SISÄLLYSLUETTELO

1 JOHDANTO 6

1.1 Aihealueen esittely ja merkitys 6

1.2 Aikaisempi tutkimus ja kirjallisuus 8

1.3 Tutkielman tavoitteet, tutkimusongelmat ja rajaukset 10

1.4 Tieteenfilosofiset lähtökohdat 12

1.5 Tutkimusmenetelmät ja -aineisto 15

1.6 Keskeisten käsitteiden määrittely 18

1.7 Tutkielman teoreettinen viitekehys ja rakenne 20

2 FINANSSISEKTORIN RISKIENHALLINTA 23

2.1 Riskienhallinnan perusta finanssialalla 23

2.2 Vakuutusyhtiöiden riskienhallinta 24

2.3 Pankkien riskienhallinta 28

2.3.1 Basel-kehikko 31

2.3.2 CRD-direktiivi ja riskienhallinta 33

2.3.3 CRR-asetus ja sisäiset mallit 34

2.4 Pankkien ja vakuutusyhtiöiden riskienhallinnan eroavaisuudet 35

3 EU:N TEKOÄLYASETUS (AI ACT) SÄÄNTELYKEHYKSENÄ 37

3.1 Tausta ja tavoitteet 37

3.2 Riskiperusteinen luokittelu 38

3.3 Suuririskisen tekoälyjärjestelmien velvoitteet 39

3.4 Suuririskiset tekoälyjärjestelmät finanssialalla 42

3.5 AI Actin vaikutukset finanssisektorille ja asetuksen noudattamisen edellytykset 44

4 INSTITUTIONAALINEN TEORIA 47

4.1 Institutionaalisen teorian lähtökohdat 47

4.2 Legitimaatio 49

4.3 Vakuutusyhtiöiden ja pankkien vertailu institutionaalisesta näkökulmasta 51

5 FINANSSISEKTORIN TEKOÄLYKÄYTTÖTAPAUKSET JA VIRANOMAISOHJEISTUKSET 53

5.1 Aineiston kuvaus 53

5.2 Tekoälyn käyttötapaukset finanssisektorilla 54

5.3 AI Actin suhde olemassa olevaan sektorisääntelyyn 56

6 AI ACTIN TOIMEENPANO JA KÄYTTÖ ORGANISAATIOISSA 59

6.1 Aineiston esittely 59
6.2 Tekoälyn käyttötavat tarkastelluissa organisaatioissa 60
6.3 Tekoälyn käyttöönotto tarkastelluissa organisaatioissa 63
6.4 AI Actin vaikutukset riskienhallintaan tarkastelluissa organisaatioissa 68
7 YHTEENVETO JA JOHTOPÄÄTÖKSET 74
7.1 Tutkimuskysymyksiin vastaaminen ja johtopäätökset 74
7.2 Tutkielman arviointi 81
8 LÄHTEET 85
9 LIITTEET 91
Liite 1: Haastattelurunko 91

1 JOHDANTO

Tutkielman johdantoluku luo perustan työn ymmärtämiselle ja kokonaisuuden hahmottamiselle. Luvun keskeisenä tarkoituksena on esitellä tutkielman lähtökohdat ja periaatteet, joiden avulla lukija saa ensikosketuksen aiheeseen ja sen toteutusprosessiin. Johdanto alkaa tutkielman aihealueen esittelyllä sekä sen merkityksen perustelulla. Tämän jälkeen tarkastellaan aiempaa tutkimusta ja kirjallisuutta, joka liittyy aihepiiriin. Lukijan orientoinnin kannalta olennainen osa johdantoa on tutkimustavoitteiden ja -ongelmien määrittely, minkä jälkeen kuvataan tutkielman tieteenfilosofiset lähtökohdat sekä käytetyt tutkimusmenetelmät ja aineisto. Johdantoluvussa avataan lisäksi keskeiset käsitteet ja lopuksi esitellään tutkielman teoreettinen viitekehys sekä työn rakenne.

1.1 Aihealueen esittely ja merkitys

Tekoäly on nostanut suosiotaan viime vuosina ja se tuottaa monenlaisia taloudellisia, ympäristöön liittyviä ja yhteiskunnallisia hyötyjä kaikilla teollisuudenaloilla ja kaikessa sosiaalisessa toiminnassa (European Comission, 2026). Tekoäly tulee mullistamaan eri toimialojen toimintaympäristöjä ja tuoden mukanaan merkittäviä lainsäädäntömuutoksia.

EU on tunnistanut tekoälyn nopean kehityksen ja nähnyt tarpeelliseksi luoda sitä koskevaa sääntelyä. EU:n tekoälyasetuksen johdanto-osassa (kohdat 4, 5 ja 8) todetaan, että tekoäly voi hyödyistään huolimatta aiheuttaa olosuhteitten mukaan riskejä ja vahingoittaa unionin oikeudella suojattuja yleisiä etuja ja perusoikeuksia. Tällainen vahinko voi olla aineellista tai aineetonta, esimerkiksi fyysistä, psykologista, yhteiskunnallista tai taloudellista. Tämän vuoksi tarvitaan unionin oikeudellinen kehys, joka vahvistaa tekoälyä koskevat yhdenmukaistetut säännöt. Kehyksen tavoitteena on edistää tekoälyn kehittämistä, käyttöä ja käyttöönottoa sisämarkkinoilla sekä samalla varmistaa unionin oikeudessa tunnustettujen ja suojattujen yleisten etujen, kuten terveyden, turvallisuuden, demokratian, oikeusvaltion ja ympäristön, sekä perusoikeuksien korkea taso.

EU:n tekoälyasetus (AI Act) hyväksyttiin vuonna 2024 ja jonka täysimääräinen soveltaminen alkaa asteittain vuosina 2025–2027. AI Act on maailman ensimmäinen laaja tekoälyä koskeva sääntelykehys, joka koskee Euroopan alueella toimivia yrityksiä ja organisaatioita. Tekoälysäädös vahvistaa riskiperusteiset säännöt tekoälyn kehittäjille (European Comission, 2026). AI Act perustuu riskiperustaiseen lähestymistapaan: mitä suurempi riski tekoälyjärjestelmällä on yksilöiden oikeuksiin, turvallisuuteen tai yhteiskuntaan, sitä tiukemmat vaatimukset järjestelmälle asetetaan. Tekoälysäädös muodostaa osan laajempaa toimenpidekokonaisuutta, jonka tavoitteena on edistää luotettavan tekoälyn kehittämistä. Kokonaisuuteen sisältyvät myös tekoälyn innovointipaketti, tekoälytehtaiden perustaminen sekä koordinoitu tekoälysuunnitelma (European Commission, 2026).

Finanssisektori on luonteeltaan yhteiskunnallisesti merkittävä toimiala, minkä vuoksi sen toimintaa valvotaan tiukasti. Näin ollen myös tekoälyn käyttöön kohdistuu vaatimuksia. Vakuutussektorilla tekoälyä hyödynnetään riskinvalinnassa, hinnoittelussa, korvauskäsittelyssä ja petosten havaitsemisessa ja se mainitaan yhä useammin operatiivisena riskinä. Pankit ovat käyttäneet tekoälyä hyödyksi muun muassa asiakkaiden profilointiin, petosten havaitsemiseen, asiakastukeen sekä luottoriskin mallintamiseen (EIOPA, 2025; EBA, 2024). Tekoälyn sivutuotteena hyötyjen ohella syntyy myös riskejä, joiden hallitsemiseksi on luotu sääntelyä. Sääntely itsessään muodostaa yrityksille ja organisaatioille lisähaasteen, joka voi näyttäytyä esimerkiksi operatiivisena riskinä. Suurimmat riskit liittyvät erityisesti kustannuksiin, kilpailukykyyn ja sääntelyn monimutkaisuuteen.

Finanssisektori on koko talouden vakauden kannalta keskeinen, ja tekoälyn vastuullinen käyttö on ratkaisevaa kuluttajansuojan sekä luottamuksen säilyttämiseksi. Lainsäädännön noudattaminen on elintärkeää alan toimijoille, sillä jo pienikin virhe voi horjuttaa luottamusta ja johtaa merkittäviin seurauksiin. Vaikka pankit ja vakuutusyhtiöt toimivat samalla sektorilla, niiden riskienhallintajärjestelmät poikkeavat huomattavasti toisistaan. Vakuutusyhtiöiden riskienhallinta keskittyy perinteisesti aktuaarisiin ja vakuutusteknisiin riskeihin sekä asiakasdatan hyödyntämiseen, kun taas pankeilla painopiste on luottoriskeissä, markkinariskeissä ja vakavaraisuusvaatimuksissa (Basel III). EU:n tekoälyasetus (AI Act) voi korostaa näitä eroja entisestään: vakuutusyhtiöissä tekoäly liittyy erityisesti riskien arviointiin, hinnoitteluun ja vahinkojen käsittelyyn, kun

taas pankeissa sen rooli korostuu luotonmyönnössä, petosten havaitsemisessa ja asiakasprofiloinnissa.

1.2 Aikaisempi tutkimus ja kirjallisuus

Aikaisempaa tutkimusta koskien pankki – ja vakuutussektorin riskienhallintaa löytyy laajalti, johtuen niiden yhteiskunnallisesta roolista ja historiasta. Tutkimusta AI Actin soveltamista näiden sektoreiden välillä ei löydy, koska kyseessä on uusi asetus, mitä ei kokonaisuudessaan ole otettu käyttöön. Olemassa oleva kirjallisuus keskittyy etenkin siihen, mitkä finanssisektorin tekoälyn käyttötapaukset ovat ja miten niiden riskejä tulisi hallita ottaen huomioon kaikki velvoitteet.

Maria Lucia Passador (2024) tarkastelee tutkimuksessaan *AI in the Vault: AI Act's Impact on Financial Regulation* EU:n AI Actin vaikutuksia pankki- ja rahoitussektorin sääntelyyn. Tutkimus keskittyy tekoälyteknologian ja finanssialan vakavaraisuusvalvonnan rajapintaan sekä analysoi, miten uusi sääntelykehys vaikuttaa tekoälysovellusten hallintaan ja valvontaan rahoitusalalla. Passador korostaa erityisesti EU:n AI Office -toimiston ja AI Board -lautakunnan roolia tekoälysovellusten valvonnassa ja sääntelyn toimeenpanossa.

Tutkimuksessa tarkastellaan yleisellä tasolla AI Actin tuomia muutoksia finanssisektorin sääntelyyn. Passador käsittelee muun muassa pankkien riskienhallintaa ja sitä, miten tekoälyä hyödyntävät järjestelmät sijoittuvat olemassa oleviin sääntelyrakenteisiin. Vakuutussektoria tutkimuksessa ei kuitenkaan tarkastella erikseen. Passadorin mukaan AI Act muodostaa merkittävän uuden sääntelykehyksen finanssialalle: se lisää tekoälysovellusten läpinäkyvyyttä ja turvallisuutta sekä auttaa hallitsemaan tekoälyn aiheuttamia riskejä, mutta samalla se tuo finanssiyrityksille uusia compliance-vaatimuksia.

Hacker tarkastelee tutkimuksessaan (2025), millaisia tekoälyn käyttötapauksia finanssisektorilla tulee huomioida erityisesti EU:n AI Actin näkökulmasta. Tutkimuksessa käsitellään muun muassa luottoluokitusta (credit scoring) ja vakuutusten underwriting-prosesseja, joissa tekoälyä hyödynnetään automatisoidussa

päätöksenteossa. Tarkastelun keskiössä ovat AI Actin vaikutukset finanssisektorin automatisoitujen päätöksentekojärjestelmien sääntelyyn. Tutkimuksessa analysoidaan esimerkiksi sitä, mitä pankkien on huomioitava käyttäessään tekoälyjärjestelmiä luottokelpoisuuden arvioinnissa.

Vakuutussektorin osalta tutkimuksessa tarkastellaan, miten tekoälyjärjestelmien käyttö vaikuttaa compliance-toimintojen ja riskienhallinnan suhteeseen sekä millaisia päällekkäisyyksiä voi syntyä suhteessa olemassa oleviin sääntelykehyksiin, kuten Solvenssi II -järjestelmään (Hacker, 2025). Hackerin mukaan AI Act lisää finanssisektorilla sääntelyä ja compliance-vaatimuksia, mutta samalla se voi vahvistaa luottamusta tekoälyjärjestelmiin ja siten tukea riskienhallinnan kehitystä. Lisäksi sääntelyllä voi olla kansainvälinen vaikutus, koska EU-markkinoilla toimivien yritysten on noudatettava AI Actia riippumatta niiden kotipaikasta

Golpayegani esittelee tutkimuksessaan (2025) AI Risk Ontology (AIRO) -mallin, joka kuvaa korkean riskin tekoälyjärjestelmiin liittyvää tietoa EU:n AI Act -ehdotuksen sekä ISO 31000 -riskienhallintastandardien pohjalta. Mallin avulla voidaan tunnistaa korkean riskin tekoälyjärjestelmiä, ylläpitää ja dokumentoida niihin liittyvää riskitietoa, toteuttaa vaikutusarviointeja sekä tukea sääntelyn edellyttämää vaatimustenmukaisuutta. Tutkimuksessa havainnollistetaan AIRO-mallin toimivuutta mallintamalla reaalimaailman tapauksia AIAAIC-tietokannasta ja tuottamalla niistä dokumentaatiota EU:n AI Act -ehdotuksen mukaisesti

Tutkimuksen tavoitteena on kehittää ontologinen tietomalli, jonka avulla voidaan kuvata tekoälyjärjestelmiä, tunnistaa niihin liittyviä riskejä sekä dokumentoida riskienhallintaa tavalla, joka tukee AI Actin sääntelyn noudattamista. Golpayeganin mukaan tekoälyyn liittyvä riskienhallinta edellyttää yhtenäisiä käsitteitä, standardoituja dokumentaatiokäytäntöjä sekä teknisiä työkaluja, joiden avulla sääntelyn vaatimuksia voidaan käytännössä toteuttaa.

Tutkimuksessaan *Enterprise Risk Management and Solvency II: The System of Governance and the Own Risk and Solvency Assessment* (2020) Durán analysoi, miten Solvenssi II -sääntely on vaikuttanut vakuutusyhtiöiden kokonaisvaltaiseen riskienhallintaan. Tutkimuksessa tarkastellaan erityisesti hallintojärjestelmän (system of

governance) kehitystä sekä sitä, miten ORSA-prosessi (Own Risk and Solvency Assessment) toimii käytännössä vakuutusyhtiöissä.

Tutkimuksen tulosten mukaan Solvenssi II on parantanut vakuutusyhtiöiden riskienhallintaa Euroopassa. Lisäksi ORSA-prosessi koetaan hyödylliseksi työkaluksi, sillä sen tuottamat hyödyt nähdään suurempina kuin sen toteuttamisesta aiheutuvat kustannukset.

Hacker & Eber (2025) tutkimuksessaan ”The Future of credit underwritin and insurance under the EU AI Act: Implication for Europé and Beyond”, tutkii mihin riskiluokkaan luottopisteytys ja underwriting määritellään tekoälyasetuksessa, mitä finanssitoimijoiden tulee ottaa huomioon ja miten olemassa oleva sääntely sopii AI Actin kanssa.

1.3 Tutkielman tavoitteet, tutkimusongelmat ja rajaukset

Tämän pro gradu -tutkielman tavoitteena on tarkastella vertailevasti, miten uusi tekoälyasetus AI Act suhteutuu pankki- ja vakuutussektorin olemassa olevaan sektorikohtaiseen sääntelyyn sekä millaisia eroavaisuuksia sektoreiden välille syntyy asetuksen käyttöönoton yhteydessä. Näihin eroihin vaikuttavat erityisesti se, millaisia tekoälyn käyttötapauksia kullakin sektorilla painotetaan, sekä se, miten sektorikohtaiset viranomaisohjeistukset suuntaavat asetuksen tulkintaa ja toimeenpanoa.

Pankki- ja vakuutussektorit muodostavat yhdessä osan EU:n finanssialasta, mutta niitä ohjaavat osittain erilaiset sektorikohtaiset sääntelykehikot. Pankkisektorilla keskeisiä sääntelyinstrumentteja ovat Basel III, CRR ja CRD ja kun taas vakuutussektorilla vastaavan aseman saavat Solvenssi II ja IDD. Molemmat sektorit kuuluvat kuitenkin AI Actin soveltamisalaan. Tämän vuoksi samat AI Actin velvoitteet kohdistuvat kahteen institutionaalisesti erilaiseen toimintaympäristöön, joissa ne limittyvät osaksi jo olemassa olevia sääntely-, hallinto- ja riskienhallintarakenteita.

Näiden teemojen pohjalta tutkielman tavoitteen saavuttamiseksi tutkimuskysymyksiä valikoitui kolme kappaletta.

1. Kuinka suuririskisiä tekoälysovelluksia finanssisektorin eri toimijat käyttävät?

2. Miten AI Actin velvoitteet sopivat yhteen vakuutus- ja pankkialan olemassa olevan sääntelyn kanssa?

3. Miten AI Actin vaatimukset vaikuttavat riskienhallintaan vakuutus- ja pankkisektorilla?

Ensimmäisen tutkimuskysymyksen tarkoituksena on selvittää, millaisia tekoälyn sovelluksia pankit ja vakuutusyhtiöt hyödyntävät liiketoiminnassaan sekä miten nämä käyttötapaukset sijoittuvat AI Actin mukaisiin riskiluokkiin. EU:n tekoälyasetuksessa tekoälyn käyttötapaukset jaetaan eri riskiluokkiin, joihin liittyy erilaisia sääntelyvelvoitteita (Hacker, 2025, 4). Velvoitteiden määrä ja laajuus riippuvat suoraan järjestelmän riskiluokasta, minkä vuoksi riskiluokittelu on keskeisessä asemassa myös tekoälyjärjestelmien riskienhallinnan kannalta.

Toisen tutkimuskysymyksen tavoitteena on tarkastella, miten AI Act sijoittuu osaksi jo ennestään vahvasti säänneltyä finanssialaa. Tarkoituksena on analysoida AI Actin ja olemassa olevan sektorikohtaisen sääntelyn välisiä yhtäläisyyksiä ja eroja sekä sitä, miten nämä sääntelykehykset täydentävät toisiaan. Lisäksi tarkastellaan mahdollisia toimialakohtaisia eroja sekä pankki- ja vakuutussektorille annettujen viranomaisohjeistusten erityispiirteitä.

Kolmas tutkimuskysymys keskittyy siihen, miten AI Actin velvoitteet vaikuttavat organisaatioiden riskienhallintajärjestelmiin ja miten ne integroituvat olemassa oleviin riskienhallintamalleihin. Tämän yhteydessä tarkastellaan myös, aiheuttaako uusi sääntely muutoksia organisaatioiden toimintaprosesseihin, kuten dokumentaatiovaatimusten lisääntymistä tai compliance-toimintoihin liittyvien resurssitarpeiden kasvua.

Vaikka EIOPA:n ja EBA:n ohjeistukset koskevat koko eurooppalaista finanssisektoria, tutkimuksen empiirinen aineisto koostuu suomalaisten finanssialan toimijoiden edustajista. Näin ollen tutkimuksen maantieteellinen tarkastelu rajautuu Suomeen.

Tutkielman tavoitteena on vertailla uuden asetuksen vaikutuksia finanssisektorin toimijoiden riskienhallintaan sääntely- ja governance näkökulmasta. Näin ollen näkökulma ei ole teknologinen, eikä näin analysoi tekoälyn teknisiä riskejä tai

algoritmien toiminnallisia uhkia. Pääpaino on AI Actin velvoitteiden vaikutukset riskienhallinnan rakenteisiin ja prosesseihin eri finanssisektorin toimijoissa.

Riskienhallintaan kuuluu olennaisesti riskit. Tutkielma ei kuitenkaan kuvaa tekoälyyn liittyviä riskejä, ellei niitä käsitellä nimenomaan AI Actin määrittelemien vaatimusten kautta. Riskien käsittelyyn vaikuttaa niiden osallisuus sääntelylogiikkaan ja sitä kautta vaikutus pankkien ja vakuutusyhtiöiden riskienhallinnan velvoitteisiin. Huomio kohdistuu siten erityisesti siihen, miten tekoälyyn liittyvät riskit jäsentyvät osaksi pankkien ja vakuutusyhtiöiden sääntely- ja hallintorakenteita.

Keskeinen tarkasteltava näkökulma on pankkien ja vakuutusyhtiöiden institutionaaliset ja sääntelyn erot. Näiden erojen takia AI Act ”laskeutuu” olemassa oleviin rakenteisiin eri tavoin. Tämän takia tutkielman ensisijainen fokus on AI Actin tuottamissa eroissa sektorien riskienhallinnan välillä, ei tekoälyn itsenäisissä riskeissä.

Näin tutkielma tarkentuu nimenomaan siihen kysymykseen, miten AI Act vaikuttaa riskienhallintaan, sen rakenteisiin ja prosesseihin pankki- ja vakuutussektorilla, ja miksi vaikutukset eroavat toisistaan sektorikohtaisen sääntelyn ja institutionaalisten rakenteiden vuoksi.

1.4 Tieteenfilosofiset lähtökohdat

Tieteenfilosofia käsitteenä viittaa uskomusten ja oletusten järjestelmään, joka ohjaa tiedon tuottamista. Se kuvaa, millaisista lähtökohdista tutkimusta tehdään ja millä tavoin tutkimuksessa tuotettua tietoa voidaan perustella. Uuden tiedon tuottamisen ei tarvitse olla mullistavaa, vaan myös tietyn ilmiön systemaattinen tarkastelu voi tuottaa uutta ymmärrystä (Saunders, ym., 2019, 130)

Tutkimusprosessin aikana tutkija tekee oletuksia, jotka vaikuttavat esimerkiksi tutkimuskysymysten muotoiluun, tutkimusmenetelmien valintaan sekä tulosten esittämiseen. Hyvin perustellut oletukset muodostavat tutkimuksen tieteenfilosofisen perustan. Oletukset voidaan jakaa kolmeen pääluokkaan: ontologisiin, epistemologisiin ja aksiologisiin oletuksiin. Ontologia viittaa oletuksiin siitä, millainen tutkittava todellisuus on. Epistemologia puolestaan käsittelee sitä, millaista tietoa pidetään

hyväksyttävänä ja millä tavoin tietoa voidaan tuottaa. Aksiologiset oletukset liittyvät tutkijan arvoihin ja niiden mahdolliseen vaikutukseen tutkimusprosessiin (Saunders, ym., 131).

Tämän tutkielman tieteenfilosofiset lähtökohdat perustuvat tutkijan omiin oletuksiin ja analyyttisiin pohdintoihin tutkittavasta ilmiöstä. Tutkielman aihe juontaa kiinnostuksesta tekoälyn yleistyvään käyttöön finanssisektorilla sekä sen merkitykseen organisaatioiden riskienhallinnan näkökulmasta. Finanssiala on vahvasti säännelty toimiala, jossa uudet sääntelyhankkeet vaikuttavat suoraan organisaatioiden riskienhallintakäytäntöihin ja hallintorakenteisiin. Tämän vuoksi tutkimuksessa pyritään selvittämään, miten uusi tekoälysääntely integroidaan pankkien ja vakuutusyhtiöiden olemassa oleviin riskienhallintajärjestelmiin.

Tutkielmassa oletetaan, että tekoälyn käyttö ja siihen liittyvä riskienhallinta muodostuvat organisaatioiden käytännöissä ja päätöksentekoprosesseissa. Näihin käytäntöihin vaikuttavat sekä ulkoinen sääntely-ympäristö että organisaation omat toimintamallit ja tulkinnat sääntelyn vaatimuksista. Näin ollen tekoälyn riskienhallinnan toteutuminen ei ole täysin yhdenmukaista eri organisaatioissa, vaan siihen vaikuttavat muun muassa organisaation toimiala, riskienhallintakehikko sekä tulkinta sääntelyn vaatimuksista.

Oletuksena on myös se, että EU-tason sääntely, kuten AI Act, luo organisaatioille yhteisen normatiivisen viitekehyksen, joka ohjaa tekoälyjärjestelmien käyttöönottoa ja riskienhallintaa. Vaikka organisaatiot voivat soveltaa sääntelyä eri tavoin, niiden toimintaa ohjaavat kuitenkin samat keskeiset periaatteet, kuten riskiperusteisuus, dokumentointivaatimukset ja ihmisen valvonnan säilyttäminen tekoälyjärjestelmien käytössä.

Näiden oletusten perusteella tutkimuksessa tarkastellaan tekoälyn käyttöä ja riskienhallintaa finanssisektorilla asiantuntijahaastattelujen sekä viranomaisohjeistusten kautta. Haastatteluaineiston avulla pyritään muodostamaan kuva siitä, miten organisaatiot tulkitsevat ja soveltavat AI Actin vaatimuksia käytännössä sekä millaisia eroja pankki- ja vakuutussektorin riskienhallinnassa voidaan havaita.

Mm. Saunders ym. (2019, 144-145) esittelevät viisi liiketaloustieteissä yleisesti käytettyä tieteenfilosofista lähestymistapaa: *positivismi, kriittinen realismi, interpretivismi,*

postmodernismi ja pragmatismi. Nämä lähestymistavat eroavat toisistaan niiden ontologisten ja epistemologisten oletusten sekä tyypillisten tutkimusmenetelmien perusteella. Positivismi perustuu ajatukseen, että todellisuus on olemassa tutkijasta riippumatta ja että sitä voidaan tutkia objektiivisesti tieteellisin menetelmin. Positivismin mukaan on olemassa yksi todellinen todellisuus, jota voidaan tarkastella mittaamalla ja havainnoimalla. Kriittinen realismi puolestaan olettaa, että todellisuus on olemassa tutkijasta riippumatta, mutta sitä voidaan ymmärtää vain osittain ja tulkinnan kautta. Tämän näkemyksen mukaan tutkimuksen tavoitteena on tarkastella havaittavien ilmiöiden taustalla vaikuttavia rakenteita ja syy-mekanismeja. Interpretivismi perustuu ajatukseen, että sosiaalinen todellisuus rakentuu ihmisten tulkinnoista, kokemuksista ja vuorovaikutuksesta. Postmodernismi korostaa, että tieto ja todellisuus ovat sidoksissa valtaan, ideologioihin ja yhteiskunnallisiin rakenteisiin. Pragmatismi puolestaan painottaa tutkimuksen käytännöllistä merkitystä ja keskittyy tutkimusongelman ratkaisemiseen hyödyntämällä tilanteeseen sopivia tutkimusmenetelmiä.

Tutkimuksen tieteenfilosofinen lähtökohta voidaan sijoittaa kriittisen realismin viitekehykseen. Tutkimuksessa oletetaan, että finanssisektorin sääntely ja organisaatioiden riskienhallintarakenteet ovat tutkijasta riippumattomia ilmiöitä, mutta niiden tulkinta ja soveltaminen voivat vaihdella organisaatioiden välillä. Haastatteluaineiston analyysi sisältää tulkitsevia piirteitä, sillä tutkimuksessa tarkastellaan asiantuntijoiden näkemyksiä ja kokemuksia AI Actin soveltamisesta käytännössä. Tutkimuksessa on myös pragmaattisia piirteitä, sillä sen tavoitteena on tuottaa käytännöllistä ymmärrystä tekoälysääntelyn vaikutuksista finanssisektorin riskienhallintaan.

Tutkijan tulee myös määrittää, millaista päättelytapaa tutkimuksessa hyödynnetään. Päättely voi olla deduktiivista, induktiivista tai abduktiivista. Deduktiivisessa päättelyssä johtopäätös johdetaan yleisistä teorioista tai oletuksista yksittäisiin havaintoihin. Induktiivisessa päättelyssä tutkimus etenee yksittäisistä havainnoista kohti yleisempiä johtopäätöksiä ja teoreettisia selityksiä. Abduktiivinen päättely yhdistää deduktiivisen ja induktiivisen lähestymistavan piirteitä, minkä tavoitteena on joko kehittää uutta teoriaa tai tarkentaa jo olemassa olevaa teoriaa aineiston perusteella (Saunders,ym., 2019,154).

Tämän tutkielman päättelylogiikka on pääosin abduktiivinen. Abduktiivisessa lähestymistavassa tutkimus etenee vuorovaikutteisesti teorian ja empiirisen aineiston

välillä yhdistäen deduktiivisen ja induktiivisen päättelyn piirteitä (Saunders, ym., 2019, 155). Tutkimuksessa hyödynnetään olemassa olevaa teoriapohjaa ja sääntelykehikkoa, kuten EU:n tekoälyasetusta sekä finanssisektoria koskevia viranomaisohjeistuksia, mutta samalla empiirisen aineiston avulla tarkastellaan, miten nämä periaatteet näyttäytyvät käytännössä pankkien ja vakuutusyhtiöiden riskienhallinnassa.

Empiirinen aineisto koostuu sekä primääri- että sekundääriaineistosta**.** Primääriaineistona toimivat asiantuntijahaastattelut, joiden avulla pyritään tunnistamaan keskeisiä teemoja, käytäntöjä ja näkökulmia liittyen tekoälyasetuksen vaikutuksiin finanssialan organisaatioissa. Sekundääriaineistona hyödynnetään viranomaisohjeistuksia ja toimialaselvityksiä, joiden avulla haastatteluista saatuja havaintoja voidaan tarkastella suhteessa laajempaan sääntely- ja toimialakontekstiin. Aineiston analyysin tarkoituksena ei ole pelkästään testata olemassa olevaa teoriaa, vaan myös tarkastella, miten teoria ja sääntelykehikko vastaavat käytännön toimijoiden kokemuksia ja tulkintoja. Abduktiiviselle tutkimukselle tyypillisesti analyysi etenee aineiston ja teorian välillä, jolloin empiiriset havainnot voivat täydentää, tarkentaa tai uudelleen jäsentää teoreettista viitekehystä.

Abduktiivinen lähestymistapa mahdollistaa tutkimusprosessissa joustavan etenemisen sekä ilmiön tarkastelun useista näkökulmista. Saunders ym. (2019, 156) mukaan abduktiivinen päättely on erityisen tyypillistä liiketaloustieteellisessä tutkimuksessa, jossa tutkimus perustuu usein sekä teoreettiseen että empiiriseen aineistoon.

1.5 Tutkimusmenetelmät ja -aineisto

Tämän tutkielman tavoitteena on muodostaa syvällinen ymmärrys tutkimuskohteena olevasta ilmiöstä ja siihen liittyvistä tutkimusongelmista kerätyn aineiston sekä sen perusteella tehtyjen havaintojen pohjalta. Tutkimuksen tavoitteet, aineiston luonne, tutkimusilmiön ymmärtämiseen liittyvät lähtökohdat sekä valitut tieteenfilosofiset näkökulmat huomioon ottaen laadullinen eli kvalitatiivinen tutkimusmenetelmä soveltuu tähän tutkielmaan hyvin.

Terminä ”laadullinen” tai ”kvalitatiivinen” ymmärretään aineiston muodon kuvaukseksi, jolloin aineistoon voidaan soveltaa eri lukutapoja. Laadulliselle tutkimukselle tyypillisiä tunnusmerkkejä ovat hypoteesittomuus, teoreettinen otanta, tutkittavien näkökulma ja aineistonkeruumenetelmä. Laadullinen aineisto ymmärretään pelkistetysti tekstinä, kuten haastattelut. Kvalitatiivinen tutkimus on aineistolähtöinen analyysi, jossa pelkistetysti teoria rakennetaan empiirisestä aineistosta lähtien. Laadullisessa tutkimuksessa hypoteesittomuus ymmärretään siten, että tutkijalla ei ole ennalta olettamuksia tutkimustuloksista, jotka rajaisivat tutkimuksellisia toimenpiteitä. Laadullisessa tutkimuksessa opitaan uutta tutkimuksen edetessä, jolloin tutkija aineiston avulla löytää uusia näkökulmia (Eskola, 1998).

Tutkielman empiirinen aineisto muodostuu sekä sekundääri- että primääriaineistosta. Sekundääriaineistona hyödynnetään Euroopan valvontaviranomaisten asiakirjoja sekä Finanssivalvonnan laatimaa tutkimusta tekoälyn käytöstä suomalaisella finanssisektorilla. Sekundääriaineiston avulla tutkielmaan tuodaan laajempi näkökulma tekoälyn hyödyntämiseen suomalaisella finanssisektorilla sekä lainsäädännöllinen näkökulma vahvasti säännellylle toimialalle, jolla sääntelyllä on keskeinen merkitys alan toimijoiden toimintaan. Primääriaineisto puolestaan tarjoaa konkreettisen näkökulman siihen, miten AI Act on organisaatioissa otettu käyttöön, sekä syventää ymmärrystä tarkasteltavasta ilmiöstä.

Primääriaineisto kerättiin puolistrukturoiduilla teemahaastatteluilla. Menetelmä soveltuu laadulliseen tutkimukseen tilanteissa, joissa tavoitteena on tarkastella tutkittavaa ilmiötä syvällisesti ja antaa haastateltaville mahdollisuus kuvata näkemyksiään omin sanoin. Puolistrukturoitu haastattelu mahdollistaa ennalta määriteltyjen teemojen käsittelyn, mutta jättää samalla tilaa haastateltavien omille tulkinnoille, havainnoille ja esimerkeille. Teemahaastattelussa haastattelu kohdistuu etukäteen määriteltyihin aihepiireihin, joiden varassa keskustelu etenee. Menetelmän etuna on sen kyky kohdistua tutkimuksen kannalta olennaisiin teemoihin samalla, kun se mahdollistaa aineiston riittävän joustavan muodostumisen. (Eskola, 1998, luku 3; Hirsijärvi, 2022, luku 4.)

Laadullisessa tutkimuksessa tavoitteena on usein kuvata ilmiötä ja ymmärtää tiettyä toimintaa, minkä vuoksi tiedonantajien valinnassa korostuu tarkoituksenmukaisuus. Tästä syystä on olennaista, että haastateltavilla on kokemusta tutkittavasta ilmiöstä ja että

he pystyvät tuottamaan tutkimuskysymysten kannalta relevanttia tietoa (Tuomi & Sarajärvi, 2018, luku 3.)

Haastateltaviksi valittiin vakuutus- ja pankkisektorin asiantuntijoita, joilla oli relevanttia kokemusta AI Actin käyttöönotosta sekä siihen liittyvästä riskienhallinnasta omassa organisaatiossaan. Teemahaastatteluissa edettiin ennalta määriteltyjen teemojen mukaisesti samassa järjestyksessä. Haastateltavat saivat vastata kysymyksiin avoimesti, mutta tarpeen mukaan esitettiin myös tarkentavia jatkokysymyksiä (Tuomi & Sarajärvi, 2018, luku 3 ; Hirsjärvi & Hurme, 2022, luku 4).

Asiantuntijahaastattelut toteutettiin täysin anonyymisti siten, että henkilötietoja ei säilytetty tunnistettavassa muodossa eikä organisaatioita nimetä tutkimuksessa. Aineistoa käsiteltiin Tampereen yliopiston tietosuojaohjeistuksen mukaisesti ja se säilytettiin luottamuksellisesti.

Tutkielman sekundääriaineisto koostui Finanssivalvonnan laatimasta tutkimuksesta tekoälyn käytöstä suomalaisella finanssisektorilla sekä Euroopan unionin viranomaisohjeistuksista, jotka koskevat vakuutus- ja pankkisektoria. Eskolan (1998) mukaan olemassa olevan sekundääriaineiston hyödyntäminen on monissa tapauksissa tarkoituksenmukaisempaa kuin kokonaan uuden aineiston kerääminen. Tässä tutkielmassa sekundääriaineiston käyttö oli perusteltua, sillä Euroopan viranomaiset olivat jo analysoineet voimassa olevan sääntelyn ja AI Actin välistä suhdetta. Lisäksi Finanssivalvonnan tutkimus muodosti kattavan yleiskuvan tekoälyn käytöstä suomalaisella finanssisektorilla, joten vastaavan laajan primääriaineiston kerääminen ei ollut tutkimuksen tavoitteiden kannalta tarpeellista.

Tässä tutkielmassa empiirisen aineiston analyysi toteutettiin laadullisena sisällönanalyysina, jossa aineistoa tarkastellaan systemaattisesti ja mahdollisimman objektiivisesti. Sisällönanalyysin tavoitteena on tuottaa kirjallisesta aineistosta tiivistetty ja yleiseen muotoon jäsennetty kuvaus tutkimuksen kohteena olevasta ilmiöstä. Menetelmän avulla aineistosta voidaan tehdä selkeitä ja perusteltuja johtopäätöksiä sekä lisätä analyysin kautta aineiston jäsentyneisyyttä ja ymmärrettävyyttä. (Tuomi & Sarajärvi, 2018, luku 4.)

Analyysia täydennettiin teemoittelulla, jonka avulla aineistosta nostettiin esiin tutkimusongelman kannalta olennaisia teemoja. Teemoittelu mahdollistaa sen, että aineistosta voidaan tarkastella ja vertailla tiettyjen teemojen esiintymistä ja ilmenemistä eri osissa aineistoa. (Eskola, 1998, luku 4.)

Tavoitteena oli analysoida primääri- ja sekundääriaineistosta esiin nousseita havaintoja ja kokemuksia sekä jäsentää ne temaattiseksi kokonaisuudeksi. Analyysin perusteella pyrittiin kokoamaan tutkielman keskeiset tulokset yhteen ja muodostamaan tutkimuskysymyksiin vastaava kokonaisuus.

Tutkielman teoriaosuuden perustana hyödynnettiin laajasti alan kirjallisuutta, oikeuslähteitä sekä muita luotettavia julkaisuja. Teoriaosuuden uskottavuus perustuu käytetyn lähdeaineiston laatuun, minkä vuoksi lähteiden on oltava tutkimusaiheen kannalta keskeisiä ja lähdeviitteiden asianmukaisia (Tuomi & Sarajärvi, 2017, luku 1). Tuomi ja Sarajärvi (2017) nostavat hyvän tutkimuksen keskeisiksi kriteereiksi sisäisen johdonmukaisuuden ja eettisen kestävyyden. Näiden toteutumiseksi tutkielmassa on huomioitu hyvän tieteellisen käytännön periaatteet koko tutkimusprosessin ajan.

1.6 Keskeisten käsitteiden määrittely

Artificial Intelligence (AI)

Tekoälyllä tarkoitetaan tietokoneiden ja koneiden kykyä jäljitellä inhimillistä älykkyyttä ja ongelmanratkaisukykyä. Tekoälyn ihanteellinen ominaisuus on sen kyky rationaaliseen päättelyyn ja toimintaan tietyn tavoitteen saavuttamiseksi. Koneoppiminen on tekoälyn osa-alue, jonka perusajatus on, että tietokoneohjelmat voivat automaattisesti oppia ja mukautua uuteen dataan ilman ihmisen apua. Tärkeä osa tekoälyn rakennetta ovat algoritmit. (Investopedia, AI, 2025).

EU Artificial Intelligence Act (AI Act)

Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689 tekoälyä koskevista yhdenmukaisista säännöistä. Asetuksen tarkoituksena on vahvistaa yhtenäinen oikeudellinen kehys tekoälyjärjestelmien käytölle.

Enterprise Risk Management (ERM)

Kokonaisvaltainen riskienhallinta on menetelmä, jossa riskienhallintaa tarkastellaan strategisesti koko yrityksen tai organisaation näkökulmasta. Se on ylhäältä alas -lähestymistapa, jonka tavoitteena on tunnistaa, arvioida ja varautua mahdollisiin menetyksiin, vaaratilanteisiin, uhkiin ja muihin haittoihin, jotka voivat häiritä organisaation toimintaa ja tavoitteiden saavuttamista ja/ tai aiheuttaa taloudellisia tappioita (Investopedia, ERM 2025)

Solvenssi II

Solvenssi II on sääntelykehys, joka koskee Euroopassa henki-, vahinko- ja jälleenvakuutusyhtiöiden toimintaa. Direktiivissä säädetään vakuutusyhtiöiden vakavaraisuudesta, hallintojärjestelmästä, raportoinnista sekä valvonnasta. Direktiivillä pyritään edistämään EU:n sisämarkkinoiden toimintaa sekä suojaamaan vakuutuksenottajia, vakuutettuja ja edunsaajia (Finanssivalvonta, 2025).

Basel III

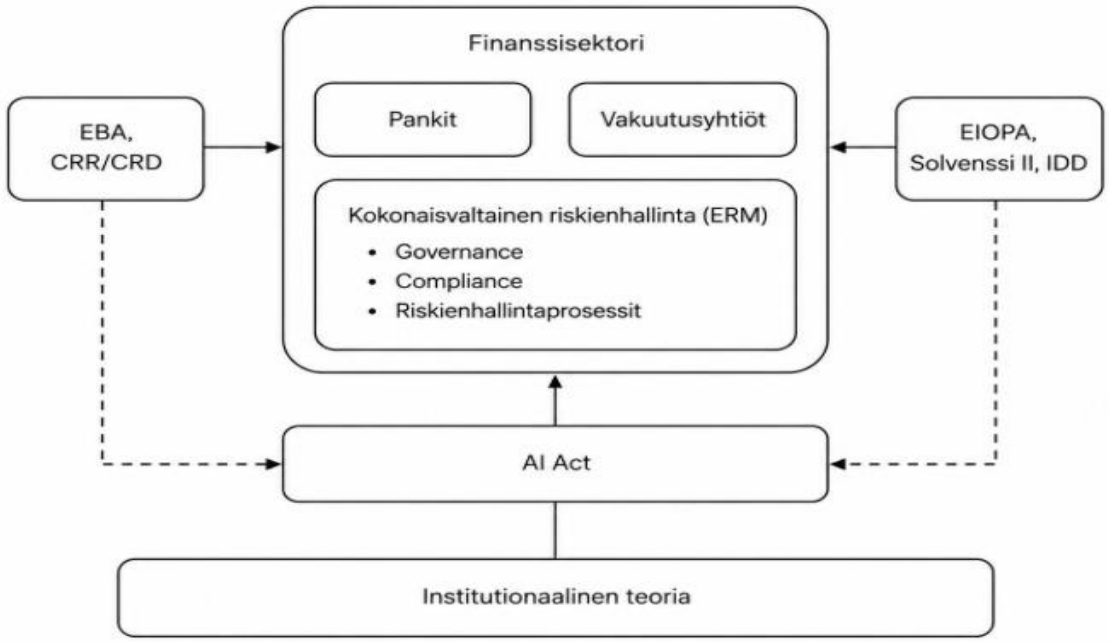
Baselin standardit ovat kansainvälinen pankkisäätelykokonaisuus, jonka Baselin pankkivalvontakomitea on laatinut vähimmäispääomavaatimuksia, stressitestejä ja maksuvalmiusriskin hallintaa varten. Standardien tavoitteena on vahvistaa pankkien kykyä kestää taloudellisia shokkeja ja vähentää uuden maailmanlaajuisen finanssikriisin todennäköisyyttä. Basel III on kolmas peräkkäinen kansainvälinen pankkisäätelysopimus, jonka on laatinut Baselin pankkivalvontakomitea (BCBS) (Finance eu, 2024; Council of the european union, 2024).

Tekoälyjärjestelmä

Konepohjainen järjestelmä, joka on suunniteltu toimimaan vaihtelevilla autonomian tasoilla sekä voi käyttöönoton jälkeen osoittaa mukautuvuutta. Järjestelmä päättelee vastaanottamastaan syötteestä, miten tuottaa esimerkiksi ennusteita, sisältöä, suosituksia tai päätöksiä, jotka voivat vaikuttaa fyysisiin tai virtuaalisiin ympäristöihin (1689,2024, EU)

1.7 Tutkielman teoreettinen viitekehys ja rakenne

Tässä alaluvussa esitellään tutkielman teoreettinen viitekehys, jonka tavoitteena on havainnollistaa ja jäsentää työn keskeinen sisältö. Teoreettinen viitekehys on näkökulma, jossa havaintoja tarkastellaan eksplisiittisesti määritellystä näkökulmasta (Alasaari, 2011). Viitekehyksen visuaalinen esitystapa selkeyttää teoriaosuuden rakennetta ja johdattaa lukijan tutkielman kokonaisuuteen. Seuraavaksi tarkastellaan tutkielman teoreettista viitekehystä (Kuvio 1) sekä koko työn rakennetta.



Kuvio 1 Teoreettinen viitekehys

Tutkielman teoreettinen viitekehys koostuu kolmesta pääteemasta ja niiden vuorovaikutuksista keskenään. Teoreettisen viitekehykset pääteemat ovat, kokonaisvaltainen riskienhallinta (ERM) pankki- ja vakuutussektorilla, AI Act ja institutionaalinen teoria.

Tutkielman teoreettinen viitekehys rakentuu finanssisektorin ja erityisesti pankkien ja vakuutusyhtiöiden kokonaisvaltaisen riskienhallinnan ympärille. Näiden toimijoiden riskienhallintaa ohjaa vahvasti olemassa oleva sääntelykehys. Pankkisektorin osalta ohjeistuksesta ja valvonnasta vastaa Euroopan pankkiviranomainen EBA, kun taas vakuutussektorilla vastaavaa roolia hoitaa Euroopan vakuutus- ja lisäeläkeviranomainen EIOPA. Riskienhallinnan näkökulmasta keskeisiä sääntelykokonaisuuksia ovat

pankkisektorilla CRR/CRD-sääntelykehikko ja vakuutussektorilla Solvenssi II, joiden tutkielman kannalta olennaisimpia osa-alueita tarkastellaan teoriaosuudessa

Lousuitin (2014) mukaan ERM:n tavoitteena on yhdistää organisaation keskeiset riskit yhden hallintakehyksen alle siten, että riskit voidaan tunnistaa, arvioida ja hallita kokonaisvaltaisesti. Tämä näkökulma on keskeinen myös AI Actin tarkastelussa, sillä tekoälyyn liittyvät riskit eivät useinkaan muodostu irrallisiksi kokonaisuuksiksi, vaan ne kietoutuvat osaksi organisaatioiden olemassa olevia prosesseja, järjestelmiä ja palveluita. Tässä tutkielmassa tarkastellaan, miten AI Actin velvoitteet sovitetaan yhteen pankkien ja vakuutusyhtiöiden nykyisten compliance- ja riskienhallintaprosessien kanssa. Tavoitteena on analysoida, miten AI Act integroidaan osaksi kokonaisvaltaista riskienhallintaa sekä millaisia päällekkäisyyksiä ja eroavaisuuksia sillä on suhteessa jo olemassa olevaan finanssisektorin sääntelyyn.

Tutkielman kannalta keskeinen sääntelykokonaisuus on AI Act (Artificial Intelligence Act, (EU) 2024/1689), jonka olennaisimpia artikloja käsitellään teoriaosuudessa. Tarkastelussa korostuvat erityisesti korkean riskin tekoälyjärjestelmiä koskevat velvoitteet. Korkean riskin tekoälyjärjestelmät asettavat organisaatioille velvoitteita muun muassa datan laadun ja hallinnan, läpinäkyvyyden sekä riskienhallinnan osalta koko järjestelmän elinkaaren ajan. Lisäksi tekoälyjärjestelmien riskitaso vaikuttaa siihen, millaisia hallinnollisia vaatimuksia organisaatioihin kohdistuu (Artificial Intelligence Act, (EU) 2024/1689). AI Act ei vaikuta ainoastaan organisaatioiden riskienhallintaan, vaan laajemmin finanssisektorin toimintaan kokonaisuudessaan. Koska asetus perustuu riskiperusteiseen lähestymistapaan, tutkielmassa painottuu erityisesti riskienhallinnan näkökulma.

Tutkielman vertailukohteina toimivat pankit ja vakuutusyhtiöt. Tarkastelun teoreettisena taustana hyödynnetään institutionaalista teoriaa, jonka avulla voidaan selittää, miksi AI Actin käyttöönotto voi erota pankkien ja vakuutusyhtiöiden riskienhallintajärjestelmissä sekä niitä koskevissa viranomaisohjeistuksissa. Institutionaalisen teorian mukaan organisaatiot mukautuvat sääntelyyn omien institutionaalisten rakenteidensa sekä legitimiteettiin kohdistuvien paineiden mukaisesti. DiMaggion ja Powellin (1983) mukaan organisaatioiden toimintaa yhdenmukaistavat erityisesti pakottavat, mimeettiset ja normatiiviset paineet, jotka voivat näkyä esimerkiksi sääntelyn noudattamisena, muiden toimijoiden käytäntöjen jäljittelynä sekä alan ammattikäytäntöjen

omaksumisena. Vaikka finanssisektorin toimijoita koskevat velvoitteet ovat lähtökohtaisesti samat, voivat ne ilmetä käytännössä eri tavoin. Institutionaalinen teoria auttaa ymmärtämään näitä eroja, sillä sääntelyperinne, valvojien painotukset ja sektorikohtainen riskiprofiili ohjaavat sitä, millaiseksi sääntelyn käyttöönotto käytännössä muodostuu. Lisäksi legitimiteetin säilyttäminen on finanssisektorilla keskeistä, minkä vuoksi tekoälyjärjestelmien käytön tulee näyttäytyä sidosryhmille läpinäkyvänä, oikeudenmukaisena ja sääntelyn mukaisena (Suchman, 1995).

2 FINANSSISEKTORIN RISKIENHALLINTA

Finanssisektorin riskienhallinta muodostaa tämän tutkielman teoreettisen perustan, sillä pankkien ja vakuutusyhtiöiden sääntely- ja riskienhallintarakenteet vaikuttavat suoraan siihen, miten AI Actin velvoitteet tulevat sektorilla sovellettaviksi. Riskienhallintaa tarkastellaan ensin laajemmalla tasolla ja tämän jälkeen toimialakohtaisesti, jotta voidaan myöhemmin arvioida, miten tekoälyä koskeva sääntely kytkeytyy näihin rakenteisiin.

2.1 Riskienhallinnan perusta finanssialalla

Finanssialalla kokonaisvaltainen riskienhallinta on olennainen osa toimintaa johtuen toimialan luonteesta. Finanssialan toimijoilla on keskeinen yhteiskunnallinen tehtävä, jolla varmistetaan toiminnan luotettavuutta ja vastuullisuutta. Toimijoiden vakavaraisuus on koko finanssisektorin vakauden kannalta merkittävä tekijä (Finanssivalvonta, toimintakertomus 2023). Finanssikriisin jälkeen ala koki kolhauksen luottamukseen aikaisemman mallinnuksen oikeellisuuteen, mikä on aiheuttanut kiristyksiä lainsäädännössä sekä korostanut riskienhallinnan roolia (Kivisaari, E, ym., 2017, luku 14).

Louisot (2014) kuvailee kokonaisvaltaisen riskienhallinnan kehitystä perinteisestä riskienhallinnasta. ERM on kehittynyt tarpeesta laajentaa riskienhallintaa koskemaan sekä taloudellisia, että ei -taloudellisia organisaatioita, jotta riskejä ja tapahtumia voidaan hallita perinteisten operatiivisten rajojen ulkopuolella. ERM nähdään keinona yhdistää ja hallita kaikkia organisaation riskejä yhden kokonaisuuden alla, jotta kaikki kriittiset riskit voidaan tunnistaa, ohjata ja hallita. Muutosta perinteisestä riskienhallinnasta ERM:ään, voidaan kuvata ilmaisulla ”riskienhallinnan liittäminen strategiaan”. ERM on laajasti tunnettu termi, jota käytetään kuvailemaan organisaatioiden prosesseja ja käytäntöjä hallitakseen riskiportfolioonsa.

Tyypillisesti ERM sijoittuu organisaation strategisten tavoitteiden kontekstiin, ja oikein toteutettuna vahva ERM-kehikko tukee aktiivisesti pitkän aikavälin arvonluontia, kassavirran ja riskien hallintaa, jotta konsernin toiminnassa voidaan sekä luoda että

suojata arvoa. (Hitchcox, 2022, 341-342). Kokonaisvaltaiseen riskienhallintaan on luotu erilaisia työkaluja, kuten ISO 31000.

ISO 31000 on kansainvälinen standardi, joka tarjoaa periaatteet ja ohjeet riskienhallintaan. Se määritellee kokonaisvaltaisen lähestymistavan riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan ja viestintään koko organisaation tasolla. ISO 31000 ohjeistuksessa perustellaan kokonaisvaltaista riskienhallintaa useasta eri näkökulmasta. Heidän mukaansa riskienhallinta on toistuva prosessi, joka auttaa organisaatioita määrittämään strategiansa, saavuttamaan tavoitteensa ja tekemään tietoon perustavia päätöksiä. Se on olennainen osa hallintoa ja johtamista sekä keskeinen osa sitä, miten organisaatiota johdetaan kaikilla tasoilla. Riskienhallinta huomioi organisaation ulkoisen ja sisäisen toimintaympäristön, mukaan lukien lainsäädännölliset, inhimilliset ja kulttuurilliset tekijät. Riskienhallinta perustuu periaatteisiin, viitekehykseen ja prosessiin. Näihin liittyvät osatekijät voivat olla olemassa osittain tai kokonaan organisaatiossa, mutta niitä voidaan joutua muokkaamaan tai kehittämään, jotta riskienhallinta olisi tehokasta, tuloksellista ja johdonmukaista (International Organization for Standardization, 2018).

2.2 Vakuutusyhtiöiden riskienhallinta

Jokaisella yrityksellä on omat riskinsä, jotka ovat tyypillisiä kyseisen toimialan ympäristössä. Kyseisessä riskiympäristössä toimiva yritys pyrkii jatkuvaan sekä kannattavaan liiketoimintaan. Perinteisessä vakuutusajattelussa riskit ovat pääosin olleet vakuutusriskejä ja niihin liittyviä sijoitusriskejä, mutta nykyään riskienhallinta sisältää kaikki liiketoimintaan vaikuttavat riskit (Kivisaari, E, ym., 2017, luku l1).

Vakuutustoiminnan riskit jakautuvat varsinaisen toiminnan riskeihin ja muihin toimintaan liittyviin riskeihin. Varsinaisilla toiminnan riskeillä tarkoitetaan suoranaisia riskejä johtuen vakuutusten myöntämisestä. Vakuutussektorin riskienhallinta perustuu vakuutusteknisten, markkina-, operatiivisten ja malliriskien kokonaisvaltaiseen hallintaan. Vakuutusyhtiöiden riskiprofiili poikkeaa pankkisektorista, koska vakuutustoiminnan ydin liittyy puhtaiden riskien siirtämiseen ja riskipoolien muodostamiseen. Mallin tarkoituksena on muuntaa yksittäiset, yksilölliset riskit suureksi

ja hallittavaksi kokonaisuudeksi. Tämän vuoksi vakuutusyhtiöiden riskit painottuvat erityisesti pitkäaikaisiin velvoitteisiin, vakuutustekniseen epävarmuuteen sekä sijoitustoiminnan ja riskienhinnoittelun hallintaan. (Kivisaari, ym., 2017, luku 3.2). Seuraavaksi tarkastellaan operatiivisen riskin määritelmää, sekä vakuutustoiminnan perusriskejä, joita ovat markkina-, luotto-, henkivakuutus-, aineettomat hyödykkeet-, sairausvakuutus- ja vahinkovakuutusriskit.

Direktiivin 2009/138/EY 13 artiklan 33 kohdan mukaan operatiivinen riski tarkoittaa riittämättömistä tai epäonnistuneista sisäisistä prosesseista, henkilöstöstä ja järjestelmistä tai ulkoisista tapahtumista aiheutuvaa tappioriskiä. Operatiivinen riski on vahvasti sidoksissa yrityksen omiin toimintoihin, ja sitä voidaan hallita sekä kontrollitoimenpiteillä että tarvittaessa pääomalla. Operatiivista riskiä arvioidaan tyypillisesti kolmella menetelmällä: keräämällä tietoa toteutuneista operatiivisista tappioista, tekemällä riskien itsearviointeja sekä hyödyntämällä avainriskimittareita ja riskienhallinnan suorituskykymittareita. Osa operatiivista riskiä on sääntely riski.

Sääntelyriskillä tarkoitetaan, että organisaatiolla aiheutuu oikeudellisia tai sääntelyyn liittyviä seuraamuksia, taloudellisia menetyksiä tai mainehaittaa sen vuoksi, että se ei noudata toimialaa koskevaa sääntelyä ja eettisiä sääntöjä. Tämä riski voi johtaa organisaation maineen menetykseen, liiketoiminnan kasvu - ja laajentumis-mahdollisuuksien kaventumiseen, sopimusehtojen täyttämisen estymiseen ja äärimmillään jopa liiketoiminnan lopettamiseen (Kocziszky ym., 2017, 54)

Markkinariski syntyy markkinoiden keskeisten muuttujien, kuten korkojen, osakekurssien, valuuttakurssien, inflaation, kiinteistöjen arvon, pääomasijoitusten tai luottomarginaalien muutoksista. Markkinariski ilmenee varojen ja vastuiden arvon vaihteluna ja liitetään usein sijoitustoimintaan, vaikka se vaikuttaa koko taseeseen. Markkinariskejä voidaan hallita esimerkiksi johdannaisilla, hajauttamisella sekä varojen ja vastuiden yhteensovittamisella (ALM). Solvenssi II direktiivissä 13 (31) markkinariski määritellään tappioriskiksi tai taloudellisen aseman epäedulliseksi muutokseksi, joka johtuu suoraan tai välillisesti omaisuuden vastuiden ja rahoitusvälineiden markkinahintojen tason ja volatiliteetin heilahteluista.

Luottoriski tarkoittaa tappiota, joka syntyy, kun sopimuskumppani ei kykene täyttämään velvoitteitaan tai kun vastapuolen luottoluokitus heikkenee. Luottoriski voi ilmetä

esimerkiksi vastapuolen maksukyvyttömyytenä tai luottokelpoisuuden heikentymisenä. Riskin toteutuminen voi lisäksi aiheuttaa selvittelyriskejä sekä altistaa jälleenvakuuttamiseen liittyville vastapuoliriskeille. Luottoriskit liittyvät tyypillisesti joukkovelkakirjoihin, kiinnitysluottoihin, jälleenvakuutusvastapuoliin ja johdannaissopimusten vastapuoliin (Kivisaari, ym., 2017, luku 3).

Henkivakuutusriski on kuolevuuden toteutuminen ennusteista poiketen. Henkivakuutusriski voidaan jakaa seuraaviin komponentteihin: volatiliteettiriski, malliriski, trendiriski ja katastrofiriski. Näihin riskeihin voi varautua luonnollisesti vakavaraisuudella, mutta muita keinoja ovat muun muassa: riskin jakaminen vakuutuksenottajan kanssa, jälleenvakuutus ja siirtyminen sijoitussidonnaisiin vakuutuksiin (Kivisaari, ym., 2017, luku 3).

Vahinkovakuutusriski voidaan määrittää korvausmenona, jonka korvaukset ovat ylittäneet. Vahinkovakuuttamisen hinnoittelu perustuu korvausmenon odotusarvoon, mikäli tämä toteutuu toiminnan tulisi olla ylijäämäistä. Vahinkovakuutusriski voidaan jakaa seuraaviin komponentteihin: vakuutusmaksun riittävyyden riski, vastuun riittävyyden riski ja katastrofi riski. Perinteisiä suojauskeinoja näihin ovat jälleenvakuuttaminen ja vastuunvalinta (Kivisaari, ym., 2017, luku 3).

Perinteisen vakuutusliiketoiminnan lisäksi toimintaympäristön viimeaikaiset muutokset ovat tuoneet mukanaan uudenlaisia riskejä. Teknologinen kehitys, digitaalisten toimintamallien yleistyminen, datan määrän nopea kasvu sekä mallien ja algoritmien laajempi hyödyntäminen ovat lisänneet erityisesti operatiivisia ja malliperusteisia riskejä, jotka on integroitava osaksi vakuutusyhtiöiden olemassa olevaa riskienhallintajärjestelmää (EIOPA , 2024, 49-52)

2.2.1 Solvenssi II -kehikko

Euroopan unionissa toimivien vakuutusyhtiöiden sääntely perustuu pääosin Solvenssi II -direktiiviin (2009/138/EY), joka koskee vakuutus- ja jälleenvakuutustoiminnan aloittamista ja harjoittamista. Solvenssi II:n päätavoitteena on edistää sisämarkkinoiden toimintaa ja vahvistaa vakuutuksenottajien ja edunsaajien suojaa. Direktiivin mukaan

vakuutus- ja jälleenvakuutussektorin ensisijaisena tavoitteena on turvata vakuutuksenottajien ja edunsaajien asema, ja toissijaisina tavoitteena on rahoitusmarkkinoiden vakaus sekä markkinoiden oikeudenmukainen ja tehokas toiminta (Santomil & González, 2020, 319). Direktiivi perustuu taloudelliseen ja riskiperusteiseen lähestymistapaan, joka kannustaa yhtiöitä tunnistamaan ja hallitsemaan riskejään kokonaisvaltaisesti. Solvenssi II koostuu kolmesta pilarista, joista Pilari I asettaa määrilliset tavoitteet koskien vakavaraisuuspääomaa, Pilari II asettaa laadulliset tavoitteet sisältäen muun muassa riskienhallinnan ja Pilari III asettaa raportointivelvoitteet (EIOPA, Solvency II).

Pilari I määrittelee määrälliset pääomavaatimukset, joiden pohjalta oletetaan yrityksen johdon muodostavan oman näkemyksensä riskeistä ja tarvittavasta pääomasta. Yrityksen johdon vastuulla on varmistaa, että kaikki olennaiset riskit on havaittu ja niitä hallitaan asianmukaisesti. Vakavaraisuus säädöksien mukaan vakuutusyrityksen tulee arvottaa varat ja velat, vastuuvelka, omat varat, vakavaraisuuspääomavaatimus (SCR), vähimmäispääomavaatimus (MCR) ja sijoitukset (Kivisaari, ym.,2017,luku 12).

Pilari II asettaa tavoitteet sisäiseen riskienhallintajärjestelmään, tämä kannustaa vakuuttajia kehittämään ja käyttämään parempia riskienhallinta keinoja ja aktiivisesti tarkkailemaan ja hallitsemaan näitä riskejä (Pardon, 2016, 319). Tällä pilarilla on suuri merkitys Solvenssi II kehikossa. Tässä ajattelussa olennaista on, että vakuutusyritykseltä edellytetään järjestävänsä hallintonsa niin, että riskienhallinta tulee asianmukaisesti järjestettyä. Solvenssi II -direktiivin (2009/138/EY) 41–49 artiklojen mukaan vakuutusyhtiöillä on oltava tehokas, kattava ja yrityksen toimintaan integroitunut riskienhallintajärjestelmä, joka mahdollistaa riskien jatkuvan tunnistamisen, mittaamisen, seurannan, hallinnan ja raportoinnin. Järjestelmän on oltava suhteutettu yhtiön toiminnan laajuuteen, monimutkaisuuteen ja riskiprofiiliin. Riskienhallinta Solvenssi II kehyksessä ei rajoitu ainoastaan teknisiin menetelmiin, vaan kattaa myös vakuutusyhtiön hallintojärjestelmän, joka sisältää toimivan johdon vastuut, sisäisen valvonnan, compliance -toiminnon ja sisäisen tarkastuksen.

Kolmas pilari, eli toisin sanottuna ”markkinakuri”, käsittää tiedonanto- ja raportointivelvollisuuden. Tässä pilarissa edellytetään hyvää raportointia, jotta toimialalle muodostuu aikaisempaa parempia käytäntöjä ja toimintatapoja. Vakuutus toimialalla markkinakurille on annettu pienempi painoarvo, kuin pankkien sääntelyssä

(Kivisaari, ym., 2017, 1). SFCR eli vakavaraisuus- ja taloudellisen aseman selvitys on raportti, jossa vakuutusyhtiö kuvaa toimintansa ja tuloksensa, operatiiviset prosessinsa, riskiprofiilinsa sekä periaatteet, joilla sen varat ja velat arvostetaan. Raportissa esitetään myös tekniset vastuuvelat, muu velkarakenne ja pääomanhallinta (De Nederlansche Bank, 2023).

Julkisen SFCR-raportin lisäksi Solvenssi II edellyttää vakuutusyhtiöiltä valvontaraportin laatimista valvontaviranomaiselle. Sen kuvaileva osa noudattaa samaa rakennetta kuin SFCR, mutta sisältää tietoja, joita pidetään joko liian yksityiskohtaisina tai luottamuksellisina julkiseen julkaisuun. Lisäksi valvontaviranomaisille toimitetaan oma riski- ja vakavaraisuusarvio, eli ORSA (De Nederlansche Bank, 2023). ORSA muodostaa keskeisen osan Solvenssi II -kehikon toista pilaria ja vakuutusyhtiöiden kokonaisvaltaista riskienhallintaa. ORSA on yhtäältä yhtiön sisäinen arviointiprosessi, joka integroidaan strategiseen suunnitteluun ja päätöksentekoon, ja toisaalta valvontaviranomaisten käyttämä valvontatyökalu (Santomil & González, 2020, 319). ORSA:n tulee olla kiinteä osa liiketoimintastrategiaa siten, että sen tulokset huomioidaan kaikessa keskeisessä päätöksenteossa.

ORSA:n merkitys yhtiölle korostuu siinä, että yhtiön hallituksen on oltava tietoinen kaikista merkittävistä riskeistä riippumatta siitä, sisältyvätkö ne vakavaraisuuspääomavaatimuksen (SCR) laskentaan tai siitä, ovatko ne kvantifioitavissa. ORSA painottaa yrityksen tulevaisuutta, mukaan lukien keskipitkän ja pitkän aikavälin ennusteet sekä erityisesti niiden riskien arviointi, joita yhtiö voi kohdata liiketoiminnan suunnittelukauden aikana (Santomil & González , 2020, 321).

2.3 Pankkien riskienhallinta

Pankkien riskienhallinta muodostaa keskeisen osan pankin strategista johtamista, sillä sen avulla varmistetaan liiketoiminnan vakaus, tulovirtojen kestävyys ja pankin toimintakyky pitkällä aikavälillä. Tehokkaat riskienhallintaprosessit tukevat pankin taserakenteen kestävyyttä ja mahdollistavat sen, että pankki kykenee toimimaan myös epäedullisissa markkinaolosuhteissa. Riskienhallinta edellyttää selkeästi määriteltyjä riskistrategioita,

toimivaa infrastruktuuria ja organisaatiota sekä vahvaa riskienhallintakulttuuria, joka ulottuu läpi koko organisaation (Choudhry, 2022).

Pankilla tulee olla selkeästi määritelty riskienhallintatoiminto, jossa vastuut ja tilivelvollisuus on jaoteltu johdonmukaisesti. Hyvin organisoitu riskienhallintatoiminto toimii sekä tehokkaana sisäisenä kontrollimekanismina että mahdollisena kilpailuetuna markkinoilla. Pankkitoimialalla riskienhallinnan rakenteessa noudatetaan tyypillisesti mallia, jossa riippumaton middle office -yksikkö vastaa pankin riskilinjauksista, riskinotto- ja kaupankäyntilimiiteistä sekä niistä markkina-alueista, joilla pankki saa toimia. Tämän lisäksi pankissa toimii riskienhallintajohtaja, joka raportoi itsenäiselle johtajalle, joka on samalla myös johtokunnan jäsen. Keskeinen osa rakennetta on myös tehtävien selkeä erottelu front office-, middle office- ja back office -toimintojen välillä, usein yhdessä sisäisen tarkastuksen kanssa. Riskienhallintaan kuuluu lisäksi raportointi ylimmälle johdolle, mukaan lukien pankin kokonaisriskiasema sekä sen arviointi, pysyykö front officen toiminta pankin kokonaisstrategian mukaisena. Lisäksi riskien ja riskistrategian tulee välittyä asianmukaisesti myös sidosryhmille, kuten osakkeenomistajille (Choudhry, 2022). Edellä mainittujen lisäksi investointipankeissa ja kaupankäynnin ympäristössä riskienhallintarakenteeseen kuuluu usein päivittäiset raportoinnit, VaR -mittarin käyttö keskeisenä mittarina, eskalointimenettelyt ja johdon aktiivinen osallistuminen riskiasioihin (Choudhry, M. 2018, 397-398)

Pankkien riskienhallinnan rakenteellinen vahvuus luo perustan sille, miten pankit tunnistavat ja hallitsevat toimintaympäristössään esiintyviä erilaisia riskityyppejä. Näistä keskeisimmät riskit muodostavat pankkitoiminnan perusprofiilin. Pankkien ydintoiminta, eli rahoitustoiminta, altistaa pankit väistämättä monenlaisille riskeille, jotka niiden on kyettävä tunnistamaan, mittaamaan ja hallitsemaan johdonmukaisesti. Pankit tarjoavat asiakkailleen lainoja, erilaisia maturiteetteja, korko- ja valuuttasopimuksia sekä muita rahoituspalveluita, joihin jokaiseen liittyy oma riskiprofiilinsa. Pankkitoiminnan perusta onkin taseen molempien puolien riskien kokonaisvaltainen hallinta, sillä sekä varojen että velkojen rakenne vaikuttaa suoraan pankin riskialttiuteen ja kannattavuuteen (Choudhry, 2018, 383).

Pankkitoiminnan keskeisin liiketoiminnasta johtuva riski on luottoriski, jota kutsutaan myös liikkeeseenlaskijariskiksi. Sillä tarkoitetaan riskiä siitä, että asiakas laiminlyö

lainan takaisinmaksun, mutta myös riskiä luottokelpoisuuden heikkenemisestä, mikä heijastuu tasearvoon kasvaneen maksukyvyttömyyden todennäköisyyden kautta. Luottoriskiä arvioidaan altistuksen (nimellisarvon), maksukyvyttömyyden todennäköisyyden ja maksukyvyttömyystilanteessa syntyvän tappion perusteella. Riskin mittaamisessa hyödynnetään sekä virallisia luottoluokituksia että pankin omia sisäisiä luokitusmenetelmiä, jotka muodostavat osan luottoanalyysiprosessia. Pankki arvioi luottoriskiä sekä yksittäisen asiakkaan tasolla että koko luottosalkun kokonaisriskinä (Choudhry, 2022).

Likviditeettiriski viittaa kahteen erillisiin, mutta toisiinsa liittyviin ilmiöihin. Rahastonhoitajan tai rahamarkkinoista vastaavan henkilön näkökulmasta likviditeettiriski ymmärretään varojen riittämättömyytenä täyttää pankin sitoumukset eräpäivään mennessä. Toisaalta arvopaperi- tai johdannaiskauppiaan näkökulmasta kyseessä on riski omaisuuserien markkinan muuttuessa liian ohueksi, jolloin oikeudenmukainen ja tehokas kaupankäynti ei ole mahdollista. Toisin sanoen, omaisuuseriä ei voida myydä tai ostaa tarpeen tullen. Likviditeetti voidaan näin ymmärtää joko rahoituslikviditeettinä tai kaupankäyntilikviditeettinä (Choudhry, 2018, 394).

Markkinariski syntyy rahoitusmarkkinoiden hintojen muutoksista. Kyseinen riski esiintyy sekä kaupankäyntikirjassa että pankkikirjassa. Markkinariskejä ovat muun muassa seuraavat: valuuttariski, osakeriski, uudelleensijoitusriski, ennakkomaksuriski sekä pankeille olennainen korkoriski. Korkoriski johtuu korkojen vaihteluista ja vaikuttaa suoraan kaikkiin tahoihin, jotka lainaavat tai sijoittavat varoja. Tätä keskeistä riskiä mitataan ja raportoidaan toisinaan erillään muista markkinariskeistä (Choudhry, 2020).

Muita olennaisia riskejä pankkitoiminnassa ovat malliriski ja operatiivinen riski. Pankit käyttävät rahoitusinstrumenttien hinnoitteluun ja suojaamiseen matemaattisia malleja. On mahdollisuus, että mallit ovat määritelty virheellisesti, ne perustuvat kyseenalaisiin oletuksiin tai ei kuvaa tarkasti markkinoiden todellista käyttäytymistä (Choudhry, 2020). CRR-asetuksen (EU) N:o 575/2013 4 artiklan 1 kohdan 52 alakohdan mukaan operatiivinen riski tarkoittaa riittämättömistä tai epäonnistuneista sisäisistä prosesseista, henkilöstöstä ja järjestelmistä tai ulkoisista tapahtumista aiheutuvaa tappioriskiä, mukaan lukien tieto- ja viestintätekniikkaan liittyvä riski, mutta pois lukien strateginen riski ja maineriski.

Edellä kuvatut riskityypit selittävät pankkitoiminnan riskiperusteisen luonteen ja sen, miksi pankkien vakavaraisuus ja riskienhallinta ovat vahvasti sääntelyohjattuja. Näiden riskienhallintaan ja pääomavaatimusten määrittelyyn perustuu kansainvälinen Basel-kehikko, jota tarkastellaan seuraavassa alaluvussa.

2.3.1 Basel-kehikko

Basel-kehikon tavoitteena on vahvistaa pankkien sääntelyä, valvontaa ja riskienhallintaa. Sen keskeisiä päämääriä ovat finanssijärjestelmän vakauden parantaminen, pankkikriisien todennäköisyyden pienentäminen sekä globaalin pankkisektorin resilienssin lisääminen. Basel-kehikko muodostuu kolmesta perättäisestä pankkisääntelysopimuksesta: Basel I, Basel II ja Basel III (Witte, 2024).

Basel I otettiin käyttöön vuonna 1988 Basel Committee on Banking Supervisionin (BCBS) toimesta. Sen tavoitteena oli vahvistaa kansainvälisen pankkijärjestelmän vakautta ja luotettavuutta sekä luoda yhdenmukaiset pääomavaatimukset eri maiden pankeille kilpailullisen epätasa-arvon vähentämiseksi (BCBS, 1988, 1). Sopimuksen koetut rajoitteet, erityisesti vähäinen riskiherkkyys herättivät nopeasti keskustelua, minkä seurauksena Basel-komitea käynnisti laajan uudistustyön. Useiden kuulemisasiakirjojen jälkeen Basel II -kehikko julkaistiin vuonna 2004 (Choudhry, 2020).

Basel II -kehikon tavoitteena oli edelleen vahvistaa kansainvälisen pankkijärjestelmän luotettavuutta ja vakautta siten, ettei pääomavaatimussääntelystä muodostuisi kilpailullista haittaa kansainvälisesti toimiville pankeille (BCBS, 2006, 2). Basel III on Basel II -kehikon laajennus ei niiden korvaaja. Näin ollen kehikon keskeiset tavoitteet, soveltamisala ja rakenne ovat säilyneet ennallaan (Choudhry, 2020). Basel II perustuu kolmeen pilariin, jotka käydään seuraavaksi läpi.

Pilari I sisältää vähimmäispääomavaatimukset, jotka laajensivat ja täsmensivät Basel I:n sääntöjä. Pilari I määrittelee luotto-, markkina- ja operatiivisten riskien vähimmäispääomavaatimukset, ohjaa riskipainotettujen saamisten (RWA) laskentaa sekä mahdollistaa lisäpääomapuskureiden asettamisen (Witte, 2024).

Pilari II muodostaa valvojan arviointiprosessin, jonka ytimessä on pankin sisäinen vakavaraisuuden arviointiprosessi (ICAAP). Sen keskeisenä tavoitteena on tunnistaa ne riskit, joita Pilari I ei kata, sekä varmistaa, että pankki arvioi kattavasti kaikki toimintansa kannalta olennaiset riskit. Pilari II:n sisältö ja soveltaminen määräytyvät pitkälti kansallisen valvontaviranomaisen ohjeistuksen perusteella.

Pilari II perustuu neljään perusperiaatteeseen, joista ensimmäinen liittyy pankin velvollisuuteen arvioida kokonaispääomansa riittävyyttä. Valvojan tehtävänä on tarkastella pankin sisäistä pääoman riittävyyden arviointia, asettaa odotuksia vähimmäispääomavaatimuksia täydentävästi sekä puuttua tilanteisiin riittävän varhaisessa vaiheessa, jotta pankin pääoma säilyy sen riskiprofiilin edellyttämällä tasolla (Choudhry, 2020.)

Pilari III keskittyy markkinakurin vahvistamiseen ja sisältää pankkien julkiset tiedonantovaatimukset. Sen tavoitteena on lisätä pankkien läpinäkyvyyttä ja antaa markkinaosapuolille valmiudet arvioida pankin riskiasemaa, pääomarakennetta ja kokonaisvaltaista vakavaraisuutta. Choudhryn (2020) mukaan Pilari III:n keskeinen sisältö voidaan jäsentää kolmeen osa-alueeseen. Ensinnäkin pankin on julkistettava tiedot pääomastaan, mukaan lukien eri pääomainstrumenttien luokittelu Tier 1- ja Tier 2 -eriksi. Toiseksi pankkien tulee raportoida pääomavaatimukset, jotka liittyvät luotto-, markkina- ja operatiivisiin riskeihin sekä näiden riskien suhteesta pankin kokonaispääomaan. Kolmanneksi Pilari III edellyttää pankkien kuvaavan kokonaisriskiasemansa, mikä sisältää muun muassa luotto-, markkina-, operatiiviset ja likviditeettiriskit sekä varainhankinnan ja varainkäytön rakenteen, erääntymisprofiilit, korkoriskin ja vastapuoliluottoriskin.

Basel-kehikko muodostaa kansainvälisen pankkisääntelyn perusrakenteen, mutta sen periaatteet eivät sellaisenaan ole suoraan sovellettavaa oikeutta Euroopan unionissa. EU:ssa Basel-kehikon vaatimukset on saatettu voimaan erityisesti luottolaitosdirektiivin (CRD) ja vakavaraisuusasetuksen (CRR) kautta, jotka täsmentävät pankkien riskienhallintaa, hallintojärjestelmiä ja valvontakäytäntöjä koskevat velvoitteet. Seuraavissa alaluvuissa käsitellään CRD-direktiiviä pankkien riskienhallintaa ja hallintojärjestelmiä koskevana sääntelynä sekä CRR-asetusta vakavaraisuus- ja riskimittausvaatimusten näkökulmasta.

2.3.2 CRD-direktiivi ja riskienhallinta

Direktiivi 2013/36/EU luottolaitosten toiminnan aloittamisesta ja harjoittamisesta sekä vakavaraisuusvalvonnasta (CRD IV -direktiivi) sisältää liiketoiminnan aloittamista ja palvelujen tarjoamista koskevat vaatimukset sekä säännökset viranomaisvalvonnasta, seuraamuksista ja luotettavasta hallinnosta. Lisäksi se kattaa lisäpääomavaatimukset erilaisten puskurien muodossa. Kyseinen direktiivi on pantava täytäntöön kansallisella lainsäädännöllä (Finanssivalvonta, 2021). CRD perustuu Basel -kehikkoon, joka on kansainvälisesti sovittu joukko toimenpiteitä, jotka on kehittänyt Basel -pankkivalvontakomitea. Direktiivin päätavoitteena ja kohteena on sovittaa yhteen kansalliset säännökset, jotka koskevat oikeutta harjoittaa luottolaitosten ja sijoituspalveluyritystentoimintaa, niiden ohjausta ja hallintoa koskevia yksityiskohtaisia sääntöjä sekä niiden valvontakehystä. Direktiivi 2013/36/EU sisältää muun muassa luottolaitosten sisäistä hallintoa, riskienhallintajärjestelyjä, sisäisiä valvontamekanismeja ja johdon vastuuta koskevia vaatimuksia.

Direktiivin (2013/36/EU) II osaston 2 a luvun 76–95 artikloissa säädetään riskienhallintaa koskevista vaatimuksista. Sen 76 artiklassa säädetään riskienhallinnasta hallintojärjestelmän tasolla sekä luodaan perusta uusien riskien käsittelylle. Artiklassa käydään läpi luottolaitosten ylimmän hallintoelimen roolia riskienhallinnassa: heidän on hyväksyttävä ja arvioitava laitoksen riskistrategiat ja -periaatteet. Hallintoelimen tulee varmistaa, että laitoksella on riittävät strategiat ja prosessit kaikkien olennaisten riskien tunnistamiseen ja hallintaan sekä ylimmän hallitonelimen jäsenten tulee osallistua aktiivisesti riskien käsittelyyn ja ymmärtää riskien vaikutukset luottolaitoksen kokonaisstrategiaan ja vakavaraisuuteen.

Artiklan toinen kohta edellyttää luottolaitoksilta riittäviä resursseja riskien tunnistamiseen, arviointiin ja mittaamiseen. Tämä sisältää muun muassa selkeästi määritellyt riskienhallintaprosessit ja raportointirakenteet sekä riittävät tietojärjestelmät riskidatan keruuseen ja analyysiin. 76 artiklan kohdissa 3 määritellään, että luottolaitoksella tulee olla riippumaton riskikomitea, jonka jäsenillä on oltava riittävät tiedot, taidot ja asiantuntemus, jotta he voivat täysimääräisesti ymmärtää laitoksen

riskistrategian ja riskinottohalun sekä valvoa niitä. Lisäksi CRD IV:ssä on säädetty laaja-alaisia vaatimuksien eri riskityyppien hallinnalle.

CRD luo vahvan institutionaalisen kehyksen, jossa pankit ovat jo tottuneet dokumentoimaan, valvomaan ja raportoimaan malleja sekä hallitsemaan merkittäviä riskejä. Tämän vuoksi AI Act:in tuomat vaatimukset, kuten dokumentaatio ja valvottavuus, integroituvat pankkien prosesseihin luontevasti. Pankkisektorin valmiit jo olemassa olevat governance – ja riskienhallintarakenteet luovat pohjan AI Act -vaatimusten täyttämiseksi.

2.3.3 CRR-asetus ja sisäiset mallit

CRR-asetus, eli Euroopan parlamentin ja neuvoston asetus (EU) N:o 575/2013 luottolaitosten vakavaraisuusvaatimuksista, on suoraan sovellettavaa lainsäädäntöä. Vakavaraisuusasetus kattaa omien varojen ja vähimmäisvakavaraisuusvaatimusten laskentaan, maksuvalmiuteen, vähimmäisomavaraisuusasteeseen sekä suuriin asiakasriskeihin liittyvät säännökset. Lisäksi se sisältää kattavat säännökset julkistamisvaatimuksista. Asetusta täydentävät Euroopan pankkiviranomaisen (EBA) valmistelemat ja EU -komission päätöksinä tai asetuksina annettavat tekniset sääntely -ja täytäntöönpanostandardit (Finanssivalvonta, 2021).

Asetukseen sisältyy artikloita, jotka käyvät läpi mallijärjestelmien yleisiä vaatimuksia. Asetuksen artikla 174 sisältää vaatimuksia koskien tilastollisia malleja, mikä käsittää esimerkiksi tekoälyn avulla laskettuja luottoluokitus pisteytyksiä. Sisäisten mallien perustana datan tulee olla täsmällistä, riittävää, luotettavaa ja historiallisesti kattavaa. Artiklassa 175 käydään läpi luottoluokitusmenetelmien dokumentointia. Sen mukaan laitoksen on dokumentoitava luottoluokitusmenetelmiensä rakenne ja toiminnalliset yksityiskohdat, luokituskriteerin valinnassa käytetyt perusteet ja valintaa tukenut analyysi, kaikki riskiluokitusprosessissa tapahtuneet merkittävät muutokset, sisäisesti käytettävät maksukyvyttömyyden sekä tappion määritelmät.

Asetuksen artikla 185 käsittelee sisäisten estimaattien validointia ja niiden vaatimuksia. Laitoksilla tulee olla luotettavat järjestelmät, joilla validoidaan erilaisten prosessien ja riskiparametrien estimoinnin tarkkuus sekä johdonmukaisuus. Riskienhallintaa ja valvontaa säädetään artiklassa 187, joka määrittää vaatimukset sisäisten mallien käytänteisiin, menettelyihin ja valvontajärjestelyihin. Nämä artiklat muodostavat yhdessä CRR:n ydinvaatimukset sisäisten mallien luotettavuudelle ja valvonnalle.

Operatiivista riskienhallintaa koskee myös asetuksen 323 artikla, jossa säädetään operatiivisen riskin hallintajärjestelmästä. Se määrittää, että laitoksella tulee olla oma dokumentointi, arviointi ja hallintajärjestelmä, jolle on asetettu selkeät vastuualueet. Laitoksen tulee muun muassa arvioida ja tunnistettava operatiiviset riski, joille laitos altistuu.

CRR-asetus sisältää lukuisia muitakin malleihin ja riskienhallintaan liittyviä vaatimuksia. Tässä luvussa tarkastellaan niitä artikloita, jotka ovat olennaisimpia pankkien malliperusteisen riskienhallinnan ja AI Act -sääntelyn vertailun kannalta.

2.4 Pankkien ja vakuutusyhtiöiden riskienhallinnan eroavaisuudet

Vakuutusyhtiöt ja pankit toimivat monilla liiketoiminta-alueilla lähellä toisiaan. Siksi on perusteltua, että eri toimialoille asetetut pääomavaatimukset ovat keskenään johdonmukaisia. Mikäli vaatimustasot poikkeavat merkittävästi toisistaan, riskinä on, että tiukemman sääntelyn piirissä oleva toimiala menettää liiketoimintaa kevyemmin säännellylle puolelle. Tämä voisi vääristää markkinoita ja johtaa sääntelyn kannalta ei-toivottuihin lopputuloksiin. Vaikka pankit ja vakuutusyhtiöt toimivat samalla sektorilla, eroaa heidän toimintansa toisistaan, mikä luo eroavaisuuksia riskienhallintaan (Kivisaari, ym.,2017, luku 5)

Pankkien riskienhallinnan lähtökohtana on riittävä pääomapuskuri, joka ylläpitää tallettajien ja muiden rahoittajien luottamusta pankin kykyyn suoriutua velvoitteistaan. Pankkien vastuut ovat tyypillisesti lyhytaikaisia ja altistuvat likviditeettiriskille, minkä

vuoksi pääoman merkitys korostuu erityisesti talletuspaon skenaarioissa. Vakuutusyhtiöillä taas vastuut ovat pitkäaikaisia, ja niiden pääomatarve määritellään tulevien kassavirtojen ja teknisten vastuuvelkojen perusteella. (Kivisaari, ym., 2017, luku 5)

Toinen huomattava ero saman sektorin toimijoiden välillä liittyy velkapääoman rooliin ja sen käyttäytymiseen. Pankit rahoittavat pitkät ja epälikvidit luottonsa lyhytaikaisella markkinarahalla, talletuksilla ja velkapääomalla. Sijoitukset ovat varainhankintaan nähden pitkäaikaisia ja ei-likvidejä. Vakuutusyhtiöissä rahoitus perustuu ennakkoon perittyihin vakuutusmaksuihin, joiden kassavirrat sovitetaan vastaamaan tulevia korvausmenoja. Näin vakuutusyhtiöiden sijoitukset ovat usein likvidimpiä kuin niiden pitkäaikaiset vastuut (Kivisaari, ym.,2017, luku 5).

Toimialakohtaisessa sääntelyssä löytyy myös eroja. Solvenssi II perustuu koko taseen laaja-alaiseen riskitarkasteluun, kun taas Basel III painottaa likviditeettiriskiä ja pääomapuskureita. Riskimittareiden suhteen Basel III käyttää pääosin standardoituja riskimittareita, kun taas Solvenssi II hyödyntää laajasti mallipohjaisia arvioita, mukaan lukien tekniset vastuuvelat. Lisäksi Basel III keskittyy lähinnä pääomavaatimuksiin, kun taas Solvenssi II tarkastelee velkojen arvostusta yksityiskohtaisemmin (Solvenssi II -direktiivi (2009/138/EY); Basel Committee on Banking Supervision, 2010).

Molemmat sääntelykehikot käyttävät vuositason arviointia ja riskiperusteisia pääomavaatimuksia, mutta niiden painotukset eroavat. Basel III on muuttanut merkittävästi pankkitoimintaa, kun taas Solvenssi II ei todennäköisesti aiheuta yhtä radikaaleja muutoksia vakuutusyhtiöissä, vaikka se uudistaa riskienhallinnan rakenteita. Molemmat kehikot luokittelevat varat samankaltaisiin kelpoisuusluokkiin, mutta luokitusten sisällössä ja käsittelyssä on huomattavia eroja (Kivisaari, ym.,2017, luku 5).

3 EU:N TEKOÄLYASETUS (AI ACT) SÄÄNTELYKEHYKSENÄ

Tässä luvussa tarkastellaan Euroopan unionin tekoälyasetusta (AI Act), joka muodostaa keskeisin sääntelykehyksen tekoälyn kehittämiselle ja käytölle. Asetus vaikuttaa suoraan finanssisektorin toimijoihin sekä niiden riskienhallinnan rakenteisiin ja velvoitteisiin. Luvun tarkoituksena on luoda pohja myöhemmälle analyysille siitä, miten AI Act:in vaatimukset kytkeytyvät pankkien ja vakuutusyhtiöiden olemassa olevaan sääntelyyn.

3.1 Tausta ja tavoitteet

EU:n tekoälyasetus (Artificial Intelligence Act, (EU) 2024/1689) on maailman ensimmäinen laajamittainen tekoälyn käyttöä säätelevä kehikko, minkä Euroopan parlamentti ja neuvosto antoi asetuksen koskien yrityksien ja organisaatioiden tekoälyn käyttöä 13.07.2024. Tekoälyasetuksen täytäntöönpanosta vastaavat sekä jäsenvaltioiden rahoituspalveluviranomaiset, että EU:N kolme finanssialan valvontaviranomaista: Euroopan pankkiviranomainen (EBA), Euroopan arvopaperimarkkinaviranomainen (ESMA) ja Euroopan vakuutus- ja lisäeläkeviranomainen (EIOPA) joita yhdessä kutsutaan Euroopan valvontaviranomaisiksi (ESAs) (Henderson, ym., 2024).

EU:n tekoälyasetuksen (1689,2024, EU) 8 artiklan mukaan unionin oikeudellinen kehys vahvistaa tekoälyä koskevat yhdenmukaistetut säännöt, mikä edistää tekoälyn kehittämistä, käyttöä ja käyttöönottoa sisämarkkinoilla sekä turvaa yleisten etujen ja perusoikeuksien korkean suojan tason.

Asetuksen tarkoituksena on parantaa sisämarkkinoiden toimintaa vahvistamalla yhtenäinen oikeudellinen kehys. EU:n jäsenvaltiot ovat harkinneet kansallisten sääntöjen hyväksymistä, jolloin kansallisesti toisistaan poikkeavat säännökset voivat pirstaloida sisämarkkinoita sekä heikentää tekoälyjärjestelmien vapaata liikkuvuutta, innovointia ja käyttöönottoa. Asetuksella, joka koskee kaikkia EU:n jäsenvaltioita, varmistetaan

yhdenmukainen ja korkea taso unionissa, suojaudutaan tekoälyjärjestelmien haitallisilta vaikutuksilta unionissa sekä tuetaan innovointia (1689, 2024, EU, Art. 1-3)

Tekoäly tuo mahdollisuuksia sekä taloudellisia, ympäristöön liittyviä ja yhteiskunnallisia hyötyjä kaikilla teollisuuden aloilla ja kaikessa sosiaalisessa toiminnassa. Samaan aikaan se voi aiheuttaa riskejä ja vahingoittaa unionin oikeudella suojattuja yleisiä etuja ja perusoikeuksia. Vahinko voi olla aineellista tai aineetonta, fyysistä, psykologista, yhteiskunnallista tai taloudellista vahinkoa (1689,2024, EU, Art. 5). Tekoälyllä voi olla huomattavia vaikutuksia yhteiskuntaa, etenkin suuririskisillä tekoälyjärjestelmillä, näillä tulee olla yhteiset säännöt, jotka ovat perusoikeuskirjan mukaisia ja syrjimättömiä (1689,2024, EU Art. 6)

3.2 Riskiperusteinen luokittelu

Tekoälyasetus perustuu riskiperusteiseen luokitteluun, eli se asettaa velvoitteita tekoälyjärjestelmille riskiperusteisesti. Tekoälyjärjestelmä voi olla kielletty sen riskien takia tai sen riski on niin vähäinen, että sillä ei ole asetuksen perusteella mitään velvollisuuksia. Säädöksessä on määritelty tekoälyjärjestelmille neljä riskitasoa: kielletty riski, suuri riski, vähäinen riski ja minimaalinen/ olematon riski (Traficom, 2025).

Tekoälyasetuksessa ei oteta kantaa minimaalisten riskien tekoälyjärjestelmien käytön sääntöihin. Tällaisia tekoälyjärjestelmiä ovat esimerkiksi tekoälyä hyödyntävät videopelit tai roskapostisuodattimet (European Commission, 2025)

Matalan riskin tekoälyjärjestelmille ei aseteta tiukkoja vaatimuksia, mutta niiden on täytettävä avoimuus- ja läpinäkyvyysvelvoitteet. Käyttäjälle on aina oltava selvää, että hän on vuorovaikutuksessa tekoälyjärjestelmän kanssa, ja järjestelmän tuottama sisältö on erotettava selkeästi ihmisen tuottamasta sisällöstä. Esimerkiksi chatbotin käytössä käyttäjälle tulee olla selvää, että hän on vuorovaikutuksessa koneen kanssa, jotta hän voi tehdä tietoon perustuvan päätöksen. Generatiivisten tekoälyn tarjoajan on varmistettava, että tekoälyn tuotettu sisältö on tunnistettavissa (Traficom, 2025).

Tietyt tekoälyjärjestelmät on kielletty niiden mahdollisten haitallisten vaikutusten vuoksi. Tekoälyä ei saa käyttää esimerkiksi manipuloivissa tai harhaanjohtavissa tekniikoissa,

ihmisten haavoittuvuuksien hyväksikäytössä, sosiaalisessa pisteytyksessä tietyissä käyttötapauksissa, rikollisuuden ennustamisessa profiloinnin perusteella, tunteiden tunnistamisessa työpaikoilla tai kouluissa, verkko- ja turvakameradatan kaapimisessa kasvojentunnistustietokantojen rakentamiseksi sekä ihmisten biometrisessä luokittelussa (Traficom, 2025). Näiden järjestelmien käyttö on kielletty, koska ne loukkaavat perusoikeuksia, yksityisyyden suojaa ja lisäävät joukkovalvonnan riskiä (1689,2024,EU Art. 42). Asetus kuitenkin mahdollistaa tarkoin rajatuissa poikkeustapauksissa kiellettyjen järjestelmien käytön tiukkojen ehtojen mukaisesti.

Suuririskiset tekoälyjärjestelmien käyttöönotto ja hallinta ovat asetuksen ydinaluetta, ja niitä koskevat velvoitteet ovat huomattavasti tiukempia kuin muiden riskiluokkien. Näiden järjestelmien tarkempi määrittely sekä niitä koskevat velvoitteet käsitellään seuraavassa alaluvussa.

3.3 Suuririskisen tekoälyjärjestelmien velvoitteet

Suuririskisillä tekoälyjärjestelmillä voi olla merkittävä haitallinen vaikutus terveyteen, turvallisuuteen ja perusoikeuksiin. Suuririskisen tekoälyjärjestelmän käyttöönotto edellyttää, että järjestelmä täyttää asetuksessa määritellyt tekniset vaatimukset sekä läpäisee tarvittaessa kolmannen osapuolen arvioinnin ennen markkinoille saattamista (Traficom, 2025).

Suuririskiset järjestelmät määritellään asetuksen liitteessä Annex III. Ne kattavat muun muassa kriittisen infrastruktuurin turvakomponentit, keskeisten yksityisten ja julkisten palveluiden, kuten lainanannon, edellyttämät päätöksentekojärjestelmät sekä työelämään liittyvät järjestelmät, joita käytetään rekrytoinnissa ja työntekijöiden hallinnoinnissa (European Commission, 2026).

Asetuksen mukaan suuririskisille järjestelmille on asetettu joukko tiukkoja velvoitteita. Ennen markkinoille saattamista järjestelmän kehittäjän tulee osoittaa, että järjestelmä on vaatimusten mukainen, ja markkinoilla ollessaan sen käyttöä valvovat sekä viranomaiset että järjestelmän käyttöönottaja. Käyttöönottajan vastuulla on varmistaa asianmukainen ihmisen suorittama valvonta ja järjestelmän seuranta sekä ilmoittaa mahdollisista

toimintahäiriöistä (European Commission, 2026). Suuririskisiä tekoälyjärjestelmiä koskevat keskeiset vaatimukset voidaan jäsentää seuraaviin osa-alueisiin:

1.Riskienhallintajärjestelmä (Art. 9)

Suuririskisille tekoälyjärjestelmille on luotava riskienhallintajärjestelmä, joka jatkuu koko elinkaaren ajan ja se on säännöllisesti ja järjestelmällisesti tarkastettava. Riskienhallintajärjestelmään tulee sisältyä riskien tunnistaminen ja analysointi, joita suuririskinen tekoälyjärjestelmä voi aiheuttaa liittyen terveyteen, turvallisuuteen tai perusoikeuksiin. Järjestelmän tulee myös huomioida riskit, jotka syntyvät tekoälyjärjestelmän käyttöönotosta. Riskienhallintatoimenpiteitä määriteltäessä tulee huomioida mahdollisuudet riskien poistamiseen tai niiden vähentämiseen. Tekoälyjärjestelmiä on testattava asianmukaisessa testiympäristössä ennen sen käyttöönottoa, jotta ne toimivat asiamukaisesti.

2. Data ja datan hallinta (Art. 10)

Suuririskinen tekoälyjärjestelmä, joka käyttää dataa oppiakseen tulee täyttää kohdissa 2-5 määritellyt laatuvaatimukset. Datanhallinta – ja hallinnointikäytäntöjen tulee erityisesti huomioitava muun muassa datan laatu (keruuprosessi, alkuperä, tarkoitus), asiaankuuluvat tietojenkäsittelytoimet, mahdollisten vinoumien selvittäminen ja puutteellisten tietojen tunnistaminen. Koulutus-, validointi- ja testausdatajoukkojen vaatimuksiin kuuluu: riittävän edustavia, käyttötarkoitukseen merkityksellisiä, asianmukaiset tilastolliset ominaisuudet ja mahdollisimman virheettömiä ja täydellisiä. Mikäli vinoutumien havaitseminen ja korjaaminen vaatii erityisten henkilötietojen käsittelyä, tulee toiminnan täyttää kaikki siihen tarkoitetut ehdot.

4.Tekninen dokumentaatio (Art.11)

Järjestelmästä on laadittava kattava tekninen dokumentaatio, jonka avulla valvontaviranomaiset voivat arvioida vaatimustenmukaisuuden. Dokumentaation tulee osoittaa, että järjestelmä täyttää asetuksen tekniset ja organisatoriset edellytykset.

4.Lokitiedot ja jäljitettävyys (Art.12)

Järjestelmän toiminnan tulee olla läpinäkyvää ja jäljitettävää. Lokitietojen tarkoituksena on mahdollistaa järjestelmän päätösten arviointi sekä virheiden tai haittatilanteiden jälkikäteinen selvittäminen.

5.Avoimuus ja tietojen antaminen käyttöönottajille (Art. 13)

Tekoälyjärjestelmä on suunniteltava ja kehiteltävä siten, että niiden toiminta on avointa, jolloin käyttöönottajat voivat tulkita järjestelmän tuotoksia ja käyttää näitä asianmukaisesti. Tekoälyjärjestelmissä tulee olla selkeät käyttöohjeet, jossa tietojen tulee olla käyttöönottajien kannalta olennaisia, esteettömiä ja ymmärrettäviä

6. Ihmisen suorittama valvonta (Art.14)

Luonnolliset henkilöt tulee valvoa järjestelmien käyttöä, millä pyritään ehkäisemään järjestelmistä aiheutuvia riskejä. Valvontatoimenpiteet suhteutetaan järjestelmien riskeihin, itsenäisyyden tasoon ja käyttöympäristöön.

7.Tarkkuus, vakaus ja kyberturvallisuus (Art.15)

Järjestelmien on toimittava luotettavasti ja turvallisesti myös poikkeustilanteissa. Ne on suunniteltava ja kehitettävä niin, että ne saavuttavat asianmukaisen turvallisuuden tason. Tähän kuuluu kestävyys mahdollisia kyberhyökkäyksiä vastaan.

Suuririskisiä tekoälyjärjestelmiä koskevia velvoitteita on asetuksessa useita, mutta tässä luvussa keskitytään niihin vaatimuksiin, jotka ovat tutkimuksen kannalta olennaisimmat erityisesti finanssialan riskienhallinnan näkökulmasta. Tarkastellut velvoitteet tähtäävät siihen, että suuririskiset tekoälyjärjestelmät toimivat turvallisesti ja läpinäkyvästi ja että niiden käyttöön liittyvät riskit ovat asianmukaisesti hallittuja. Tämä korostuu erityisesti finanssialalla, jossa suuririskisiin luokitellut järjestelmät voivat vaikuttaa suoraan asiakkaiden oikeuksiin ja yhdenvertaiseen kohteluun.

3.4 Suuririskiset tekoälyjärjestelmät finanssialalla

Tekoälyjärjestelmien käyttöönotto kiihtyy maailmanlaajuisesti, myös pankeissa ja vakuutusyhtiöissä. Tekoälyn kehitys tarjoaa merkittäviä hyötyjä erityisesti vakuutussektorilla koko vakuutusarvoketjussa. Sen avulla voidaan esimerkiksi vahvistaa vakuutuksenottajien sitoutumista yksilöllisemmän asiakasvuorovaikutuksen kautta, saavuttaa kustannussäästöjä vakuutusten hallinnassa ja korvauskäsittelyssä sekä kehittää riskien valintaa ja hinnoittelua aiempaa tarkemmaksi (EIOPA, 2024, 24–25).

AI Actin liitteessä III määritellään korkean riskin tekoälyjärjestelmien käyttötapaukset. Finanssisektorin kannalta erityisen olennaisia ovat järjestelmät, joita käytetään luottokelpoisuuden tai luottopisteiden arviointiin, sekä henki- ja sairausvakuutusten riskinarvioinnissa ja hinnoittelussa käytettävät järjestelmät. Nämä kuuluvat asetuksessa korkean riskin kategoriaan. Korkean riskin järjestelmille on ominaista, että niiden käyttö voi altistaa henkilön syrjinnälle erityisesti hänen taloudellisen profiilinsa perusteella (Almada, 2025, 110; Deloitte, 2023).

Keskeinen kysymys finanssialalla on, milloin käytetty malli on katsottava AI Actin tarkoittamaksi tekoälyjärjestelmäksi ja siten asetuksen velvoitteiden piiriin kuuluvaksi. Asetuksen 3 artiklan 1 kohdan mukaan tekoälyjärjestelmällä tarkoitetaan:

”konepohjaista järjestelmää, joka on suunniteltu toimimaan käyttöönoton jälkeen vaihtelevilla autonomian tasoilla ja jossa voi ilmetä mukautuvuutta käyttöönoton jälkeen ja joka päättelee vastaanottamastaan syötteestä eksplisiittisiä tai implisiittisiä tavoitteita varten, miten tuottaa tuotoksia, kuten ennusteita, sisältöä, suosituksia tai päätöksiä, jotka voivat vaikuttaa fyysisiin tai virtuaalisiin ympäristöihin;”

EU:n AI Office on antanut tekoälyn määritelmästä ei-sitovaa ohjeistusta. Ohjeistuksen keskeisen tulkinnan mukaan matemaattiseen optimointiin perustuvia menetelmiä ei välttämättä pidetä oikeudellisessa mielessä tekoälynä, koska niiden katsotaan kuuluvan perusmuotoisen tietojenkäsittelyn piiriin. Toisaalta voidaan esittää, että AI Actin laaja tekoälyn määritelmä kattaa myös tilastolliset mallit sekä automatisoidut päätöksentekojärjestelmät, jotka muodostuvat esimerkiksi ulkoisista pisteytyksistä, sisäisistä tilastollisista malleista, heuristiikoista ja säännöistä. Tällaisia menetelmiä hyödynnetään muun muassa luottopisteytyksessä, minkä vuoksi toimijoiden on

perusteltua olettaa niiden kuuluvan AI Actin soveltamisalaan siihen saakka, kunnes asiasta annetaan sitova tuomioistuinratkaisu (Hacker & Eber, 2025, 5–6).

Luottokelpoisuuden ja luottopisteiden arviointi on finanssisektorilla keskeistä taloudellisen kestävyyden arvioinnin ja päätöksenteon näkökulmasta. Perinteiset luottoriskimallit ovat usein nojanneet subjektiiviseen arviointiin ja rajalliseen tietopohjaan. Näihin perinteisiin järjestelmiin liittyy useita rajoitteita, kuten joustamattomuus luottokelpoisuuden arvioinnissa sekä puutteellinen kyky huomioida lainanottajan laadullisia ja määrällisiä ominaisuuksia kattavasti (Darwish, 2025, 586; Nallakaruppan ym., 2024, 2).

Vastaavasti AI Act luokittelee korkean riskin järjestelmiksi myös tekoälyjärjestelmien käytön luonnollisiin henkilöihin kohdistuvassa riskinarvioinnissa ja hinnoittelussa henki- ja sairausvakuutuksen yhteydessä (EIOPA, opinion, 2024, 3). Sammiudinin ym. (2023) mukaan vakuutusyhtiöiden näkökulmasta on olennaista määrittää mahdollisimman tarkasti vakuutuksella katettava määrä sekä vakuutuksesta aiheutuvat kustannukset, joiden arviointi perustuu useisiin eri tekijöihin. Tässä yhteydessä koneoppimisella voi olla merkittävä rooli, sillä mallit voidaan kouluttaa aiemman aineiston perusteella hyödyntämään historiallista dataa vakuutusten hinnoittelun tukena. Näin voidaan parantaa hinnoittelun tarkkuutta, vähentää manuaalisen työn tarvetta sekä tehostaa toimintaa ja vahvistaa sen tuottopotentiaalia.

Luottopisteytyksen ja vakuutusten hinnoittelun lisäksi korkean riskin tekoälyjärjestelmää voidaan hyödyntää finanssisektorilla myös petosanalytiikassa. Perinteiset petosten havaitsemismenetelmät ovat usein manuaalisia, minkä vuoksi ne ovat aikaa vieviä, kalliita, epätarkkoja ja käytännössä vaikeasti toteutettavia. Tekoälyn kehityksen myötä koneoppimista ja laajojen aineistojen analysointia on alettu hyödyntää finanssisektorilla petollisen toiminnan havaitsemisessa (Ali ym., 2022, 2). Ali ym. (2022) toteavat, että finanssisektorilla tyypillisiä petosmuotoja ovat esimerkiksi luottokorttipetokset, joissa maksukortteja käytetään oikeudettomiin maksutapahtumiin, mistä aiheutuu huomattavia tappioita sekä pankeille että kortinhaltijoille. Vakuutusalalla keskeiset petokset liittyvät puolestaan petollisiin vakuutuskorvausvaatimuksiin erityisesti terveydenhuollon ja autovakuutusten yhteydessä.

Lisäksi korkean riskin kategoriaan kuuluu tekoälyjärjestelmiä, joita käytetään henkilöiden rekrytointiin sekä sellaiseen päätöksentekoon, joka vaikuttaa työsuhteen ehtoihin. Pankkien ja vakuutusyhtiöiden näkökulmasta tämä merkitsee uudenlaisen, osittain päällekkäisen sääntelykerroksen muodostumista. Samalla finanssialan valvojien rooli laajenee, mikä edellyttää niiltä uudenlaista teknistä ja oikeudellista osaamista. Finanssisektorin toimijoiden on huomioitava myös AI Actin kieltämät tekoälyjärjestelmät ja erityisen ongelmalliset käyttötavat, kuten sosiaalinen pisteytys, kasvojentunnistustietokantojen luominen sekä manipuloivien tekniikoiden hyödyntäminen (Almada, 2025, 111; Henderson ym., 2024).

3.5 AI Actin vaikutukset finanssisektorille ja asetuksen noudattamisen edellytykset

AI Act tulee sovellettavaksi suoraan finanssipalvelualan toimijoihin ilman, että sen voimaansaattaminen edellyttää erillistä kansallista lainsäädäntöä. Finanssisektorin toimijoihin kuuluvat muun muassa pankit ja muut kuin pankkilainanantajat, välittäjät, vakuutusyhtiöt ja vakuutusmeklarit sekä varainhoitajat ja neuvonantajat, erityisesti silloin, kun innovatiivinen teknologia muodostaa keskeisen osan niiden liiketoimintaa.

AI Actin käyttöönotto asettaa finanssialan toimijoille merkittäviä vaatimuksia. Keskeisenä haasteena on varmistaa, että sekä uudet että jo olemassa olevat tekoälyjärjestelmät täyttävät asetuksen tiukat standardit esimerkiksi läpinäkyvyyden, oikeudenmukaisuuden, vastuuvelvollisuuden ja valvonnan osalta. Finanssilaitosten käyttämien tekoälyjärjestelmien määrä vaihtelee huomattavasti muun muassa organisaation koon, sen toiminta-alueen maantieteellisen laajuuden sekä digitaalisen transformaation vaiheen mukaan (Consultancy, 2025).

Niiden finanssilaitosten, jotka ovat kehittäneet tai ottaneet käyttöön tekoälyjärjestelmiä jo ennen asetuksen soveltamisen alkamista, on arvioitava uudelleen, täyttävätkö nämä järjestelmät AI Actin vaatimukset, ja tarvittaessa mukautettava niitä vastaamaan asetuksen edellytyksiä. Erityisesti korkean riskin järjestelmiin liittyy lisävaatimuksia, kuten velvollisuus tiedottaa asiakkaille heidän tietojensa käytöstä sekä siitä, miten tekoälyjärjestelmät muodostavat suosituksia ja päätöksiä. Asetusta sovelletaan myös

kolmansien osapuolten tekoälyjärjestelmiin. Jaetun vastuun mallin mukaisesti sekä järjestelmän tarjoajalla että sitä käyttävällä finanssilaitoksella on omat vastuunsa vaatimustenmukaisuuden varmistamisessa. Toisaalta AI Act voi myös tarjota finanssialan toimijoille mahdollisuuden vahvistaa asiakkaiden luottamusta toimintaansa (Hacker & Eber, 2025, 25).

Asetuksen noudattaminen edellyttää finanssilaitoksilta useita käytännön toimenpiteitä. Organisaatioiden tulisi tehdä AI Actin vaikutustenarviointi ja suhteuttaa sen vaatimukset olemassa oleviin käytäntöihin, menettelyihin ja ohjelmiin, kuten malliriskienhallintaan, datahallintaan ja kolmannen osapuolen riskienhallintaan, joissa voi esiintyä riippuvuuksia ja päällekkäisyyksiä (Consultancy, 2025). Luottopisteytyksen ja vakuutustoiminnan osalta AI Actia aletaan soveltaa elokuussa 2026. Käyttöönoton näkökulmasta vankan ja ketterän infrastruktuurin merkitys korostuu erityisesti automatisoitujen luottopäätösten yhteydessä, minkä vuoksi mallinnus-, compliance- ja hallintajärjestelmiä on päivitettävä. Näin voidaan varmistaa AI Actin mukaisten toimintojen oikea-aikainen ja asianmukainen käyttöönotto (Hacker& Eber, 2025, 27).

Lisäksi finanssilaitosten on koulutettava henkilöstöään tekoälyn eettisestä käytöstä ja AI Actin erityisvaatimuksista. Organisaatioiden tulee tunnistaa kaikki EU:ssa käyttämänsä tekoälyjärjestelmät, mukaan lukien kolmansien osapuolten järjestelmät, ja ryhmitellä ne asetuksessa määriteltyihin riskiluokkiin. Tekoälyjärjestelmiä koskeva dokumentaatio on tarkistettava ja tarvittaessa täydennettävä siten, että se vastaa asetuksen standardeja ottaen huomioon finanssilaitoksen roolin joko järjestelmän tarjoajana tai käyttöönottajana (Consultancy, 2025).

EU:n ulkopuolelle sijoittautuneiden finanssilaitosten on lisäksi arvioitava EU:n vaatimusten ja niiden kotivaltion sekä muiden toimintamaiden sääntelyn väliset erot ja laadittava strategia kaikkien sovellettavien vaatimusten noudattamiseksi. Tämän strategian tulisi olla dokumentoituna laitoksen tekoälyn käyttöä koskevassa politiikassa (Consultancy, 2025). Samalla organisaatioiden on arvioitava tekoälyjärjestelmien käyttämät tietoaineistot sen varmistamiseksi, että ne ovat tarkkoja, kattavia, oikeudenmukaisia ja puolueettomia sekä että niiden käyttö on tietosuojasääntelyn mukaista. Lisäksi on tunnistettava, mitä muutoksia toimintatapoihin, kuten tiedonhallintaan tai järjestelmälokeihin, on tehtävä asetuksen jatkuvan noudattamisen varmistamiseksi. Myös lisäasiakasviestinnän tarve on arvioitava ja sitä varten laadittava

asianmukainen viestintäsuunnitelma. Tämän lisäksi organisaatioiden on pohdittava, kuinka AI Actin noudattamiseksi toteutetut toimenpiteet suhteutuvat niiden globaaliin tekoälyohjelmaan ja voidaanko tekoälystandardeja soveltaa johdonmukaisesti koko organisaatiossa (Consultancy, 2025).

Viranomaisilla on keskeinen rooli AI Actin toimeenpanossa ja sen jatkokehityksessä. Euroopan komissiolle on annettu valtuutus päivittää AI Actia säännöllisesti tarpeen mukaan, mukaan lukien korkean riskin käyttötapausten luettelo, jota voidaan tulevaisuudessa laajentaa. Lisäksi useita AI Actissa käytettyjä käsitteitä, kuten datan hallintaan liittyviä edustavuuden ja virheettömyyden vaatimuksia, on tarkoitus täsmentää teknisten standardien avulla. Näiden standardien odotetaan konkretisoivan asetuksen velvoitteita ja tarjoavan toimintakehyksen, jonka avulla vaatimukset voidaan sisällyttää finanssialan toimijoiden luottopisteytystä ja vakuutustoimintaa koskeviin malleihin ja menettelyihin. Tämän vuoksi jokaisen luotonmyöntö- tai vakuutustoimijan, joka pyrkii säilyttämään toimintansa ajantasaisena ja vaatimustenmukaisena, tulisi seurata tarkasti AI Actin kehitystä sekä siihen liittyvää standardointia (Hacker & Eber, 2025, 28).

4 INSTITUTIONAALINEN TEORIA

Institutionaalinen teoria toimii tässä tutkimuksessa analyysikehyksenä, jonka avulla voidaan tarkastella, miksi AI Actin velvoitteet kohdistuvat pankkeihin ja vakuutusyhtiöihin eri tavoin, vaikka sääntelykehikko on sama. Teoria mahdollistaa sääntelyn vaikutusten tarkastelun paitsi muodollisina vaatimuksina myös toimintaa ohjaavina normeina, paineina ja legitimiteettivaatimuksina. Tätä taustaa vasten seuraavissa alaluvuissa käsitellään institutionaalisen teorian keskeiset mekanismit ja legitimiteetin muodot.

4.1 Institutionaalisen teorian lähtökohdat

Institutionaalinen teoria on vakiinnuttanut asemansa keskeisenä selitysmallina niin yksilöiden kuin organisaatioidenkin toiminnalle. Kyseinen teoria on monipuolinen ja dynaaminen, jota on sekä yhdistetty että vertailtu muihin lähestymistapoihin (Dacin, etc. 2002, 45).

Meyer ja Rowan (1977) lanseerasivat ”uuden institutionaalisen teorian” esittämällä, että organisaatiot luovat kertomuksia toiminnastaan sillä periaatteella, mitä ne uskovat vaikutusvaltaisten sidosryhmien haluavan kuulla. Näyttäytyäkseen legitiimeinä organisaatiot omaksuvat käytäntöjä ja piirteitä, jotka voivat olla toiminnallisesti tehokkaita tai tehottomia, mutta joita ne uskovat keskeisten resurssien tarjoajien pitävän asianmukaisina. DiMaggio ja Powell (1983) laajensivat tätä näkemystä ehdottamalla, että yhteiskunnalliset rakenteet sekä organisaatiotoimijoiden kollektiivinen rationaalisuus johtaa organisaatiokenttien muotoutumiseen homogeeniseksi.

DiMaggion ja Powellin (1983) mukaan institutionaaliselle isomorfiselle muutokselle on kolme mekanismia: pakottava, mimeettinen ja normatiivinen. Pakottava isomorfismi on peräisin hallitukselta ja muilta vaikutusvaltaisilta organisaatioilta, jotka sääntelevät tai muuten suoraan rajoittavat organisaatioiden toimintaan. Pakottava isomorfismi näkyy esimerkiksi tilanteessa, jossa pankin on muutettava AI-mallin dokumentaatio AI Actin

vaatimusten mukaiseksi, koska valvova viranomainen (esim. EBA tai EKP) voi muutoin puuttua mallin käyttöön tai jopa edellyttää sen poistamista käytöstä. Tällöin muutos ei perustu organisaation vapaaehtoiseen päätökseen, vaan sääntelyn ja valvonnan aiheuttamaan pakkoon.

Mimeettinen isomorfismi johtuu organisaatioiden luontaisesta epävarmuudesta, koska toimijat eivät tiedä mitä tulevaisuus tuo tulessaan, heillä on taipumus katsoa ympärilleen menestyviltä vihjeitä siitä, mitä heidän tulisi tehdä menestyäkseen. AI Actin käyttöönotossa mimeettinen isomorfismi voi ilmetä siten, että organisaatiot alkavat jäljitellä toistensa AI-governance-ratkaisuja. Jos jokin finanssialan toimija onnistuu rakentamaan toimivan mallin, muut voivat kopioida sen vähentääkseen epävarmuutta ja riskiä omissa ratkaisuissaan, ei siksi, että asetus sitä edellyttäisi, vaan koska toisen toimijan esimerkki tarjoaa ”turvallisen” suunnan.

Normatiivista isomorfismia esiintyy organisaatioiden päätöksentekijöiden ammattimaistumisen vuoksi tai johtajien taipumuksen vuoksi toteuttaa johtoryhmänsä jäseniltä odotettuja ideoita, normeja ja kieltä (Hambrick, ym., 2004, 314). AI Act voi vahvistaa normatiivista isomorfismia siten, että organisaatiot alkavat edellyttää samanlaisia sertifikaatteja ja osaamisvaatimuksia tekoälyn hallintaan liittyvissä rooleissa. Kyse ei ole lain suorasta vaatimuksesta, vaan alan odotuksesta “näin kuuluu toimia”, mikä heijastaa normatiivista painetta yhdenmukaistaa käytäntöjä.

Organisaatiorakenteet syntyvät rationaalistettujen ja institutionaalisten sääntöjen heijastumina. Tällaisten sääntöjen kehittyminen nykyaikaisissa valtioissa ja yhteiskunnissa selittää osaltaan muodollisten organisaatiorakenteiden laajenemisen ja lisääntyneen monimutkaisuuden. Institutionaaliset säännöt toimivat myytteinä, jotka organisaatiot omaksuvat saadakseen legimiteettiä, resursseja, vakautta ja paremmat selviytymismahdollisuudet (Meyey, J.W., & Rowan, 1977, 340).

Organisaatiot reagoivat ympäristöön, joka koostuu muista organisaatioista, jotka puolestaan reagoivat omaan ympäristöönsä. Prosessia, jossa alan yksiköt alkavat muistuttaa toisiaan, kuvaa käsite isomorfismi (DiMaggio, Powell, 1983) Isomorfismi on pakottava prosessi, joka saa yhden yksikön muistuttamaan muita yksiköitä, joihin kohdistuu samanlaisia ympäristöpaineita (Hawley, 1968). Isomorfismi voi syntyä kun ei-

optimaaliset muodot karsiutuvat pois tai kun organisaatiopäättäjät oppivat jäljittelemään muiden kehittämiä ratkaisuja.

Kaikki institutionaalinen yhdenmukaisuus ei johdu pakottavista tekijöistä, esimerkiksi epävarmuus on voimakas yhdenmukaistava tekijä. Kun ympäristö muuttuu arvaamattomaksi tai tavoitteet ovat epäselviä, organisaatiot voivat alkaa jäljitellä toisiaan. Organisaatio voi olla tietoinen jäljittelystä tai se voi tapahtuma tahattomasti esimerkiksi työntekijöiden vaihtuvuuden tai konsulttien kautta. Yritykset omaksuvat tapoja tai innovaatioita legitimaation saavuttamiseksi ja näyttääkseen toimivansa alan parhaiden käytäntöjen mukaisesti. Organisaatiot pyrkivät usein mallintamaan itseään muiden saman kentän organisaatioiden mukaan, jotka ne kokevat legitiimeiksi tai menestyviksi (DiMaggio, Powell, 1983,150-151)

4.2 Legitimaatio

Legitimiteetille on vuosien aikana esitetty useita määritelmiä, jotka vaihtelevat täsmällisyydellään. Yksi varhaisin määritelmä on Maurer 1971 ”legitimaatio on prosessi, jonka kautta organisaatio oikeuttaa olemassaolonsa vertaiselle tai ylemmälle järjestelmälle”. Myöhemmin Pleffer kollegoidensa (Doeling & Pleffer, 1975; Pleffer & Salancik 1981) kanssa painotti kulttuurillista yhdenmukaisuutta. Legitimiteetti on yleistetty havainto tai oletus siitä, että toimijan tekemät teot ovat toivottavia, asianmukaisia tai sopivia jonkin sosiaalisesti rakentuneen normien, arvojen, uskomusten ja määritelmien järjestelmän puitteissa. Suchman (1995) erottaa legitimiteetin kolme ulottuvuutta: pragmaattinen, moraalinen ja kognitiivinen.

Pragmaattinen legitimiteetti perustuu sidosryhmien tarkastellessa omaa etuaan: organisaatio koetaan legitiimiksi silloin, kun sen toiminta tuottaa sidosryhmille konkreettista hyötyä. Yksinkertainen muoto tästä on vaihdantalegitimiteetti, jossa sidosryhmät tukevat organisaatiota, koska organisaation koetaan tuottavan arvokkaita palveluja, etuja tai resursseja. Kun sidosryhmät kokevat, että organisaatio huomioi heidän tarpeensa, esimerkiksi antamalla heille mahdollisuuksia vaikuttaa päätöksenteossa, puhutaan vaikutuslegitimiteetistä. Kolmas muoto on dispositionaalinen legitimiteetti, mikä voi suojata organisaatiota vaikeina aikoina. Tämä perustuu siihen, että organisaatio

nähdään luonteeltaan rehellisenä ja luotettavana toimijana (Suchman, 1995). Vakuutusyhtiöiden kohdalla tämä voi näkyä esimerkiksi AI -mallin käyttöönotossa, mikä nopeuttaa korvauspalvelua: asiakas hyötyy, saa korvauksen nopeasti ja asiakaskokemus paranee. Konkreettinen hyöty saa asiakkaat hyväksymään AI:n käytön, jolloin organisaation toiminta koetaan omaa etua palvelevaksi.

Moraalinen legitimiteetti heijastaa organisaation normatiivista kehitystä ja sen aktiviteetteja. Sen voidaan ajatella olevan arvio, onko aktiviteetti ”oikea asia tehdä”. Yleisesti ottaen moraalinen legitimiteetti ottaa yhden muodon kolmesta: tulosten ja seurausten arviointi, tekniikoiden ja menetelmien arviointi sekä kategorioiden ja rakenteiden arviointi. Seurauslegitimiteetti perustuu siihen, että organisaation toimintaa arvioidaan sen tuottamien lopputulosten perusteella, jolloin organisaation tulokset koetaan laadukkaiksi, joko markkinoiden asiakkaiden tai sääntelyviranomaisten näkökulmasta. Menettelytapoihin perustuva legitimiteetti syntyy organisaation noudattaessa kulttuurillisesti hyväksyttyjä ja sosiaalisesti arvostettuja toimintatapoja riippumatta lopputulosten mitattavuudesta. Rakenteellinen legitimiteetti perustuu taas organisaation tunnistettavaan ja kulttuurillisesti hyväksyttyyn organisaatiokategoriaan, jonka rakenteelliset piirteet viestivät kyvykkyyttä ja sopivuutta tehtävään (Suchmann, 1995). Pankeilla moraalinen legitimiteetti voi liittyä esimerkiksi luotonantoon. He voivat linjata, etteivät myönnä luottoja yrityksille, joiden toiminta aiheuttaa ympäristö- tai ihmisoikeusrikkomuksia. Linjaus ei välttämättä maksimoi pankin voittoja, mutta se vastaa yhteiskunnan normeja oikeudenmukaisesta ja vastuullisesta toiminnasta. Näin ollen eri sidosryhmät kokevat pankin toiminnan eettiseksi, mikä vahvistaa sen moraalista legitimiteettiä

Kognitiivinen legitimiteetti perustuu ymmärrykseen, että organisaation toiminta koetaan ymmärrettäväksi, ennakoitavaksi ja kulttuurillisesti sopivaksi. Kognitiivinen legitimiteetti on usein voimakkain, mutta myös vaikeimmin saavutettava legitimiteetin muoto. Kognitiivinen legitimiteetti voi ilmetä kahdessa muodossa: ymmärrettävyys ja itsestäänselvyys. Ymmärrettävyydellä tarkoitetaan organisaation toiminnan ”järkeen käymisestä” sidosryhmien näkökulmasta. Itsestäänselvyydellä tarkoitetaan tilannetta, jossa organisaation olemassaolo ja toiminta koetaan niin luonnolliseksi, jolloin sen haastaminen on käytännössä mahdotonta. (Suchhman, 1995). Vakuutusyhtiöiden kohdalla kognitiivinen legitimiteetti näyttäytyy esimerkiksi sidosryhmien hyväksyntänä

yhtiöiden käyttämään tilastolliseen riskien arviointiin, mallintamiseen ja datan analysointiin.

Finanssisektori on institutionaalisesti vahvasti säännelty toimiala, jossa legitimiteetin ylläpitäminen on kriittistä. AI Act lisää uuden ulottuvuuden legitimiteettivaatimuksiin, sillä tekoälyjärjestelmien läpinäkyvyys, oikeudenmukaisuus ja valvottavuus vaikuttavat suoraan asiakkaiden luottamukseen. Pankeille ja vakuutusyhtiöille legitimiteetti muodostuu paitsi sääntelyn noudattamisesta (pragmaattinen ja moraalinen legitimiteetti) myös siitä, että niiden tekoälyn käyttö koetaan yhteiskunnallisesti hyväksyttäväksi ja ennakoitavaksi (kognitiivinen legitimiteetti).

4.3 Vakuutusyhtiöiden ja pankkien vertailu institutionaalisesta näkökulmasta

Kun tarkastellaan pankkien ja vakuutusyhtiöiden välisiä eroja legitimiteetin näkökulmista, on se oleellinen lähtökohta AI Actin vaikutuksiin finanssialan toimijoihin tarkasteluun. Pankit toimivat perinteisesti vahvasti säännellyssä ympäristössä, jossa niiden toiminnan jatkuvuus kytkeytyy vahvasti yhteiskunnalliseen vakauteen ja luottamukseen. Tässä kontekstissa pankkien legitimiteetti rakentuu ennen kaikkea regulatiivisen ja moraalisen legitimiteetin varaan. Pankkien on osoitettava, että he noudattavat lainsäädäntöä ja toimivat viranomaisten määrittelemällä tavalla. AI Act pakottaa pankkeja osoittamaan, että heidän AI-järjestelmänsä ovat hallittuja, jäljitettäviä ja eettisesti hyväksyttäviä.

Vakuutusyhtiöiden legitimiteettitarpeet eroavat suhteessa pankkeihin. Vakuutustoiminta on laajasti säännelty, mutta niiden toiminnan perustana on pitkälti tekninen ja kognitiivinen legitimiteetti. Vakuutusyhtiöiden toiminnan ydin perustuu tilastolliseen pätevyyteen, dataperusteisuuteen ja matemaattisesti johdonmukaiseen riskien arviointiin. Näin ollen vakuutusyhtiöiden AI-ratkaisut voivat asettua arvioitavaksi teknisen toimivuuden kannalta. Lisäksi vakuutusyhtiöt voivat kohdata eettisiä legitimiteettihaasteita, sillä AI -pohjaiset hinnoittelu – ja riskimallinnukset voivat synnyttää syrjiviä tuloksia. Näin ollen vakuutusyhtiöt tasapainottelevat teknisen uskottavuuden ja eettisen kestävyyden välillä.

Institutionaalisen teorian näkökulmasta pankkien ja vakuutusyhtiöiden väliset erot voidaan jäsentää regulatiivisen, normatiivisen ja kognitiivisen pilarin kautta. Pankkien näkökulmasta keskeinen pilari on regulativiinen, sillä pankkien sujuva liiketoiminta kytkeytyy makrotaloudelliseen vakauteen ja finanssijärjestelmän turvallisuuteen. AI Act vahvistaa entisestään pilarin merkitystä, sillä pankkien tulee osoittaa noudattavansa sääntelyä ja hallitsevansa asetukseen liittyvät riskit. Lisäksi pankkeihin kohdistuu normatiivinen paine toimia vastuullisesti ja läpinäkyvästi, mikä toisaalta korostaa moraalisen legitimiteetin merkitystä. Vakuutusyhtiöillä keskeisempi pilari on kognitiivinen: vakuutusyhtiöiden odotetaan toimivan rationaalisella ja dataan perustuvalla tavalla, jolloin legitimiteetti rakentuu mallien odotetun pätevyyden ja ymmärrettävyyden ympärille. Normatiiviset odotukset ovat siltä osin läsnä, että ne korostuvat tilanteissa, joissa tekoälyn käyttö uhkaa tuottaa epäoikeudenmukaiseksi koettuja lopputuloksia.

Institutionaaliset pilarit näkyvät konkreettisella tasolla siinä, millaisia AI- governance- ja riskienhallintakäytäntöjä toimijat painottavat. Pankeissa regulatiivisten ja normatiivisten pilarien korostuminen näkyy toimiin, joilla pyritään osoittamaan sääntöjenmukaisuutta ja moraalista vastuullisuutta, kuten dokumentaatio, jäljitettävyys, auditointi ja malliriskien hallinta. Vakuutusyhtiöissä AI -governance keskittyy mallien tekniseen validointiin, datan laadun hallintaan, tilastolliseen perusteltavuuteen ja selitettävyysmekanismeihin, jotka tukevat kognitiivisen legitimiteetin rakentumista. Samalla vakuutusyhtiöt kehittävät eettisiä käytäntöjä vastatakseen normatiivisiin odotuksiin ja suojellakseen moraalista hyväksyttävyyttä.

Näiden tekijöiden näkökulmasta voidaan päätellä, että vaikka pankit ja vakuutusyhtiöt operoivat saman AI Act:in ohjaamana, niiden legitimiteettitarpeet ja -strategiat poikkeavat institutionaalisesti. Pankkien legitimiteetti rakentuu sääntelyn, eettisen normiston ja poliittisen kontrollin kautta, kun taas vakuutusyhtiöiden legitimiteetti perustuu tekniseen pätevyyteen, dataperusteisuuteen ja kognitiiviseen hyväksyttävyyteen. Tämä eriytyminen luo vahvan teoreettisen perustan empiiriselle analyysille siitä, miten AI Act muuntuu käytännön toimintatavoiksi ja legitimaatiostrategioiksi finanssialan eri sektoreilla.

5 FINANSSISEKTORIN TEKOÄLYKÄYTTÖTAPAUKSET JA VIRANOMAISOHJEISTUKSET

Tässä luvussa tarkastellaan tutkielman ensimmäistä empiriaosuutta. Luvun tarkoituksena on muodostaa laajempi kokonaiskuva suomalaisen finanssisektorin hyödyntämistä tekoälyjärjestelmistä sekä analysoida finanssisektorin viranomaisten ohjeistuksia ja selvityksiä AI Actin suhteesta olemassa olevaan sektorisääntelyyn.

Ensimmäinen alaluku sisältää aineiston kuvauksen. Toisessa alaluvussa käsitellään suomalaisten pankkien ja vakuutusyhtiöiden käyttämiä tekoälyjärjestelmiä sekä näiden sektoreiden välisiä yhtäläisyyksiä ja eroavaisuuksia. Kolmannessa alaluvussa tarkastellaan EIOPA:n ja EBA:n laatimia selvityksiä ja ohjeistuksia, joissa arvioidaan AI Actin ja muun sääntelyn välisiä liittymäkohtia sekä AI Actin käyttöönottoa. Neljännessä alaluvussa esitetään yhteenveto luvun keskeisistä tuloksista.

5.1 Aineiston kuvaus

Sekundääriaineistona hyödynnetään Finanssivalvonnan vuonna 2025 julkaisemaa tutkimusta *Finanssialan toimijoiden tekoälyn käyttö*, joka tarjoaa kattavaa tietoa tekoälyn käyttötapauksista suomalaisella finanssisektorilla. Tutkimus perustuu finanssialalle suunnattuun kyselyyn, johon vastasi 83 finanssisektorin toimijaa. Näistä vastaajista 22 oli vakuutusyhtiöitä ja 10 pankkeja, joiden antamiin vastauksiin tässä tutkielmassa keskitytään. Aineisto tuottaa kvantitatiivista tietoa tekoälyn käyttötapauksista, riskiluokista ja käyttöönoton laajuudesta suomalaisella finanssisektorilla.

Lisäksi sekundäärilähteenä käytetään Euroopan vakuutus- ja lisäeläkeviranomaisen (EIOPA, 2025) asiakirjaa *Opinion on AI Governance and Risk Management*, jonka tavoitteena on selventää vakuutusyhtiöille AI Actin soveltamista ja siihen liittyviä riskienhallintavaatimuksia. Lausunnossa tarkastellaan myös AI Actin ja olemassa olevan vakuutussektorin sääntelyn välisiä liittymäkohtia. Kyseessä ei ole sitova säädös, vaan

ohjeistus, joka täsmentää AI Actin soveltamista vakuutussektorin riskienhallinnan ja hallintorakenteiden näkökulmasta.

Pankkisektorin osalta aineistoon sisältyy Euroopan pankkiviranomaisen (EBA, 2025) laatima kartoitus *Outcome of EBA's AI Act mapping exercise*, jossa tarkastellaan AI Actin ja olemassa olevan pankkisääntelyn välisiä yhteyksiä ja päällekkäisyyksiä. Kartoituksessa arvioidaan erityisesti sitä, missä määrin AI Actin vaatimukset integroituvat jo olemassa olevaan pankkisektorin riskienhallinta- ja sääntelykehikkoon.

Sekundääriaineistoa hyödynnetään osana vertailevaa analyysia. Finanssivalvonnan tutkimus tarjoaa yleiskuvan tekoälyn käyttötapauksista suomalaisella finanssisektorilla, kun taas EIOPA:n ja EBA:n ohjeistukset toimivat sektorikohtaisina viitekehyksinä AI Actin ja olemassa olevan sääntelyn välisen suhteen tarkastelussa. Näiden aineistojen avulla haastatteluaineistosta tehtyjä havaintoja voidaan myöhemmin peilata EU-tason sääntelyodotuksiin.

5.2 Tekoälyn käyttötapaukset finanssisektorilla

Finanssivalvonnan (2025) kyselyn mukaan pankit ja vakuutusyhtiöt ovat finanssisektorin merkittävimpiä tekoälyn hyödyntäjiä. Kyselyyn vastanneista pankeista 100 prosenttia ja vakuutusyhtiöistä noin 90 prosenttia ilmoitti joko jo käyttävänsä tekoälyratkaisuja tai suunnittelevansa niiden käyttöönottoa seuraavan kahden vuoden aikana. Tämä tulos osoittaa, että tekoälyn käyttö finanssialalla on yleistymässä nopeasti.

Kyselyn perusteella tekoälyä hyödynnetään finanssisektorilla erityisesti sisäisissä prosesseissa, mutta myös asiakasrajapinnassa. Yleisimmät käytetyt teknologiat ovat generatiivinen tekoäly ja yleiskäyttöiset tekoälymallit. Näiden ratkaisujen avulla finanssisektorin toimijat tavoittelevat etenkin sisäisten prosessien tehostamista, asiakaskokemuksen parantamista sekä kustannusten vähentämistä (Finanssivalvonta, 2025, 4-5)

Vakuutussektorilla tekoälyn käyttötapaukset painottuvat erityisesti käännöksiin, tiedonhakuun, tekstisisällön generointiin, ohjelmakoodaukseen, chatbotteihin sekä asiakasymmärryksen kehittämiseen. Nämä käyttötapaukset voidaan pääosin luokitella AI

Actin näkökulmasta matalan riskin sovelluksiksi. Korkean riskin käyttötapauksista keskeinen esimerkki on vakuutusten riskiarviointi ja hinnoittelu, jota 35 prosenttia vakuutusyhtiöistä ilmoitti hyödyntävänsä. Lisäksi tutkimuksen mukaan tekoälyä käytetään vakuutussektorilla korvausratkaisuissa. Talousrikollisuuden torjunnassa tekoälyä ilmoitti käyttävänsä noin 11 prosenttia vakuutussektorin vastaajista (Finanssivalvonta 2025, 28).

Pankkisektorilla korostuvat pitkälti samat matalan riskin käyttötapaukset kuin vakuutussektorilla. Yleisimmät käyttökohteet liittyvät niin ikään käännöksiin, tiedonhakuun, tekstisisällön tuottamiseen, ohjelmakoodaukseen, chatbotteihin ja asiakasymmärrykseen. Korkean riskin käyttötapauksista yksi kyselyyn vastannut toimija ilmoitti käyttävänsä tekoälyä luottoluokituksessa ja luottokelpoisuuden arvioinnissa, jotka luokitellaan AI Actissa korkean riskin sovelluksiksi. Pankkisektorilla korostuu lisäksi talousrikollisuuden torjunta, jossa 14 prosenttia vastaajista ilmoitti hyödyntävänsä tekoälyä (Finanssivalvonta, 2025, 26).

Kyselyn mukaan useat vastaajat ilmoittivat myös käyttävänsä tekoälyjärjestelmiä luonnollisten henkilöiden rekrytoinnissa. Tällaiset käyttötapaukset määritellään AI Actissa korkean riskin sovelluksiksi (Finanssivalvonta, 2025, 26).

Pankki- ja vakuutussektorin tekoälyn käyttötapauksissa on paljon samankaltaisuuksia, mutta myös painotuseroja. Pankkisektorilla korostuvat esimerkiksi asiakkaan tunnistamiseen, rahanpesun estämiseen, pakoteseurantaan sekä luottokelpoisuuden arviointiin liittyvät käyttötapaukset. Vakuutussektorilla puolestaan painottuvat tekstisisällön generointi, asiakastuki, tuotekehitys, petosten havaitseminen ja ohjelmistokehitys. Kokonaisuutena tarkastellen finanssisektorilla suositaan kuitenkin selvästi matalan riskin käyttötapauksia, kun taas korkean riskin sovellukset ovat toistaiseksi vähäisemmässä roolissa. Tutkimuksen perusteella korkean riskin tekoälyjärjestelmien kehittäminen ja käyttöönotto ovat kuitenkin lisääntymässä lähitulevaisuudessa. Toimijat valmistautuvat tähän muun muassa kouluttamalla henkilöstöään ja kehittämällä tekoälyyn liittyviä omia riskinarviointimallejaan.

Kyselystä käy lisäksi ilmi, että organisaation koko vaikuttaa tekoälyn käyttöönoton valmiuksiin finanssialalla. Suurilla toimijoilla on käytettävissään enemmän henkilöstöä

ja muita resursseja tekoälyn käytön edistämiseen. Niillä on myös pienempiä toimijoita valmiimmat käytännöt riskien hallintaan ja sääntelyvaatimusten täyttämiseen.

5.3 AI Actin suhde olemassa olevaan sektorisääntelyyn

Keskeinen osa tutkimusta on tarkastella AI Actin suhdetta olemassa olevaan sektorikohtaiseen sääntelyyn, kuten vakuutusalan Solvenssi II -kehykseen sekä pankkisektorin CRD- ja CRR-sääntelyyn. EIOPA:n (2025) mukaan AI Actin periaatteet ovat pitkälti linjassa vakuutussektorin olemassa olevan sääntelykehyksen kanssa, minkä vuoksi asetuksen vaatimukset integroituvat luontevasti jo olemassa oleviin riskienhallintarakenteisiin.

EBA (2025) on laatinut laajan kartoituksen AI Actin suhteesta pankkisektorilla jo olemassa olevaan sääntelykehikkoon. Kartoituksen perusteella suurin osa AI Actin velvoitteista on nykyiseen sääntelyyn nähden joko täydentäviä tai osittain yhteneviä, mutta ei täysin identtisiä. Erityisen selviä yhtymäkohtia on havaittavissa riskienhallintaa, datan hallintaa, teknistä dokumentaatiota, kirjanpitoa, laadunhallintaa sekä järjestelmien tarkkuutta, robustisuutta ja kyberturvallisuutta koskevissa velvoitteissa. Kartoituksen mukaan näille vaatimuksille löytyy vastineita erityisesti CRR/CRD-kehikosta, DORA:sta sekä EBA:n omista ohjeistuksista.

EBA:n (2025) mukaan vahvimpia yhteensopivuuden osa-alueita ovat laadunhallinta, riskienhallinta, kyberturvallisuus ja datan hallinta. Erityisesti riskienhallintajärjestelmää koskevat velvoitteet ovat jo laajasti kytköksissä pankkisektorin olemassa olevaan sääntelyyn. Vaikka vastaavuus ei ole sääntelykehysten välillä täydellistä, kartoitus osoittaa, että vahvoja yhteyksiä löytyy useista eri säädöksistä, erityisesti CRR/CRD-kehikosta ja DORA:sta. Myös dataa ja datan hallintaa koskevilla vaatimuksilla on pankkisektorilla jo ennestään laaja sääntelyllinen perusta.

Kartoituksen perusteella selvimmät sääntelylliset aukot liittyvät kuluttajan oikeuteen saada selitys sekä perusoikeusvaikutusten arviointiin, joista erityisesti jälkimmäinen näyttäytyy pankkisektorille uutena osa-alueena. Näin ollen juuri nämä kysymykset ovat

niitä, joissa AI Act tuo pankkisektorille eniten uusia vaatimuksia verrattuna aiempaan sääntelykehikkoon (EBA,2025).

EIOPA (2025) on antanut vakuutussektoria koskevan lausunnon tekoälyn hallinnasta ja riskienhallinnasta, jonka tarkoituksena on selventää, miten AI Act suhteutuu vakuutussektorin jo olemassa olevaan sääntelykehikkoon. EIOPA:n lähestymistapa eroaa EBA:sta, sillä EIOPA keskittyy laajemmin siihen, miten vakuutusyhtiöiden tulisi arvioida ja hallita tekoälyn käyttöä osana nykyisiä hallinto- ja riskienhallintarakenteitaan. AI-ohjeistus kattaa koko vakuutustoiminnan arvoketjun ja korostaa riskiperusteisuutta, suhteellisuutta, tasa-arvoisuutta, syrjimättömyyttä, läpinäkyvyyttä, selitettävyyttä, ihmiskontrollia, datan hallintaa ja dokumentointia (EIOPA, 2025, 2-4).

EIOPA (2025) tarkastelee ohjeistuksessaan AI Actin suhdetta vakuutussektorin olemassa olevaan sääntelyyn, erityisesti Solvenssi II -direktiiviin, IDD:hen ja DORA:an. EIOPA:n keskeinen näkemys on, että tekoälyjärjestelmien käyttöä ei tule käsitellä vakuutussektorilla erillisenä sääntelykokonaisuutena, vaan osana jo olemassa olevia hallinto- ja riskienhallintarakenteita. Ohjeistus korostaa riskiperusteista ja suhteellisuusperiaatetta noudattavaa lähestymistapaa, mikä liittää AI Actin luontevasti vakuutussektorin nykyiseen sääntelylogiikkaan.

EIOPA (2025) tuo esiin, että vakuutussektorilla on jo ennestään useita AI Actin kannalta relevantteja sääntelyelementtejä. Esimerkiksi IDD:n 17 artikla velvoittaa vakuutusten tarjoajat toimimaan rehellisesti, oikeudenmukaisesti ja ammattimaisesti asiakkaidensa edun mukaisesti. EIOPA peilaa tätä periaatetta tekoälyjärjestelmien käyttöön korostamalla, että myös tekoälyä hyödyntävien ratkaisujen on tuettava asiakkaiden oikeudenmukaista kohtelua.

Myös datan hallinnan osalta EIOPA (2025) tunnistaa selvän yhteyden AI Actin ja olemassa olevan sääntelyn välillä. Solvenssi II -direktiivi sekä komission delegoitu asetus 2015/35 sisältävät jo vaatimuksia datan riittävyydestä, tarkkuudesta ja tarkoituksenmukaisuudesta, erityisesti vakuutusten myöntämiseen ja teknisten varausten laskentaan liittyvissä prosesseissa. Näin ollen AI Actin dataa koskevat vaatimukset eivät näyttäydy vakuutussektorilla täysin uusina, vaan ne rakentuvat osittain jo voimassa olevan sääntelyn varaan.

Vastaavasti dokumentointia ja kirjanpitoa koskevissa kysymyksissä EIOPA viittaa olemassa olevaan sääntelyyn, jonka mukaan vakuutusyhtiöiden tulee ylläpitää asianmukaisia ja järjestelmällisiä tietoja liiketoiminnastaan, sisäisestä organisaatiostaan ja tuotehyväksyntäprosesseistaan. Tämä luo valmiin perustan myös AI Actin dokumentointia ja jäljitettävyyttä koskevien vaatimusten toteuttamiselle (EIOPA, 2025, 9).

Sisäisen valvonnan, turvallisuuden ja jatkuvuuden osalta EIOPA yhdistää AI Actin vaatimuksia Solvenssi II -direktiiviin, komission delegoituun asetukseen 2015/35 sekä DORA:an. Näiden säädösten perusteella vakuutusyhtiöillä on jo velvollisuus ylläpitää tehokkaita sisäisen valvonnan järjestelmiä, turvata tiedon eheys, turvallisuus ja luottamuksellisuus sekä hallita tieto- ja viestintäteknologiaan liittyviä riskejä. Tältä osin AI Act täydentää olemassa olevaa sääntelykehystä pikemminkin kuin muodostaa kokonaan uuden rakenteen (EIOPA, 2025, 11-12).

6 AI ACTIN TOIMEENPANO JA KÄYTTÖ ORGANISAATIOISSA

Tämä luku sisältää tutkielman toisen empiriaosuuden, jossa tarkastellaan tekoälyn ja AI Actin aiheuttamia konkreettisia muutoksia Suomen finanssisektorin organisaatioiden sisällä. Luvun aineisto koostuu kahdesta eri organisaatiosta kerätyistä asiantuntijahaastatteluista, joiden avulla sekundääriaineistoa täydennetään käytännönläheisellä näkökulmalla.

Ensimmäisessä alaluvussa esitellään aineisto ja sen keruumenetelmät. Toisessa alaluvussa tarkastellaan organisaatioissa käytettäviä tekoälyjärjestelmiä. Kolmannessa alaluvussa analysoidaan AI Actin käyttöönottoa organisaatioissa, ja neljännessä alaluvussa käsitellään AI Actin vaikutuksia riskienhallintaan sekä tekoälyyn ja asetuksen soveltamiseen liittyviä riskejä. Viidesalaluku sisältää yhteenvedon keskeisistä tuloksista.

6.1 Aineiston esittely

Asiantuntijahaastattelut toteutettiin puolistrukturoituina teemahaastatteluina marras–joulukuussa 2025. Haastattelujen tarkemmat tiedot on esitetty lähdeluettelon kohdassa ”Henkilölähteet”. Haastateltaviksi valittiin suomalaisia vakuutus- ja pankkisektorin edustajia, joilla on vastuuta AI Actin toimeenpanosta ja siihen liittyvästä riskienhallinnasta omassa organisaatiossaan. Syksyllä 2025 kontaktoitiin kahta organisaatiota, joiden edustajat osallistuivat tutkimukseen. Tutkielmassa haastateltiin yhteensä kolmea henkilöä, joista käytetään tunnisteita A, B ja C. A edustaa suomalaista vakuutusyhtiötä, kun taas B ja C edustavat finanssilaitosta, jossa harjoitetaan sekä pankki- että vakuutustoimintaa.

Haastattelut toteutettiin etäyhteydellä Microsoft Teams -sovelluksen kautta. Noin viikkoa ennen haastatteluja osallistujille toimitettiin haastattelurunko (Liite 1) sekä lyhyt taustakuvaus tutkielman aiheesta. Haastattelut nauhoitettiin ja litteroitiin, ja litteroinnit

hyväksytettiin haastateltavilla. Analyysivaiheessa aineisto käsitellään anonyymisti, eikä henkilö- tai organisaatiotietoja esitetä tunnistettavassa muodossa.

Haastattelurunko koostui neljästä teemasta ja yhteensä kahdestatoista kysymyksestä. Haastattelut alkoivat lyhyillä esittelyillä, minkä jälkeen siirryttiin varsinaisiin teemoihin. Kysymysten lisäksi esitettiin tarkentavia jatkokysymyksiä keskustelun edetessä.

Ensimmäinen teema käsitteli tekoälyn käyttötapauksia organisaatioissa. Tavoitteena oli selvittää, millaisia tekoälyratkaisuja käytetään ja missä laajuudessa, sekä tunnistaa riskienhallinnan näkökulmasta kriittisiä käyttötapauksia. Toinen teema keskittyi AI Actin velvoitteisiin ja niiden vaikutuksiin organisaation hallintajärjestelmiin sekä siihen, miten uusi sääntely on sovitettu yhteen olemassa olevan sektorisääntelyn kanssa. Kolmas teema tarkasteli AI Actin integroitumista riskienhallintaan. Kysymykset kohdistuivat riskienhallintajärjestelmiin ja -prosesseihin sekä tekoälyn synnyttämiin uusiin riskeihin. Neljäs teema käsitteli tulevaisuuden näkymiä, mukaan lukien tekoälyn mahdollisuuksia ja riskejä sekä viranomaisohjeistusten kehitystarpeita.

6.2 Tekoälyn käyttötavat tarkastelluissa organisaatioissa

Haastattelujen perusteella organisaatioissa hyödynnetään pääasiassa tekoälyjärjestelmiä, jotka sijoittuvat riskiluokitukseltaan matalan riskin kategoriaan. Matalan riskin tekoälyjärjestelmille ei aseteta tiukkoja vaatimuksia, mutta niiden on täytettävä avoimuus- ja läpinäkyvyysvelvoitteet (Traficom, 2025). Käytössä olevat tekoälyratkaisut voidaan jakaa kahteen pääryhmään: asiakasrajapinnassa käytettäviin ratkaisuihin sekä sisäisiin prosesseihin kohdistuviin sovelluksiin.

Haastateltavien mukaan matalan riskin tekoälyratkaisuja suositaan selvästi, koska niiden käyttöönotto ja hallinta on käytännössä huomattavasti helpompaa kuin korkean riskin järjestelmien. Haastateltava B kuvaa, että tekoälyä hyödynnetään organisaatiossa laajasti eri toiminnoissa ennen kaikkea useina pienempinä ratkaisuina. Asiakasrajapinnassa tekoäly näkyy erityisesti chatbotteina ja digitaalisina apureina, joita hyödynnetään sekä verkkopalvelussa että mobiilisovelluksessa. Haastateltava B kuvaa tätä seuraavasti:

> *”Meillä on brändin alla toimiva digitaalinen apuri, joka on käytössä mobiilisovelluksessa ja verkkopalvelussa. Sen kautta asiakas voi hoitaa tiettyjä perustason asioita täysin itsenäisesti, ja se vastaa myös kysymyksiin Q&A-tyyppisesti. Tämä on yksi keskeinen palvelukanava, jota kehitämme jatkuvasti ja johon pyrimme tuomaan yhä enemmän toiminnallisuuksia tukemaan asiakkaiden asiointia.”*

Asiakasrajapinnassa hyödynnettävät tekoälyjärjestelmät ovat pääosin matalan riskin ratkaisuja, joiden keskeisenä tavoitteena on asiakaskokemuksen parantaminen. Haastateltava B nostaa organisaation näkyvimmäksi tekoälyratkaisuksi asiakaspalvelussa käytettävän chatbotin. Traficomin (2025) mukaan AI Act edellyttää, että asiakkaalle on tehtävä selväksi hänen olevan vuorovaikutuksessa tekoälyjärjestelmän, kuten chatbotin, kanssa, jotta hän voi tehdä tilanteessa tietoon perustuvan päätöksen.

Toinen keskeinen tekoälyn hyödyntämiskohde liittyy sisäisten prosessien tehostamiseen. Haastateltava A kertoo, että organisaatiossa käytetyin tekoälyratkaisu on Microsoft Copilot, joka tukee satojen työntekijöiden päivittäistä työtä esimerkiksi tekstien kääntämisessä, tiedonhaussa ja sisällön muokkaamisessa. Tekoälyn monipuolista käyttöä organisaation sisällä kuvaa myös haastateltava B:

> *”Tekoälyä hyödynnetään myös esimerkiksi vakuusarvioinneissa, tietyissä riskimallinnukseen liittyvissä ratkaisuissa Suomessa sekä osassa korvauskäsittelyn prosesseja. Näissä ei ole kyse kaikista prosesseista, vaan valituista osista. Lisäksi tekoälyä käytetään jononohjauksessa, eli esimerkiksi tikettien ja palvelupyyntöjen ohjaamisessa oikeille käsittelijöille. Tätä hyödynnetään sekä sisäisissä teknisissä prosesseissa että hallinnollisissa hakemusprosesseissa.”*

Sisäisiin prosesseihin liittyvissä käyttötapauksissa korostuivat myös petos- ja rahanpesuanalytiikkaan liittyvät sovellukset. Haastateltava B toteaa, että organisaatiossa hyödynnetään tekoälyä petostentorjunnassa, vaikka ratkaisujen tarkemmasta toiminnasta ei voitu luonnollisesti kertoa yksityiskohtaisesti. Haastateltava A puolestaan pitää petos- ja rahanpesuanalytiikkaan liittyviä ratkaisuja riskienhallinnan näkökulmasta keskeisimpinä tekoälyn käyttökohteina. Ali ym. (2022) toteavat, että perinteiset petosten havaitsemismenetelmät ovat usein manuaalisia, minkä vuoksi ne voivat olla sekä aikaa vieviä että kustannuksiltaan raskaita. Tämän vuoksi tekoälyn tarjoamat hyödyt petosten havaitsemisessa ovat merkittäviä ja monipuolisia.

Lisäksi organisaatiossa käytetään analytiikkaa ryhmätason riskien arvioinnin tunnistamisvaiheessa, jossa tekoälyä hyödynnetään loogisten kokonaisuuksien

muodostamiseen sekä ideointi- ja tunnistusvaiheen tukena. Haastateltava A kuvaa vakuutusyhtiön sisäisiä tekoälyratkaisuja seuraavasti:

> *”Esimerkiksi tällainen petos- ja rahanpesuanalytiikkaan liittyvä ratkaisu ja erilaisiin vakuutustuotteisiin hinnoittelun moottoreita sekä koneenlukuratkaisuja. On olemassa ratkaisuja, jotka liittyvät vahinkojen kirjaamiseen sekä korvaushakemusten automaattiseen käsittelyyn. Lisäksi on ratkaisuja, jotka lukevat ja tulkitsevat näihin hakemuksiin liittyviä tietoja.”*

EIOPA:n (2024) mukaan tekoälyn kehitys tarjoaa hyötyjä koko vakuutusarvoketjussa, mukaan lukien haastateltava A:n esiin nostamat käyttökohteet. AI Act luokittelee Annex III -liitteessä korkean riskin tekoälyjärjestelmäksi tekoälyn käytön luonnollisiin henkilöihin kohdistuvassa riskinarvioinnissa ja hinnoittelussa henki- ja sairausvakuutusten yhteydessä. Muut vakuutuslajit, kuten omaisuusvakuutukset, eivät suoraan kuulu tämän luokituksen piiriin. Luokittelu perustuu siihen, että tekoälyjärjestelmien tekemillä riskinarviointi- ja hinnoittelupäätöksillä voi henki- ja sairausvakuutusten yhteydessä olla merkittäviä vaikutuksia yksilöiden perusoikeuksiin, yhdenvertaiseen kohteluun sekä palveluiden saatavuuteen (Traficom, 2025).

Haastatteluissa ei käsitelty yksityiskohtaisesti korkean riskin tekoälyjärjestelmien käyttöönottoa aiheen arkaluonteisuuden vuoksi. Tästä syystä korkean riskin käyttötapauksia koskeva tarkastelu perustuu ensisijaisesti sekundääriaineistoon. Haastateltava C kuitenkin toteaa, että riskienhallinnan kannalta kriittisimpinä voidaan pitää korkean riskin järjestelmiä, joita organisaatiossa on käytössä yksittäisiä. Haastateltava B täydentää tätä näkökulmaa seuraavasti:

> *”Meille syntyy joka tapauksessa velvoite rekisteröidä tietyt korkean riskin järjestelmät, jolloin tieto niistä tulee myös julkiseksi. Näiden riskienhallinta on luonnollisesti tärkeää, mutta on hyvä huomata, että monilla alueilla käytetään automaatiota ja teknologiaa, joka ei välttämättä täytä tekoälyn määritelmää.”*

B:n kommentti havainnollistaa, että käytännössä rajanveto tekoälyjärjestelmien ja muun automaation välillä ei ole aina yksiselitteinen. Tämä korostaa erityisesti AI Actin soveltamiseen liittyviä tulkintakysymyksiä sekä sitä, kuinka merkittävä vaikutus tekoälyn oikeudellisella määritelmällä on organisaatioiden velvoitteisiin. Hackerin ja Eberin (2025) mukaan AI Officen julkaisemassa ei-sitovassa ohjeistuksessa matemaattiseen optimointiin perustuvia menetelmiä ei välttämättä tulkita oikeudellisessa mielessä

tekoälyksi, koska niiden katsotaan kuuluvan tavanomaisen tietojenkäsittelyn piiriin. Haastatteluaineiston perusteella voidaan kuitenkin tulkita, että korkean riskin järjestelmien käyttöönottoon suhtaudutaan varovaisesti erityisesti niihin liittyvien velvoitteiden ja kustannusten vuoksi. Haastateltava B tiivistää tämän näkökulman seuraavasti:

> *”Uusi sääntely ohjaa osittain siihen suuntaan, että tekoälyä ei välttämättä kannata ottaa käyttöön kaikkein korkeariskisimmillä alueilla, koska sääntelyn tuoma dokumentaatio- ja vaatimustaakka on raskas eikä aina kustannustehokas. Sen sijaan tekoälyä voidaan hyödyntää tehokkaammin matalamman riskin konteksteissa.”*

Lisäksi haastateltava C nostaa datan käsittelyn keskeiseksi riskienhallinnalliseksi kysymykseksi. Hänen mukaansa tekoälyn käyttötapauksiin liittyvissä riskiarvioinneissa kiinnitetään erityistä huomiota siihen, miten dataa käsitellään, mihin se siirtyy ja millä ehdoilla sitä hyödynnetään. Tämä korostaa datan hallinnan merkitystä yhtenä keskeisimmistä riskitekijöistä tekoälyjärjestelmien käytössä finanssisektorilla.

6.3 Tekoälyn käyttöönotto tarkastelluissa organisaatioissa

Haastatteluaineiston perusteella AI Actin käyttöönotto on organisaatioissa sujunut pääosin hallitusti, mutta samalla se on edellyttänyt uusia rakenteita tekoälyn hallintaan. Keskeinen havainto on, että asetuksen myötä tekoälyn käyttöä ei enää tarkastella yksittäisinä teknisinä ratkaisuina, vaan osana laajempaa hallinta- ja riskienhallintakehikkoa. Tämä näkyy erityisesti siinä, että tekoälyjärjestelmien tunnistamisesta, luokittelusta ja dokumentoinnista on tullut aiempaa systemaattisempi osa organisaatioiden toimintaa.

Haastateltava B kuvaa tätä muutosta seuraavasti:

> *”AI Act edellyttää ensinnäkin sitä, että tunnistamme, missä tekoälyä käytetään organisaatiossa. Tämän jälkeen tekoälyjärjestelmät tulee arvioida riskiluokituksen mukaisesti ja dokumentoida asianmukaisesti. Lisäksi kaikki tekoälyyn liittyvät riskit tulee tunnistaa. Tekoälyyn liittyy toki paljon samoja riskejä kuin muuhunkin teknologiaan, mutta sen mukana tulee myös uusia riskien variaatioita ja joissain tapauksissa täysin uusia riskityyppejä. Näiden tunnistaminen on olennaista. Käytännössä AI Act on*

> *lisännyt tarpeen sisällyttää tekoälylle oma, spesifinen vaihe osaksi organisaation riskinarviointiprosessia.”*

B:n kommentista käy ilmi, että AI Act on vaikuttanut organisaation sisäisiin menettelyihin. Keskeiseksi ei nouse ainoastaan yksittäisten järjestelmien sääntelyasema, vaan myös tarve rakentaa menettely, jolla tekoälyn käyttö voidaan ensin tunnistaa ja vasta sen jälkeen arvioida. Tämän perusteella käyttöönotto näyttäytyy hallinnollisena ja organisatorisena muutoksena, jossa tekoälylle luodaan oma paikka osaksi olemassa olevia arviointi- ja dokumentointiprosesseja.

Samansuuntaisesti haastateltava A korostaa, että AI Act on vaikuttanut erityisesti tekoälyn käytön hallintamalliin:

> *”Ajattelen, että ainakin sillä tavalla, että koko tekoälyn käytön hallintamalli on pitänyt rakentaa tietyllä tavalla alusta asti. Tällä hetkellä on esimerkiksi käynnissä projekti, jossa jatketaan tekoälyn sääntelyn mukaisen käytön hallintaa. Esimerkiksi miten tunnistetut käyttötapaukset luokitellaan sääntelyn edellyttämällä tavalla ja mitä toimia näille määritetään. Sääntely vaikuttaa tähän väistämättä.”*

A:n vastaus täydentää B:n näkemystä osoittamalla, että AI Act ei ole organisaatioissa merkinnyt vain yksittäisten velvoitteiden huomioimista, vaan laajempaa hallintamallin rakentamista. Keskeisenä haasteena on varmistaa, että sekä uudet että jo käytössä olevat tekoälyjärjestelmät täyttävät asetuksen asettamat vaatimukset muun muassa läpinäkyvyyden, oikeudenmukaisuuden, vastuuvelvollisuuden ja valvonnan näkökulmista. Erityisesti niiden finanssilaitosten, jotka ovat kehittäneet tai ottaneet käyttöön tekoälyjärjestelmiä ennen asetuksen soveltamisen alkamista, tulee arvioida järjestelmänsä uudelleen AI Actin vaatimusten näkökulmasta sekä tarvittaessa mukauttaa niitä asetuksen edellyttämälle tasolle (Consultancy 2025; Hacker & Eber, 2025, 25)

Haastatteluaineiston perusteella käyttöönotto on edellyttänyt projektimuotoista valmistelua, jossa on pyritty määrittämään, miten tekoälyjärjestelmät sijoittuvat organisaation omiin menettelyihin ja millaisia toimia eri käyttötapauksiin liittyy. Tämä viittaa siihen, että AI Act toimii organisaatioissa paitsi sääntelyvaatimuksena myös hallinnollisen jäsentämisen välineenä.

Käyttöönottoon on liittynyt myös olemassa olevien asiakirjojen ja periaatteiden läpikäynti. Consultancyn (2025) mukaan tekoälyjärjestelmiin liittyvä dokumentaatio

tulee tarkistaa ja tarvittaessa päivittää vastaamaan asetuksen vaatimuksia huomioiden finanssilaitoksen asema joko järjestelmän tarjoajana tai käyttöönottajana. Haastatteluaineiston perusteella tekoälyä ei ole voitu käsitellä erillään muusta sääntely-ympäristöstä, vaan erityisesti riskienhallintaan ja tietosuojaan liittyviä dokumentteja on tarkasteltu uudelleen AI Actin näkökulmasta. Tämä osoittaa, että asetuksen voimaantulo on vaikuttanut organisaatioissa myös siihen, miten aikaisempia ohjeita, periaatteita ja hallintakäytäntöjä tulkitaan suhteessa tekoälyjärjestelmiin.

Haastatteluista käy ilmi, ettei AI Actin vaatimuksista nouse esiin yhtä yksittäistä, selkeästi haastavinta osa-aluetta. Sen sijaan vaikeudet liittyvät useisiin toisiinsa kytkeytyviin teemoihin, joista keskeisimmiksi nousevat datan laatu, selitettävyys sekä sääntelyn käytännön tulkinta. Haastateltava A nostaa datan laadun ja selitettävyyden erityisen merkittäviksi:

> *”Datan laatu on sellainen, että konkreettisesti myöskin, koska perustahan sille, että pystytään tiettyjä asioita hallitsemaan, vaatii sen, että meidän tietojen pitäisi olla sellaisessa muodossa, että vaikka tekoälyä pystyttäisiin käyttämään. Se on yksi selkeä ja ehkä haastavin jopa. Toinen tärkeä asia on selitettävyys, eli kuinka läpinäkyviä mallien toiminta ja sovellusten tulokset ovat. On oleellista ymmärtää, mihin tulokset perustuvat. Se on ehkä se toinen iso kokonaisuus.”*

A:n kommentti osoittaa, että käyttöönoton haasteet eivät liity vain juridisten velvoitteiden täyttämiseen, vaan myös organisaation tietopohjan ja teknisen valmiuden riittävyyteen. Datan laatu näyttäytyy perustavana edellytyksenä sille, että tekoälyä voidaan ylipäätään käyttää hallitusti. Samalla selitettävyys tuo käyttöönottoon uudenlaisen vaatimuksen: tekoälyjärjestelmien tuottamien lopputulosten on oltava riittävän ymmärrettäviä, jotta niiden käyttöä voidaan perustella sekä sisäisesti että ulkoisesti. Hackerin & Eberin (2025) mukaan erityisesti korkean riskin tekoälyjärjestelmiin kohdistuu lisävaatimuksia, kuten velvollisuus informoida asiakkaita heidän tietojensa käytöstä sekä siitä, miten tekoälyjärjestelmät tuottavat suosituksia ja tekevät päätöksiä.

Myös B ja C korostavat datan laadun merkitystä, mutta hieman eri näkökulmista. B:n mukaan datan laatu on yleinen liiketoiminnan haaste eikä koske vain tekoälyä, kun taas C korostaa tekoälyn vahvistavaa vaikutusta tähän kysymykseen:

> *”Lisäisin vielä, että tekoäly tuo datan laatuun ikään kuin lisäpontta. Sen myötä on entistä tärkeämpää varmistaa, että datan laatu on kunnossa*

> *kaikessa toiminnassa, koska muuten tekoälystä ei saada täyttä hyötyä irti. Tässä mielessä tekoäly toimii eräänlaisena ajurina datan laadun kehittämiselle."*

C:n havainto syventää analyysia siinä mielessä, että tekoäly ei ainoastaan edellytä laadukasta dataa, vaan myös vahvistaa tarvetta kehittää organisaation tiedonhallintaa laajemmin. Tämän perusteella tekoäly näyttää toimivan myös laajemman organisatorisen kehittämisen ajurina: asetuksen myötä huomio ei kohdistu vain tekoälyjärjestelmiin sinänsä, vaan myös niihin taustarakenteisiin, joista tekoälyn luotettava käyttö riippuu.

Toinen keskeinen haaste liittyy tarkentavan viranomaisohjeistuksen puutteeseen. Haastatteluaineiston perusteella organisaatioissa ei pidetä ongelmallisena niinkään sitä, että AI Act asettaa uusia vaatimuksia, vaan sitä, että useiden velvoitteiden käytännön sisältö on vielä osittain avoin. Tätä kuvaa haastateltava B:

> *"Moni asia on yhä epäselvä, ja vaatimusten soveltaminen käytäntöön on hankalaa ilman komission täsmällisempiä ohjeita. Sanotaan, että merkittävän muutoksen määritelmä on vielä osittain auki, ja komissiolta odotetaan tähän täsmennystä. Kun jo peruslähtökohdat ovat epäselviä, yksittäisten vaatimusten toteuttaminen on vielä haastavampaa. Tällä hetkellä ei ole täysin selvää, mikä on esimerkiksi riittävä taso datan edustavuuden varmistamisessa tai syrjinnän ehkäisyssä."*

B:n kommentti tuo esiin käyttöönoton tulkinnallisen ulottuvuuden. Hackerin & Eberin (2025) mukaan useita asetuksessa käytettyjä käsitteitä, kuten datan hallintaan liittyviä edustavuutta ja virheettömyyttä koskevia vaatimuksia, on tarkoitus täsmentää teknisten standardien avulla. Näiden standardien tavoitteena on konkretisoida asetuksen velvoitteita sekä tarjota toimintakehys, jonka avulla vaatimukset voidaan integroida finanssialan toimijoiden luottopisteytystä ja vakuutustoimintaa koskeviin malleihin ja käytäntöihin.

Organisaatioiden näkökulmasta sääntelyn toimeenpano ei ole pelkästään normien soveltamista, vaan myös jatkuvaa arviointia siitä, mitä velvoitteet tarkoittavat konkreettisissa tilanteissa. Tästä syystä tarkentavan ohjeistuksen puute lisää epävarmuutta erityisesti niissä kysymyksissä, joissa AI Act käyttää avoimia tai tulkinnanvaraisia käsitteitä. Lisäksi organisaatioiden on arvioitava tekoälyjärjestelmien hyödyntämiä tietoaineistoja varmistaakseen niiden tarkkuuden, kattavuuden, oikeudenmukaisuuden ja puolueettomuuden sekä sen, että aineistojen käyttö täyttää tietosuojasääntelyn vaatimukset. Samalla organisaatioiden tulee tunnistaa, millaisia

muutoksia esimerkiksi tiedonhallintaan ja järjestelmälokeihin on tehtävä asetuksen jatkuvan noudattamisen varmistamiseksi (Consultancy, 2025).

Haastateltava A tuo esiin, että vaikka riskiluokittelun periaatteet ovat sinänsä ymmärrettäviä, niiden soveltaminen käytännössä ei ole yksinkertaista. Erityisesti uhkamallinnukseen liittyviä menettelyjä on jouduttu kehittämään ja tarkentamaan. Tämä viittaa siihen, että käyttöönotossa ei ole kyse vain siitä, että organisaatio omaksuu uudet käsitteet, vaan myös siitä, että olemassa olevia arviointivälineitä muokataan vastaamaan AI Actin logiikkaa.

Haastattelujen perusteella AI Actin ja muun sektorikohtaisen sääntelyn yhteensopivuutta on arvioitu organisaatioissa aktiivisesti. Aineiston perusteella AI Act näyttäytyy pääosin sovitettavissa olevana osaksi jo olemassa olevia sääntely- ja riskienhallintarakenteita. Haastateltava A kytkee tekoälyn osaksi operatiivisia riskejä, joiden hallinta kuuluu jo ennestään vakuutussektorin sääntelyn piiriin. Haastateltava B puolestaan korostaa EIOPA:n ohjeistuksen vaikutusta käytäntöihin:

> *”EIOPAn ohjeistus laajentaa mielestäni AI Actin vaatimusten soveltamista koskemaan myös muita kuin vain korkeimman riskin käyttötapauksia. Se nostaa esiin teemoja, jotka koskevat yleisemmin vakuutusalan toimintaa ja tietojärjestelmiä, ja tässä mielessä sillä on selkeä vaikutus käytäntöihin.”*

Tämä havainto osoittaa, että käyttöönottoa ei tehdä organisaatioissa tyhjiössä, vaan AI Actia tulkitaan suhteessa myös sektorikohtaisiin ohjeisiin. Samalla aineisto tuo esiin, ettei yhteensopivuus ole kaikilta osin ongelmatonta. Pankkisektorin osalta haastateltava B nostaa esiin petostentorjuntaan liittyvän sääntelyllisen harmaan alueen:

> *”Tämä tekee tilanteesta haastavan, sillä jotkin AI Actin kielletyt käyttötapaukset voivat tietyissä tilanteissa limittyä petostentorjunnan käytäntöihin. Esimerkiksi tietyt profilointiin tai laajaan datan käyttöön liittyvät kiellot voivat AI Actin näkökulmasta olla ongelmallisia, vaikka petostentorjunnan kannalta ne voisivat olla perusteltuja ja asiakkaiden etua edistäviä sekä tuottavat turvaa. Tässä syntyy harmaa alue, jossa ei ole täysin selvää, mitkä ovat sallitut reunaehdot petosten torjumiseksi.”*

Aineiston perusteella voidaan todeta, että AI Actin käyttöönotto organisaatioissa on ollut ennen kaikkea hallintarakenteita, arviointimenettelyjä ja dokumentaatiota koskeva muutosprosessi. Samalla aineisto osoittaa, että käyttöönoton käytännön haasteet liittyvät erityisesti datan laatuun, selitettävyyteen ja tulkinnallisesti avoimiin velvoitteisiin.

Haastattelujen perusteella AI Act on pääosin sovitettavissa osaksi olemassa olevia rakenteita, mutta tietyillä osa-alueilla, kuten petostentorjunnassa, organisaatiot tunnistavat edelleen sääntelyllisiä epäselvyyksiä.

6.4 AI Actin vaikutukset riskienhallintaan tarkastelluissa organisaatioissa

Tämän teeman tavoitteena oli selvittää, miten AI Act on huomioitu organisaatioiden riskienhallintajärjestelmissä, millaisia muutoksia sen vuoksi on tehty sekä onko tekoälyn käyttöönotto tuonut mukanaan uusia riskejä. Haastatteluaineiston perusteella AI Act ei ole johtanut täysin uuden riskienhallintajärjestelmän rakentamiseen, vaan se on integroitunut osaksi jo olemassa olevia rakenteita. Samalla aineisto osoittaa, että tekoälyyn liittyvät kysymykset on tunnistettu riittävän erityisiksi, jotta niiden arviointiin on joissakin organisaatioissa luotu myös uusia menettelyjä.

Haastateltava A kertoo, että tekoälyn käyttö luokitellaan organisaatiossa osaksi operatiivisia riskejä. Direktiivi 2009/138/EY 13 määrittelee operatiivisen riskin tappioriskinä, joka aiheutu riittämättömistä tai epäonnistuneista sisäisistä prosesseista, henkilöstöstä ja järjestelmistä tai ulkoisista tapahtumista aiheutuvaa tappioriskiä. Tekoälyä tarkastellaan compliance-näkökulmasta erityisesti tietosuojaan liittyvänä kysymyksenä. A:n mukaan tekoälyä ei ERM-näkökulmasta ole erotettu omaksi riskiluokakseen, vaan se ymmärretään osaksi teknologiariskejä. Tämä viittaa siihen, että AI Actin vaikutus riskienhallintaan on ollut ennen kaikkea olemassa olevia rakenteita täydentävä eikä niitä korvaava. Tekoäly ei siis näyttäydy kokonaan uutena riskikategoriana, vaan uutena riskitekijänä, joka kasvattaa olemassa olevien riskien kompleksisuutta ja kokonaisriskitasoa.

A konkretisoi tätä näkökulmaa seuraavasti:

> *”Tekoälyn käyttö kuuluu operatiivisiin riskeihin, ja lisäksi se on huomioitu compliance-näkökulmasta, erityisesti tietosuojan osalta. Jos me ajatellaan terminä ERM, se kuuluu operatiivisiin riskeihin tietyllä tavalla. Se ei ole kehikossa erillisenä, vaan sen pitäisi tunnistaa yhtiöissä yhtenä teknologiariskinä.”*

A:n vastaus osoittaa, että AI Actin vaikutus riskienhallintaan ei ole organisaatiossa merkinnyt tekoälyn irrottamista omaksi erilliseksi riskialueekseen. Sen sijaan tekoälyn tuomat vaatimukset on pyritty sijoittamaan osaksi jo olemassa olevia operatiivisten riskien, compliance-toimintojen ja tietosuojan hallintaa. Samalla aineistosta käy ilmi, että tällainen integrointi ei poista sitä, että tekoäly tuo mukanaan uusia erityiskysymyksiä, joita ei voida arvioida täysin samoin kuin muuta teknologiaa.

Tätä täydentää haastateltava C, joka kuvaa organisaationsa riskienhallintajärjestelmää laajemmin. C:n mukaan organisaatiossa on käytössä keskitetty operatiivisten riskien hallintajärjestelmä, jossa tunnistetaan jatkuvia riskejä, riskitapahtumia ja läheltä piti -tilanteita. Lisäksi käytössä on erillinen riskienarviointiprosessi, jota sovelletaan aina, kun kehitetään uutta toimintaa, järjestelmää, prosessia tai palvelua. Tekoälyratkaisut on tuotu osaksi tätä kokonaisuutta siten, että niistä laaditaan erillinen riskilausunto.

Haastatteluaineiston tulokset heijastavat finanssialan valmiiksi vahvasti säänneltyä toimintaympäristöä. CRR-asetuksen 323 artiklan mukaan finanssilaitoksilla tulee olla operatiivisten riskien tunnistamiseen, arviointiin ja hallintaan liittyvät dokumentointi- ja hallintajärjestelmät, joiden voidaan tulkita kattavan myös tekoälyyn liittyvät riskit. Vastaavasti vakuutussektorilla Solvenssi II -direktiivin (2009/138/EY) 41–49 artiklat edellyttävät vakuutusyhtiöiltä riskienhallintajärjestelmää, jonka avulla riskit voidaan jatkuvasti tunnistaa, mitata, seurata, hallita ja raportoida.

C:n kuvaus osoittaa, että AI Act on vaikuttanut riskienhallintaan kahdella tasolla. Ensinnäkin tekoälyratkaisut on sisällytetty osaksi jo olemassa olevia arviointiprosesseja. Toiseksi niiden erityisluonteen vuoksi on koettu tarpeelliseksi luoda oma ennakoiva arviointivaihe ennen varsinaista riskienhallintaprosessia. C kuvaa tätä seuraavasti:

> *”Lisäksi olemme tunnistaneet, että tekoälyyn liittyvät kysymykset ovat luonteeltaan hyvin spesifejä. Tästä syystä ennen varsinaista riskilausuntoprosessia on luotu erillinen AI-katselmointiprosessi, jossa arvioidaan millaisesta AI-käyttötapauksesta on kyse, miten se suhteutuu AI Actiin ja mitä erityisiä riskejä siihen liittyy. Vasta tämän AI-katselmoinnin jälkeen tapaus etenee varsinaiseen riskienhallintaprosessiin ja lausuntokäsittelyyn.”*

C:n näkemys havainnollistaa, että vaikka AI Act on pääosin integroitunut olemassa oleviin rakenteisiin, se on samalla tuonut mukanaan uusia organisatorisia käytäntöjä. Erillinen AI-katselmointiprosessi kertoo siitä, että tekoälyä ei nähdä vain yhtenä

teknologiaratkaisuna muiden joukossa, vaan sellaisena ilmiönä, joka vaatii etukäteistä arviointia suhteessa AI Actiin sekä siihen liittyviin erityisriskeihin. C tarkentaa lisäksi, että monissa tilanteissa tekoäly ei ole toiminnan varsinainen pääasia, vaan se toimii osana laajempaa järjestelmää, prosessia tai palvelua. Tämä havainto on riskienhallinnan näkökulmasta tärkeä, koska se osoittaa, että tekoälyyn liittyvät riskit voivat olla osittain hajautuneita ja kietoutuneita muihin toiminnallisiin kokonaisuuksiin. Haastatteluaineiston perusteella tekoälyriskien hallinta näyttäytyykin osana laajempaa kokonaisvaltaista riskienhallintaa, mikä vastaa Lousuitin (2014) näkemystä ERM:stä järjestelmänä, jonka tavoitteena on yhdistää organisaation keskeiset riskit yhden hallintakehyksen alle niiden tunnistamiseksi, ohjaamiseksi ja hallitsemiseksi.

Haastatteluaineiston perusteella tekoälyyn liittyvä riskikuva on monitasoinen. Tunnistetut riskit eivät rajoitu vain sääntelyn noudattamiseen, vaan ulottuvat myös kyberturvallisuuteen, tietosuojaan, luottamukseen, maineeseen ja liiketoiminnallisiin vaikutuksiin. Erityisesti kyberturvallisuus nousee aineistossa toistuvasti esiin. Tekoälyn nähdään paitsi tuovan uusia työkaluja organisaatioiden omaan käyttöön myös lisäävän rikollisten ja hyökkääjien käytössä olevien keinojen määrää ja tehokkuutta.

Tätä kuvaa haastateltava A seuraavasti:

> *”Uusia asioita on noussut esiin myös kyberturvallisuuden näkökulmasta. On tunnistettu, että tekoäly voi vaikuttaa siihen, että kehittyneitä työkaluja on entistä helpommin saatavilla myös hakkeripuolella. Itsessään compliance riskinä tietenkin tekoäly säädöksen noudattamisen riski on se selkeä uusi riski ja toisaalta compliance puolelle tietosuojariski yhtenä riskitekijänä.”*

A:n kommentista käy ilmi, että tekoälyyn liittyvät riskit ymmärretään sekä ulkoisina että sisäisinä. Yhtäältä tekoäly lisää hyökkäyspinnan ja väärinkäytön mahdollisuuksia, toisaalta se synnyttää uudenlaisen compliance-riskin, joka liittyy suoraan AI Actin noudattamiseen. Tietosuojariski puolestaan liittyy siihen, että tekoälyä käytetään ympäristössä, jossa käsitellään usein arkaluonteista tai muuten suojattavaa dataa. Näin ollen tekoäly ei lisää vain yhtä yksittäistä riskiä, vaan tuo uusia ulottuvuuksia useisiin ennestään tunnettuihin riskikategorioihin.

Saman suuntainen mutta laajempi huoli näkyy C:n vastauksessa:

> *”Kyberturvallisuus on tunnistettu riski, mutta erityisen huolestuttavana pidän tekoälyn ja kyberuhkien yhdistelmää. Tällaiset uhat voivat muodostaa merkittäviä riskiskenaarioita. Jos luottamus horjuu, organisaation vakavaraisuus ei yksin riitä turvaamaan toimintaa.”*

C:n kommentti laajentaa riskitarkastelua teknisistä uhista institutionaaliseen luottamukseen. Finanssialalla toiminnan perustana on asiakkaiden luottamus, minkä vuoksi tekoälyyn liittyvät riskit eivät jää vain järjestelmätason ongelmiksi. Kyberuhkien ja tekoälyn yhdistelmä voi johtaa tilanteisiin, joissa vaikutukset ulottuvat maineeseen, asiakassuhteisiin ja viime kädessä liiketoiminnan jatkuvuuteen. Tämän perusteella AI Actin vaikutus riskienhallintaan näyttäytyy myös siinä, että riskien arvioinnissa joudutaan huomioimaan aiempaa vahvemmin teknisten ja reputaatioon liittyvien vaikutusten keskinäiset yhteydet.

Tulevaisuuden näkymiä koskevissa vastauksissa korostui, että tekoälyn käytön riskit eivät rajoitu teknisiin tai juridisiin kysymyksiin. Erityisesti luottamukseen ja maineriskiin liittyvät vaikutukset nähtiin merkittävinä. Haastatteluaineistossa korostuu ajatus siitä, että vaikka ihminen voisi tehdä saman virheen kuin tekoäly, tekoälyn tekemä virhe saa todennäköisesti enemmän huomiota ja voi siksi heikentää asiakkaiden luottamusta voimakkaammin. Haastateltava C nostaa esiin myös sen, että tietyissä liiketoiminnallisissa käyttötapauksissa, kuten luottoriskien tai luottotappioiden arvioinnissa, virheellisillä tekoälypäätöksillä voi olla merkittäviä taloudellisia seuraamuksia.

Tätä täydentää haastateltava B, joka korostaa nimenomaan luottamuskysymystä:

> *”Nykyisessä toimintaympäristössä tekoälyyn kohdistuva kriittinen suhtautuminen on osin lisääntynyt. Vaikka viestimme avoimesti tekoälyn käytöstä ja sen lisäämisestä, on epävarmaa, miten asiakkaat reagoivat mahdollisiin virheisiin tulevaisuudessa. Tämä luottamuskysymys on yksi keskeisimmistä huolenaiheista.”*

B:n kommentti osoittaa, että riskienhallinnassa on otettava huomioon myös tekoälyn sosiaalinen hyväksyttävyys. Riskit eivät siten muodostu vain siitä, tekeekö järjestelmä teknisesti oikeita vai vääriä päätöksiä, vaan myös siitä, miten asiakkaat ja muu toimintaympäristö suhtautuvat tekoälyn käyttöön. Tämä tekee maineriskistä finanssialalla erityisen merkityksellisen osan tekoälyyn liittyvää kokonaisriskikuvaa, sillä

asiakkaiden ja muiden sidosryhmien luottamus on keskeinen osa organisaatioiden legitimiteettiä. EIOPA:n (2024) mukaan toimintaympäristön viimeaikaiset muutokset ovat tuoneet mukanaan uudenlaisia riskejä. Teknologinen kehitys, digitaalisten toimintamallien yleistyminen, datamäärien nopea kasvu sekä mallien ja algoritmien laajempi hyödyntäminen ovat lisänneet erityisesti operatiivisia ja malliperusteisia riskejä, jotka tulee integroida osaksi vakuutusyhtiöiden olemassa olevia riskienhallintajärjestelmiä.

Haastatteluissa tunnistettiin kuitenkin myös tekoälyn merkittäviä mahdollisuuksia. A nostaa esiin korvaustoimintaan liittyvän automatisoinnin sekä riskien arvioinnin tehostamisen erityisesti vakuutussektorilla. B puolestaan korostaa tekoälyn mahdollisuuksia tuottavuuden parantamisessa erityisesti sellaisissa tehtävissä, jotka eivät edellytä luovaa inhimillistä ajattelua. Haastatteluissa nousi esiin myös agenttinen tekoäly, jonka nähtiin avaavan uusia mahdollisuuksia prosessien automatisointiin. B kuvaa tätä näin:

> *”Tällä hetkellä käydään paljon keskustelua niin sanotusta agenttisesta tekoälystä ja siitä, missä määrin erilaisia prosessin vaiheita voidaan automatisoida. Täysimittainen käyttöönotto on vielä suhteellisen kaukana, mutta uskon vahvasti, että tätä tullaan tutkimaan ja edistämään aktiivisesti.”*

Tämän lisäksi C korostaa tekoälyn hyötyjä työn tekemisen ja tuottavuuden näkökulmasta. Erityisen myönteisiä kokemuksia on saatu esimerkiksi kehittäjien koodauksen tukemisesta, ja sisäisissä tukipalveluissa tekoäly nähdään keinona vapauttaa asiantuntijoiden aikaa vaativampiin tehtäviin. Aineiston perusteella tekoäly nähdään siis yhtä aikaa sekä riskien että tehokkuushyötyjen lähteenä. Tämä kaksijakoisuus on keskeinen myös AI Actin vaikutusten arvioinnissa: sääntelyn tehtävänä ei ole estää tekoälyn käyttöä, vaan mahdollistaa sen hallittu hyödyntäminen.

Haastattelujen perusteella AI Act on lisännyt työmäärää erityisesti riskienhallinnan ja compliance-toimintojen osalta. Dokumentaatiota, periaatteita ja ohjeistuksia on päivitetty, ja juridisen osaamisen tarve on kasvanut. Organisaatioihin on perustettu uusia ohjaus- ja koordinaatiorakenteita, mutta toistaiseksi uusia rekrytointeja ei ole tehty. AI Actiin liittyvät tehtävät on pääosin jaettu olemassa olevan henkilöstön kesken. Haastateltava B tuo esiin, että resurssointi tarpeen lopullinen laajuus täsmentyy sitä mukaa, kun ymmärrys sääntelyn vaikutuksista ja sisällöstä kasvaa. AI Actin mukaan

finanssilaitosten on koulutettava henkilöstöään tekoälyn eettisestä käytöstä ja AI Actin erityisvaatimuksista (Consultancy, 2025).

Kokonaisuutena haastatteluaineisto osoittaa, että AI Actin vaikutus riskienhallintaan on ollut kaksisuuntainen. Toisaalta tekoäly on pääosin integroitu osaksi olemassa olevia riskienhallintajärjestelmiä, erityisesti operatiivisten riskien, compliance-toimintojen ja tietosuojan hallinnan yhteyteen. Toisaalta tekoälyyn liittyvien kysymysten erityisluonne on johtanut uusiin menettelyihin, kuten erillisiin AI-katselmointeihin, ja laajentanut riskienhallinnan näkökulmaa teknisistä riskeistä kohti maineeseen, luottamukseen ja taloudellisiin vaikutuksiin liittyviä riskejä. Aineiston perusteella AI Act ei siis ole muuttanut riskienhallinnan perustaa, mutta se on lisännyt siihen uuden, tekoälyä koskevan arviointi- ja hallintakerroksen.

7 YHTEENVETO JA JOHTOPÄÄTÖKSET

Tässä luvussa vastataan tutkielman alussa määriteltyihin tutkimuskysymyksiin. Ensimmäinen alaluku sisältää tutkimuskysymyksiin vastaamisen sekä johtopäätökset. Toinen alaluku käsittelee tutkielman arviointia.

7.1 Tutkimuskysymyksiin vastaaminen ja johtopäätökset

Tämän tutkielman tavoitteena oli tarkastella, miten EU:n tekoälyasetus (AI Act) näyttäytyy vakuutusyhtiöiden ja pankkien riskienhallinnassa sekä millaisia eroja sektoreiden välillä ilmenee. Tutkielma rakentui kolmen tutkimuskysymyksen varaan.

Ensimmäisen tutkimuskysymyksen tavoitteena oli selvittää, millaisia tekoälyn käyttötapauksia finanssisektorilla hyödynnetään ja miten nämä käyttötapaukset luokitellaan AI Actin riskiperusteisessa sääntelykehyksessä. Toisen tutkimuskysymyksen tarkoituksena oli arvioida, miten AI Actin vaikutukset asettuvat suhteessa jo voimassa olevaan sektorikohtaiseen sääntelyyn. Kolmannen tutkimuskysymyksen avulla tarkasteltiin, millä tavoin AI Actin vaatimukset heijastuvat pankkien ja vakuutusyhtiöiden riskienhallintaan. Tutkimuksen antamia vastauksia näihin kysymyksiin käydään seuraavaksi läpi tutkimuskysymyskohtaisesti:

1. *Kuinka suuririskisiä tekoälysovelluksia finanssisektorin eri toimijat käyttävät?*

Tutkielman tulokset osoittavat, että suomalaisilla pankeilla ja vakuutusyhtiöillä painottuvat tällä hetkellä erityisesti matalan riskin tekoälyn käyttötapaukset. Tätä tulosta tukee sekä Finanssivalvonnan tekemä kysely sekä asiantuntijahaastatteluista saadut tulokset. Tekoälykäyttötapauksen riskiluokka vaikuttaa sen tuomiin velvoitteisiin. Matalan riskin käyttötapauksilla viitataan sovelluksiin, joissa ei lähtökohtaisesti käsitellä henkilötietoja eikä vaaranneta yksityisyyden suojaa (Traficom, 2025). Tulosten perusteella tällaiset käyttötapaukset ovat finanssisektorilla varsin samankaltaisia riippumatta siitä, onko kyseessä pankki vai vakuutusyhtiö. Alla olevassa matriisissa on

havainnollistettu yleisimpiä tekoälyn käyttötapauksia, käyttö vakuutus- ja pankkisektorilla, mihin AI Actin riskiluokkaan käyttötapaus lukeutuu sekä kuinka yleisesti käytetty tämä on. Matriisi on koottu käyttäen hyväksi Finanssivalvonnan (2025) kyselyn tuloksia sekä AI Actin (Artificial Intelligence Act, (EU) 2024/1689) mukaista riskiluokittelua.

Taulukko 1 Tekoälykäyttötapauksien käyttö, riski ja yleisyys

Tekoälyn käyttötapaus	Pankkisektori	Vakuutussektori	AI Act riskiluokka	Yleisyys
Käännös	x	x	Matala	Korkea
Tiedonhaku	x	x	Matala	Korkea
Tekstisisällön generointi	x	x	Matala	Korkea
Ohjelmakoodaus	x	x	Matala	Korkea
Chatbotit/asiakastuki	x	x	Matala	Korkea
Asiakasymmärrys	x	x	Matala	Keskitaso
Talousrikollisuuden toiminta	x	x	Tapauskohtainen	Keskitaso
Luottokelpoisuuden arviointi	x		Korkea	Matala
Luottoluokitus/Luottopisteytys	x		Korkea	Matala
Vakuutusten riskiarvionti ja hinnoittelu		x	Tapauskohtainen	Keskitaso
Korvausratkaisut		x	Tapauskohtainen	Keskitaso
Rekrytointi	x	x	Korkea	Ei tietoa

Pankki- ja vakuutussektorilla yhteisiä tekoälyn käyttötapauksia ovat käännökset, tiedonhaku, tekstisisällön generointi, ohjelmakoodaus, chatbotit ja asiakastuki, asiakasymmärryksen kehittäminen sekä talousrikollisuuden torjunta. Talousrikollisuuden torjuntaa lukuun ottamatta nämä käyttötapaukset sijoittuvat pääosin matalan riskin luokkaan, ja ne ovat myös yleisiä molemmilla sektoreilla. Talousrikollisuuden torjuntaan liittyvien käyttötapausten riskiluokka voi sen sijaan vaihdella käyttötarkoituksen mukaan, eikä niiden käyttö ole yhtä yleistä kuin edellä mainittujen matalan riskin sovellusten.

Toimialojen erilaisten luonteiden takia pankki- ja vakuutussektorin välillä esiintyy kuitenkin myös sektorikohtaisia eroja. Vakuutussektorilla tekoälyä käytetään esimerkiksi vakuutusten riskiarvioinnissa ja korvausratkaisuissa. Tällaiset käyttötapaukset voivat

tietyissä tilanteissa kuulua AI Actin korkean riskin sovelluksiin riippuen siitä, miten järjestelmää käytetään ja kohdistuuko sen käyttö luonnollisiin henkilöihin asetuksessa tarkoitetulla tavalla (Artificial Intelligence Act, (EU) 2024/1689). Mikäli vakuutusyhtiö käyttää tekoälysovellusta riskinarviointiin ja hinnoitteluun henki- ja sairasvakuutuksen yhteydessä, se on luokiteltu suoraan korkean riskin järjestelmäksi (Almada, 2025,110). Pankkisektorilla korkean riskin käyttötapaukset liittyvät puolestaan erityisesti luottokelpoisuuden arviointiin sekä luottoluokitukseen tai luottopisteytykseen. Näiden käyttötapausten käyttöaste on kuitenkin toistaiseksi melko alhainen.

Lisäksi luonnollisten henkilöiden rekrytoinnissa käytettävä tekoäly luokitellaan AI Actissa korkean riskin järjestelmäksi. Tämän käyttötapauksen yleisyydestä ei kuitenkaan ole saatavilla tarkkaa tietoa, sillä Finanssivalvonnan kysely keskittyi sellaisiin käyttötapauksiin, jotka kuuluvat heidän valvontansa piiriin, eikä rekrytointi sisältynyt tähän tarkasteluun.

Käyttötapaukset voidaan jäsentää kahteen pääryhmään: asiakasrajapinnassa hyödynnettäviin ratkaisuihin sekä työntekoa tehostaviin sovelluksiin. Asiakasrajapinnassa tekoälyä käytetään esimerkiksi chatbot-ratkaisuissa, joiden avulla asiakkaat voivat saada apua ongelmiinsa ajasta riippumatta. Tällaiset ratkaisut voivat parantaa asiakaskokemusta, sillä teknologian kehittymisen myötä asiakkaiden odotukset palvelun nopeudesta ja saatavuudesta ovat kasvaneet.

Työn tehostamiseen liittyvissä käyttötapauksissa korostuu erityisesti generatiivisen tekoälyn hyödyntäminen, kuten Microsoft Copilotin kaltaiset työkalut. Näiden merkitys on organisaatioissa näkyvä, koska niitä käytetään laajasti yritysten sisällä tuhansien työntekijöiden toimesta. Käyttökohteita ovat esimerkiksi kääntäminen, tekstien muokkaaminen ja tiedonhaku. Lisäksi tekoälyä hyödynnetään sisäisissä prosesseissa, kuten petosten tunnistamisessa ja rahanpesun analytiikassa.

Matalan riskin käyttötapauksia suositaan erityisesti siksi, että niiden käyttöönotto on verrattain vaivatonta. Niihin liittyy vähemmän oikeudellisia, eettisiä ja tietosuojaan liittyviä haasteita kuin korkeamman riskin sovelluksiin, minkä vuoksi ne muodostavat luontevan lähtökohdan tekoälyn hyödyntämiselle finanssisektorilla.

2. *Miten AI Actin velvoitteet sopivat yhteen vakuutus- ja pankkialan olemassa olevan sääntelyn kanssa?*

Tutkielman tulokset osoittavat, että AI Act on mahdollista sovittaa luontevasti yhteen jo olemassa olevan sektorikohtaisen sääntelyn kanssa molempien sektorien osalta. Tämä selittyy sillä, että monet tekoälyyn liittyvät riskit, kuten datan laatuun, tietosuojaan ja maineriskeihin liittyvät kysymykset, ovat olleet laajasti esillä jo aiemmassa sääntelyssä. Lisäksi institutionaalinen teoria auttaa selittämään, miksi AI Act ei näyttäydy irrallisena sääntelynä, vaan sulautuu olemassa oleviin rakenteisiin. Meyer ja Rowan (1977) korostavat, että organisaatiot omaksuvat muodollisia rakenteita saadakseen legitimiteettiä, vakautta ja hyväksyntää ympäristössään. Eroja ilmenee kuitenkin siinä, miten eri viranomaiset, erityisesti EIOPA ja EBA, ovat ohjeistaneet sektorin toimijoita AI Actin käyttöönotossa. Alla olevassa matriisissa on koottu yhteen AI Actin keskeiset teemat sekä niitä vastaavat olemassa olevat sääntely-yhteydet vakuutus- ja pankkisektorilla.

Taulukko 2 pankkien ja vakuutusyhtiöiden sääntelyn yhteensopivuus AI Actin kanssa

Ai Act Teema	Vakuutussektorin sääntely-yhteys	Pankkisektorin sääntely-yhteys
Riskienhallinta	Solvenssi II, EIOPA	CRR/CRD
Datan hallinta	Solvenssi II, delegoitu asetus 2015/35	CRR/CRD, DORA
Dokumentaatio	Solvenssi II, delegoitu asetus 2015/35	CRR/CRD,
Läpinäkyvyys selitettävyys	IDD, EIOPA	EBA, GDPR
Ihmisen valvonta	Solvenssi II, EIOPA	CRD, EBA
Syrjimättömyys ja oikeudenmukaisuus	IDD, EIOPA	Kuluttajansuoja ja luotonantoa koskeva sääntely
Tarkkuus, robostisuus ja kyberturvallisuus	Solvenssi II, DORA	EBA, DORA
Governance ja vastuunjako	Solvenssi II, IDD, EIOPA	CRR/CRD, EBA

Taulukko osoittaa, että finanssisektorilla on jo ennestään sääntelyä lähes kaikista AI Actissa esiin nousevista teemoista. Nämä sääntelykehykset eivät kuitenkaan ole täysin yhteneviä, vaan AI Act toimii niitä täydentävänä sääntelykerroksena sekä pankki- että vakuutussektorilla.

Finanssisektorin viranomaiset lähestyvät AI Actia hieman eri näkökulmista ohjeistuksissaan. EIOPA on antanut AI Actin toimeenpanosta laaja-alaisempaa ohjeistusta kuin EBA sekä lähestyy asiaa laajemman hallinnan ja eettisen käytön näkökulmasta. EIOPA korostaa riskiperusteista ja suhteutettua lähestymistapaa, mikä on vakuutussektorin sääntelylle ja toiminnalle ominaista. Ohjeistuksessaan EIOPA kehottaa vakuutusyhtiöitä arvioimaan muun muassa datan laatua ja sensitiivisyyttä, vaikutuksia asiakkaisiin, järjestelmän autonomia-astetta, käyttötapauksen sijoittumista asiakasrajapintaan tai sisäiseen käyttöön sekä sitä, voiko tekoälyjärjestelmällä olla vaikutuksia syrjimättömyyteen ja asiakkaiden oikeuksiin. Tämä ohjeistus kattaa koko vakuutustoiminnan arvoketjun. Keskeistä EIOPA:n lähestymistavassa on näkemys siitä, ettei AI Act muodosta vakuutussektorille täysin erillistä hallintakehikkoa, vaan tekoälyn hallinta tulisi integroida osaksi olemassa olevia hallinto- ja riskienhallintarakenteita.

EBA:n lähestymistapa poikkeaa tästä painotukseltaan, sillä se lähestyy asiaa suppeammin ja sääntelykartoituksen kautta. Sen ohjeistus kohdistuu erityisesti luottokelpoisuuden arviointiin ja luottopisteytykseen liittyviin korkean riskin tekoälyjärjestelmiin. Samalla EBA:n näkemys AI Actin suhteesta muuhun sääntelyyn on kuitenkin pitkälti samansuuntainen kuin EIOPA:lla. EBA tuo esiin, että DORA kattaa laajasti kyberturvallisuuteen ja toiminnan jatkuvuuteen liittyviä vaatimuksia, kun taas CRR/CRD-kehikko tarjoaa teknologianeutraalin hallinto- ja riskienhallintakehyksen myös tekoälyratkaisujen valvontaan. Kartoituksesta käy kuitenkin ilmi, että kaikki AI Actin velvoitteet eivät sisälly nykyiseen sääntelyyn täysmääräisesti, kuten perusoikeusvaikutusten ja selitettävyyteen liittyvissä kysymyksissä.

Tulosten perusteella voidaan siten todeta, että vakuutussektorilla viranomaisohjauksessa korostuvat hallintamallit ja arviointiperiaatteet, kun taas pankkisektorilla painopiste on enemmän sääntelyn päällekkäisyyksien hallinnassa ja AI Actin integroimisessa osaksi jo olemassa olevaa sääntelykehikkoa. Pakottava isomorfismi näkyy siinä, että AI Act ja viranomaisohjeistus pakottavat organisaatiot muuttamaan hallintamallejaan (DiMaggio & Powell, 1983). Mimeettinen isomorfismi voi näkyä siinä, että epävarmuuden vuoksi

organisaatiot seuraavat toistensa AI-governance-ratkaisuja. Normatiivinen isomorfismi taas näkyy esimerkiksi siinä, että tekoälyn hallintaan liittyvät asiantuntijaroolit, osaamisvaatimukset ja "hyvät käytännöt" yhdenmukaistuvat alalla (DiMaggio & Powell, 1983; Hambrick ym., 2004).

3. *Miten AI Actin vaatimukset vaikuttavat riskienhallintaan vakuutus- ja pankkisektorilla?*

Empiirinen haastatteluaineisto ei osoittanut selkeitä eroja sektorien välillä. Tätä selittää osin aineiston rajoite: osa haastateltavista edusti finanssilaitosta, jossa harjoitetaan sekä pankki- että vakuutustoimintaa, jolloin sektorikohtaiset erot eivät välttämättä näy organisaation sisäisissä käytännöissä. Viranomaisohjeistusten ja institutionaalisen teorian perusteella voidaan kuitenkin argumentoida, että erot konkretisoituvat käytännössä erityisesti silloin, kun korkean riskin järjestelmien käyttö yleistyy ja sektorikohtaiset riskiprofiilit korostuvat.

Empiirisestä aineistosta käy ilmi, että AI Actin käyttöönotto on edellyttänyt uusia rakenteita tekoälyn hallintaan. Tämä on lisännyt työmäärää erityisesti riskienhallinnan ja compliance -toimintojen osalta. AI Actin käyttöönotto on johtanut dokumentaation lisääntymiseen, ja lisäksi olemassa olevaa tietoarkistoa on jouduttu käymään läpi, jotta asetuksen mukaiset vaatimukset voidaan täyttää. Vastuunjakoa on päivitetty, ja organisaatioiden sisälle on syntynyt uusia rooleja. Institutionaalisesta näkökulmasta organisaatiot mukauttavat riskienhallintaansa paitsi muodollisen sääntelyn vuoksi, mutta myös siksi, että niiden on ylläpidettävä legitimiteettiään suhteessa valvojiin, asiakkaisiin ja muihin sidosryhmiin (Schumann, 1995)

Haastattelujen perusteella tekoäly luokitellaan yhtiöissä ensisijaisesti operatiiviseksi riskiksi. ERM-näkökulmasta sitä ei eroteta omaksi riskiluokakseen, vaan se tunnistetaan osana teknologiariskejä. Kokonaisvaltaisen riskienhallinnan näkökulmasta tekoäly näyttäytyy läpileikkaavasti koko riskienhallinnan prosessissa, sillä se vaikuttaa sekä riskien tunnistamiseen, arviointiin että käsittelyyn (Louisot, 2014).

Samalla tekoäly muodostaa uuden riskitekijän, joka voi kasvattaa organisaation kokonaisriskitasoa. Tämä korostuu erityisesti ISO 31000 -prosessin vaiheissa, kuten riskien tunnistamisessa, analysoinnissa, arvioinnissa ja käsittelyssä (International Organization for Standardization, 2018). Haastattelujen perusteella tekoälyn yhteydessä

korostuvat etenkin malliriskit, vinoumariskit, kyberturvallisuusriskit, tietosuojariskit sekä maineriskit. Lisäksi riskien arvioinnista on tullut tekoälyn myötä aiempaa systemaattisempaa.

Toisaalta tekoäly ei näyttäydy ainoastaan riskin lähteenä, vaan myös riskienhallinnan välineenä. Sitä voidaan hyödyntää esimerkiksi petosten ja poikkeamien tunnistamisessa, jolloin tekoäly sijoittuu ISO 31000 -viitekehyksessä myös riskien käsittelyn, seurannan ja raportoinnin tueksi.

Tekoälyyn liittyvä ihmisen valvonta korostuu erityisesti silloin, kun järjestelmillä on vaikutusta taloudellisesti merkittäviin päätöksiin tai asiakkaiden asemaan. AI Act ei ole johtanut täysin uuden riskienhallintajärjestelmän rakentamiseen, vaan se on integroitunut olemassa oleviin rakenteisiin. Uutena elementtinä se on kuitenkin tuonut uusia prosessivaiheita, kuten AI-katselmoinnin. AI-katselmointivaihe voi yleistyä finanssialalla institutionaalisen teorian mukaisesti, jolloin ympärillä olevat organisaatiot kopioivat hyväksi havaittuja toimintoja.

Haastatteluaineiston perusteella organisaation riskienhallintatoiminnoissa tunnistetaan ensin tekoälyn käyttötapaus, jonka jälkeen se käsitellään erillisessä AI-katselmointiprosessissa. Prosessissa arvioidaan käyttötapaukseen liittyviä riskejä, sen suhdetta AI Actiin sekä käyttötapauksen riskiluokitusta, ja arvioinnin tulokset dokumentoidaan. Tämän esivaiheen jälkeen tekoälyn käyttötapaus etenee operatiivisten riskien hallintaprosessiin samalla tavoin kuin muutkin operatiiviset riskit. Menettelyn taustalla on ajatus siitä, että tekoäly ei useimmiten muodosta liiketoiminnallisesti hankkeen keskeisintä sisältöä, vaan toimii osana laajempaa kokonaisuutta, kuten uuden järjestelmän käyttöönottoa

Sektorikohtaisia eroja löytyy riskityyppien painottamisesta. Vakuutusyhtiöissä korostuvat hinnoitteluun ja riskinarviointiin liittyvät kysymykset, asiakkaiden oikeudet ja syrjimättömyys. Tätä voidaan tulkita niin, että vakuutusyhtiöt rakentavat AI-governancea paitsi sääntelyn vuoksi myös säilyttääkseen kognitiivisen ja moraalisen legitimiteettinsä: tekoälymallien on näyttäydyttävä teknisesti pätevinä, ymmärrettävinä ja oikeudenmukaisina (Suchman, 1995; Henderson ym., 2024). Pankeilla taas korostuu luottokelpoisuuden arviointi, luottopisteytys ja sääntelyn päällekkäisyydet. Tätä voi selittää sillä, että pankkien legitimiteetti rakentuu ennen kaikkea regulatiivisen ja

moraalisen legitimiteetin varaan. Niiden on kyettävä osoittamaan, että tekoälyjärjestelmät ovat hallittuja, valvottuja ja yhteiskunnallisesti hyväksyttäviä (Suchman, 1995; ECB, 2023). AI Act vahvistaa tätä painetta entisestään.

Vakuutussektorilla AI Actin toimeenpano näyttäytyy erityisesti selkeämpien tekoälyn hallintamallien rakentamisena, kun taas pankkisektorilla painopiste on AI Actin vaatimusten liittämisessä osaksi jo olemassa olevia prosesseja ja sääntelykehyksiä.

7.2 Tutkielman arviointi

Tuomi & Sarajärvi (2018) mukaan kaikessa tutkimustoiminnassa pyritään välttämään virheitä ja tutkimuksen luotettavuutta on arvioitava. Tutkimuksen luotettavuutta arvioidaan kokonaisuutena, jolloin sisäinen johdonmukaisuus painottuu. Oleellista on arvioida tutkimuksen kohdetta ja tarkoitusta, aineiston keruumenetelmiä, tutkimuksen tiedonantajia, aineiston analyysi ja tutkimuksen luotettavuutta.

Tutkielman tavoitteena oli selvittää AI Actin vaikutuksia pankki- ja vakuutussektorilla. Aiheen käsittely aloitettiin taustoittamalla vakuutusyhtiöiden ja pankkien riskienhallintaa, sääntelyä sekä toimialalla tyypillisiä riskejä. Toinen teorialuku käsitteli AI Actin vaatimuksia erilaisten riskiluokkien osalta sekä käsiteltiin olennaisia säädöksen kohtia, mitkä koskettavat vakuutus- ja pankkisektoria. Kolmas teorialuku kävi läpi institutionaalista teoriaa ja miten tämän vaikutukset näkyvät eri sektoreilla.

Tämän tavoitteen kannalta olennaisia kirjallisuuslähteitä, sääntelyaineistoa ja verkkolähteitä oli saatavilla monipuolisesti. AI Actin tuoreuden takia, sen vaikutuksia finanssisektoriin käsittelevää tutkimusta oli kuitenkin vielä melko vähän saatavilla, mikä rajoitti aiemman tutkimuksen hyödyntämistä ja vaikutti osaltaan tutkielman teoreettisen pohjan rakentumiseen.

Tutkielman empiriaosuus jakautui kahteen osaan, mikä vahvisti aiheen tarkastelua useasta näkökulmasta. Sekundääriaineiston avulla muodostettiin kattava yleiskuva tekoälyn nykyisistä käyttötapauksista suomalaisella finanssisektorilla. Lisäksi saatavilla olleet EIOPA:n ja EBA:n ohjeistukset tukivat ymmärrystä siitä, millaisia eroavaisuuksia pankki- ja vakuutussektorin välillä voi ilmetä AI Actin soveltamisessa nykyisen

lainsäädännön puitteissa. Viranomaisohjeistuksia oli kuitenkin tutkielman tekohetkellä saatavilla vain rajallisesti, mikä heikensi mahdollisuuksia tehdä pitkälle meneviä tulkintoja.

Asiantuntijahaastattelut täydensivät sekundääriaineistoa ja toivat tutkielmaan käytännönläheistä näkökulmaa AI Actin toimeenpanoon organisaatioissa. Haastateltavat toimivat omissa organisaatioissaan AI Actin käyttöönotossa, jolloin heidän valintansa tutkielmaan oli perusteltu. Haastattelujen perusteella saatiin kattava kuva erityisesti matalan riskin tekoälyn käyttötapauksista sekä siitä, miten AI Act on vaikuttanut organisaatioiden riskienhallintaan ja sen suhteeseen olemassa olevaan sääntelyyn. Korkean riskin tekoälyjärjestelmät jäivät kuitenkin haastatteluissa vähäiselle käsittelylle niiden arkaluonteisuuden vuoksi, mikä rajasi osaltaan tutkielman empiirisiä havaintoja.

Laadullisen tutkimuksen luotettavuutta käsitellään yleensä validiteetin ja reliabiliteetin käsittein. Validiteetilla arvioidaan sitä, onko tutkimuksessa tutkittu sitä, mitä on luvattu ja reliabiliteetilla arvioidaan tutkimustulosten toistettavuutta, sekä mahdollisia ristiriitoja. Validiteetti voidaan jakaa sisäiseen ja ulkoiseen validiteetin. Sisäinen validiteetti käsittää tutkimuksen teoreettisten ja käsitteellisten määrittelyjen sopusoinnun, mikä osoittaa tutkijan tieteenalansa hallintaa sekä tieteellisen otteen. Ulkoisella validiteetilla viitataan tehtyjen tulkintojen ja johtopäätösten sekä aineiston välisen suhteen pätevyyttä (Tuomi& Sarajärvi, 2018, 117–118; Eskola, 1998, 154.)

Validiteetin näkökulmasta tämä tutkielma on vastannut ennalta asetettuihin tutkimuskysymyksiin, mitä ovat tukeneet asianmukainen teoriaosuus sekä kaksiosainen empiria. Tutkielman sisäinen validiteetti ilmenee johdannossa, jossa perustellaan tutkimusmenetelmät ja tutkimusfilosofiset lähtökohdat. Lähteinä on hyödynnetty tieteellisiä, oikeudellisia ja ammatillisia lähteitä, jotka ovat tutkielman kannalta olennaisia ja monipuolisia. Lisäksi lähteiden valinnassa ja arvioinnissa on sovellettu kriittistä harkintaa.

Tutkielman ulkoinen validiteetti perustuu huolellisesti toteutettuun aineistonkeruuseen. Haastattelut on suunniteltu perusteellisesti, ja haastateltavat on valittu heidän asiantuntijuutensa sekä tutkimusaiheen kannalta tarkoituksenmukaisen soveltuvuuden perusteella. Myös sekundääriaineisto kytkeytyy vahvasti tutkielman johtopäätöksiin, mikä vahvistaa tutkimuksen kokonaisvaliditeettia aineiston laadun näkökulmasta.

Tutkielman reliabiliteettia tarkasteltaessa olennaista on arvioida, toistuisivatko samat tutkimustulokset uudelleen. Olennainen osa tätä on aineiston riittävyys ja analyysin kattavuus, jolloin tulkinnat eivät perustu satunnaisiin poimintoihin aineistosta (Eskola, 1998, 156). Tutkielman tulokset perustuvat sekä sekundääri- että primääriaineistoon. Sekundääriaineiston osalta reliabiliteetti on vahva, sillä aineisto perustuu viranomaisohjeistuksiin ja sääntelyyn, jolloin tulkinnanvaraa on suhteellisen vähän.

Primääriaineiston osalta eroavaisuuksia voi kuitenkin syntyä, koska aineisto perustui kahden organisaation kokemuksiin AI Actin käyttöönotosta. Toisaalta haastatellut organisaatiot ovat Suomen finanssisektorin suuria toimijoita, joiden toimintamallit voidaan arvioida vakiintuneiksi. Tämän lisäksi kahdesta eri organisaatiosta saadut haastattelutulokset muistuttavat huomattavasti toisiaan, mikä kertoo vahvasta reabiliteetista. Mikäli haastatteluihin olisi osallistunut pienempiä organisaatioita, niiden toimintamallit olisivat voineet olla vielä kehittymässä ja näin tuoda eroja AI Actin käyttöönotossa. On kuitenkin mahdollista, että niiden toimintatavat muistuttaisivat tulevaisuudessa suurempien organisaatioiden vastaavia käytäntöjä.

Tutkielman tekemiseen liittyi rajoitteita. AI Act on vielä varsin uusi säädös, eikä sitä ole toistaiseksi otettu kokonaisuudessaan käyttöön. Samanaikaisesti myös tekoälyn hyödyntäminen on edelleen kehitysvaiheessa, minkä vuoksi sen koko potentiaali ei vielä näy organisaatioiden käytännöissä. Tämä asetti tutkielmalle haasteita erityisesti korkean riskin käyttötapausten arvioinnissa, sillä niihin liittyvää empiiristä aineistoa ei ollut arkaluonteisuuden vuoksi saatavilla.

Kokonaisuutena tutkielman vahvuutena voidaan pitää aiheen ajankohtaisuutta ja yhteiskunnallista merkitystä sekä teoreettisen ja empiirisen aineiston yhdistämistä. Toisaalta tutkielman rajoitteena oli AI Actia koskevan tutkimuksen ja viranomaisohjeistuksen vähäinen määrä sekä se, että korkean riskin tekoälyjärjestelmistä ei ollut mahdollista saada kattavaa empiiristä aineistoa. Näistä rajoitteista huolimatta tutkielma tuotti perustellun ja ajankohtaisen kokonaiskuvan AI Actin vaikutuksista pankki- ja vakuutussektorilla.

Tutkimusaiheeseen liittyy useita mahdollisia jatkotutkimusmahdollisuuksia. Koska AI Act tulee täysimääräisesti sovellettavaksi vuonna 2027, sen vaikutukset tulevat todennäköisesti näkymään nykyistä selvemmin vasta lähivuosina. Samalla myös korkean

riskin tekoälyjärjestelmien käyttö finanssisektorilla todennäköisesti yleistyy, mikä lisää tarvetta niiden avoimelle tarkastelulle.

Yksi luonteva jatkotutkimuksen aihe olisi keskittyä tarkemmin johonkin yksittäiseen korkean riskin tekoälyjärjestelmään, esimerkiksi pankkisektorilla tekoälyn käyttö luottopisteytyksessä, sekä tarkastella sen vaikutuksia, riskienhallintaa ja mahdollisia seurannaisriskejä. Lisäksi jatkotutkimuksessa olisi mahdollista analysoida, miten organisaatiot viestivät korkean riskin järjestelmien käytöstä ja miten asiakkaat reagoivat tähän esimerkiksi luottamuksen, läpinäkyvyyden ja tietosuojan näkökulmista.

8 LÄHTEET

Tieteelliset lähteet

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Applied Sciences, 12(19), Article 9637.

Almada, M. (2025). *The EU AI Act: Logic, content, and implications for finance*. *SSRN Electronic Journal*.

Choudhry, M. (2018). Banks and credit risk. In *The Moorad Choudhry anthology* John Wiley & Sons Singapore Pte. Ltd.

Choudhry, M. (2022). *The principles of banking* (2nd ed.). John Wiley & Sons, Inc.

Dacin, M. T., Goodstein, J., Scott, W. R., Greenwood, R., Suddaby, R., Hinings, C. R., Thornton, P., Sherer, P. D., Lee, K., Kraatz, M. S., Moore, J. H., Pennings, J. M., Townley, B., Casile, M., Davis-Blake, A., Garud, R., Jain, S., Kumaraswamy, A., Kostova, T., … Phillips, N. (2002). Institutional theory and institutional change. Academy of Management Journal, 45(1),

Darwish, J. A. (2025). Optimization and prediction of corporate credit rating through advanced feature selection based on AI and deep learning. Alexandria Engineering Journal, 127

Durán Santomil, P., & Otero González, L. (2020). Enterprise risk management and Solvency II: The system of governance and the own risk and solvency assessment. *Journal of Risk Finance, 21*(4), 317–
332.

Eskola, J., Suoranta, J., & Ellibs. (1998). Johdatus laadulliseen tutkimukseen. Vastapaino.

Golpayegani, D., Pandit, H. J., & Lewis, D. (2022). Airo: An ontology for representing ai risks based on the proposed eu ai act and iso risk management standards. In *Towards a knowledge-aware AI* IOS Press.

Hacker, P., & Eber, M. (2025). The Future of Credit Underwriting and Insurance Under the EU AI Act: Implications for Europe and Beyond. Harvard Data Science Review, 7(3).

Hambrick, D. C., Finkelstein, S., Cho, T. S., & Jackson, E. M. (2004). Isomorphism in reverse: Institutional theory as an explanation for recent increases in intraindustry heterogeneity and managerial discretion. In B. Staw & R. Kramer (Eds.), *Research in organizational behavior* Elsevier.

Hirsjärvi, S., & Hurme, H. (2022). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö* (2. painos). Gaudeamus.

Hitchcox, A. N., Klumpes, P. J. M., McGaughey, K. W., Smith, A. D., & Taverner, N. H. (2011). ERM for insurance companies: Adding the investor's point of view. *British Actuarial Journal, 16*(2)

Kivisaari, E., & Kahola, M.-L. (2017). *Vakuutustalous: Vakuutusyrityksen riskienhallinta, tilinpäätös ja vakavaraisuus*. FINVA.

Kocziszky, G., Veres Somosi, M., & Kobielieva, T. O. (2017). Compliance risk in the enterprise.

Losiewicz-Dniestrzanska, E. (2015). Monitoring of compliance risk in the bank. *Procedia Economics and Finance, 26*, 800–805.

Louisot, J.-P., & Ketcham, C. (Eds.). (2014). *ERM, enterprise risk management: Issues and cases* (1st ed.). John Wiley & Sons.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2)

Nallakaruppan, M. K., Balusamy, B., Shri, M. L., Malathi, V., & Bhattacharyya, S. (2024). An Explainable AI framework for credit evaluation and analysis. Applied Soft Computing, 153, Article 111307.

Passador, M. L. (2024). AI in the vault: AI Act's impact on financial regulation. *Loyola University Chicago Law Journal, 56*, 257.

Ramakrishna, S. P. (2015). *Enterprise compliance risk management: An essential toolkit for banks and financial services*(1st ed.). Wiley.

Samiuddin, M., Rajender, G., Varma, K. S. A., Kumar, A. R., & Shaik, S. (2023). Health Insurance Cost Prediction Using Deep Neural Network. Asian Journal of Research in Computer Science, 16(2

Siri, M. (2017). Corporate governance of insurance firms after Solvency II.

P. Marano & M. Siri (2017), *Insurance regulation in the European Union*.Springer International Publishing.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review, 20*(3)

Sweeting, P. (2011). *Financial enterprise risk management* (1st ed.). Cambridge University Press

Tuomi, J., & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi

Oikeudelliset lähteet

Euroopan parlamentin ja neuvoston direktiivi 2009/138/EY vakuutus- ja jälleenvakuutustoiminnan harjoittamisesta (Solvenssi II).

Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689 tekoälystä (Artificial Intelligence Act).

Euroopan parlamentin ja neuvoston asetus (EU) N:o 575/2013 luottolaitosten vakavaraisuusvaatimuksista (CRR).

Euroopan parlamentin ja neuvoston direktiivi 2013/36/EU luottolaitostoiminnan aloittamisesta ja harjoittamisesta sekä vakavaraisuusvalvonnasta (CRD IV).

Verkkolähteet:

Consultancy.eu. (2025)*The EU AI Act: The impact on financial services institutions*. Viitattu 18.11.2025.Saatavilla: https://www.consultancy.eu/news/11237/the-eu-ai-act-the-impact- on-financial-services-institutions

Council of the European Union. (2024, 1 September). *Basel III: international r Regulatory framework for banks*.Viitattu 2.10.2025. Saatavilla: https://www.consilium.europa.eu/en/policies/basel-iii/

Basel Committee on Banking Supervision. (n.d.). *History of the Basel Committee*. Bank for International Settlements. https://www.bis.org/bcbs/history.htm, viitattu 8.11.2025

Deloitte. (2023). *Tekoälysäädös pähkinänkuoressa – vaikutukset finanssialalle*. Viitattu 13.4.2026. Saatavilla: https://www.deloitte.com/fi/fi/Industries/financial-services/perspectives/artificial-intelligence-act-tekoalysaados-finanssiala.html

De Nederlandsche Bank. (2023). *Solvency II: Pillar 3*. Viitattu 2.10.2025. Saatavilla: https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-sectors/insurers/statutory-reporting-insurers/solvency-ii-pillar-3/

European Banking Authority (2025). AI Act: implications for the EU banking and payments sector. Viitattu 25.1.2026. Saatavilla: https://www.eba.europa.eu/sites/default/files/2025-11/d8b999ce-a1d9-4964-9606-971bbc2aaf89/AI%20Act%20implications%20for%20the%20EU%20banking%20sector.pdf

European Banking Authority. *The Basel framework: the global regulatory standards for banks*.Viitattu 8.11.2025. Saatavilla: https://www.eba.europa.eu/activities/basel-framework-global-regulatory-standards-banks

European Central Bank, Witte, N. (2024). Capital requirements in Pillar 1 or Pillar 2: Does it matter for market discipline? Viitattu 8.11.2025. Saatavilla: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2988~25e3305cfa.en.pdf

European comission (2024) Targeted consultation on artificial intelligence in the financial sector Viitattu 4.1.2026. Saatavilla: https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-artificial-intelligence-financial-sector_en

European Commission. (2025) *AI Act — Regulatory framework on artificial intelligence*. Shaping Europe's digital future. Viitattu 2.10.2025. Saatavilla: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Commission. (2026). *AI Act*. Shaping Europe's digital future. Viitattu 13.4.2026. Saatavilla: strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European comission. Directorate-General for Financial Stability, Financial Services and Capital Markets (2024) *Basel III*. Viitattu 2.10.2025. Saatavilla: https://finance.ec.europa.eu/news/basel-iii-2024-07-25_en

European Insurance and Occupational Pensions Authority. (2024). *Report on the digitalisation of the European insurance sector*. Viitattu 4.1.2026 Saatavilla: https://www.eiopa.europa.eu/publications/eiopas-report-digitalisation-european-insurance-sector_en

European Insurance and Occupational Pensions Authority. (2025) *Solvency II — R Regulation and policy*. Viitattu 30.10.2025. Saatavilla: https://www.eiopa.europa.eu/browse/regulation-and-policy/solvency-ii_en

European Insurance and Occupational Pensions Authority. (2025) Opinion on Artificial Intelligence governance and risk management. Viitattu 15.2.2026. Saatavilla: https://www.eiopa.europa.eu/publications/opinion-artificial-intelligence-governance-and-risk-management_en

European Insurance and Occupational Pensions Authority; European BankingAuthority; European Securities and Markets Authority. (2025). *Joint Committee update on risks and vulnerabilities in the EU financial system – Spring 2025*.Viitattu 2.10.2025.

Saatavilla: https://www.eiopa.europa.eu/publications/joint-committee-update-risks-and-vulnerabilities-eu-financial-system-spring-2025_e

Finanssivalvonta. (2021) *Vakavaraisuus- ja maksuvalmiussääntely (CRR/CRD) – Sääntelykokonaisuudet*. Viitattu 14.11.2025. Saatavilla: https://www.finanssivalvonta.fi/saantely/saantelykokonaisuudet/crrcrd/

Finanssivalvonta. (2023). *Hyvä hallinto varmistaa valvottavan toimintaa, vakavaraisuutta ja sitä, että asiakkaan rahat ja vakuutetut edut ovat turvassa*. Viitattu 31.10.2025. Saatavilla: https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/toimintakertomukset/toimintakertomus-2022/teemat/hyva-hallinto-varmistaa-valvottavan-toimintaa-vakavaraisuutta-ja-sita-etta-asiakkaan-rahat-ja-vakuutetut-edut-ovat-turvassa

Finanssivalvonta (2025) Finanssialan toimijoiden tekoälyn käyttö. Viitattu 13.11.2025 Saatavilla: https://www.finanssivalvonta.fi/globalassets/fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2025/finanssialan-toimijoiden-tekoalyn-kaytto_fi_.pdf

Finanssivalvonta. (2025). *Solvenssi II – sääntelykokonaisuudet*.Viitattu 2.10.2025.Saatavilla: https://www.finanssivalvonta.fi/saantely/saantelykokonaisuudet/solvenssi-ii/

Gjerdrum, D. (2016, February 9). *A brief history of ISO 31000 – and why it matters*. Risk & Insurance. Viitattu 30.10.2025. Saatavilla https://riskandinsurance.com/a-brief-history-of-iso-31000-and-why-it-matters/

Goodwin, 2024. Henderson, A., Scott, G., Moille, C., & Dixon-Ward, M. *EU AI Act: Key Points for Financial Services Businesses*. Viitattu 3.10.2025. Saatavilla: https://www.goodwinlaw.com/en/insights/publications/2024/08/alerts-practices-pif-key-

Insurance Europe. (2024). *Response to EC targeted consultation on AI in the financial sector*.Viitattu3.10.2025.Saatavilla: https://www.insuranceeurope.eu/mediaitem/ea84f6c3-c1be-478a-9892-e666bfb2905f/Insurance+Europe+response+to+EC+targeted+consultation+on+AI+in+the+financial+sector.pdf

International Organization for Standardization. (2018). *ISO 31000:2018 Risk Management — Guidelines* (Standard No. ISO 65694). https://www.iso.org/standard/65694.html

Investopedia. Hargrave, M. (2025). *Understanding the role and duties of the compliance department*. Viitattu 2.10.2025.Saatavilla: https://www.investopedia.com/terms/c/compliancedepartment.asp

Investopedia. Hayes, A. (2025). *Enterprise risk management (ERM): What it is and how it works*. Investopedia. Viitattu 2.10.2025. Saatavilla: https://www.investopedia.com/terms/e/enterprise-risk-management.asp

Investopedia (2025) *Artificial Intelligence (AI): What It Is, How It Works, Types, and Uses*. Viitattu2.10.2025.Saatavilla: https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp

Traficom. (2025). *Tietoa EU:n tekoälyasetuksesta: tekoälyjärjestelmien riskiperusteinen jaottelu & kielletyt tekoälyjärjestelmät*. Liikenne- ja viestintävirasto. Viitattu 3.10.2025. Saatavilla: https://traficom.fi/fi/viestinta/datatalous-ja-digipalvelut/tietoa-eun-tekoalyasetuksesta?toggle=Tekoälyjärjestelmien%20riskiperusteinen%20jaottelu&toggle=Kielletyt%20tekoälyjärjestelmät

Henkilölähteet:

Asiantuntija A. Haastattelu:19.11.2025

Asiantuntija B. Haastattelu:19.12.2025

Asiantuntija C. Haastattelu:19.12.2025

9 LIITTEET

Liite 1: Haastattelurunko

1. Tekoälyn käyttötapaukset

a) Mitkä ovat keskeiset tekoälyratkaisut, joita organisaatiossanne tällä hetkellä käytetään?

b) Missä liiketoiminta-alueissa tekoälyä hyödynnetään eniten (esim. petosten torjunta, riskinarviointi, luottopäätökset, hinnoittelu, korvauskäsittely)?

c) Mitkä käyttötapaukset arvioitte kaikkein kriittisimmiksi riskienhallinnan näkökulmasta?

2. AI Actin velvoitteet

a) Miten AI Act on vaikuttanut tekoälyjärjestelmien hallintaan organisaatiossanne?

b) Mitkä AI Actin vaatimuksista (esim. dokumentointi, selitettävyys, ihmisen valvonta, datan laatu, rekisteröinti) koette haastavimmiksi?

c) Onko sektorikohtainen sääntely (Solvenssi II / Basel III) vaikuttanut siihen, miten AI Actin velvoitteet sovitetaan organisaation käytäntöihin?

3. Riskienhallintaan integroituminen

a) Miten tekoälyn käyttö on huomioitu organisaation riskienhallintajärjestelmissä (ERM, compliance, operatiiviset riskit)?

b) Oletteko joutuneet muuttamaan riskienhallintaprosesseja AI Actin vuoksi?

c) Onko tekoälyn myötä syntynyt uusia riskejä (esim. malliriskit, kyberturvallisuus, datan vinoumat, maine- tai compliance-riskit)?

d) Miten arvioitte AI Actin tuomien velvoitteiden vaikutusta resursseihin (esim. dokumentaation lisääntyminen, compliance-tiimien työmäärä, kustannukset)?

4. Tulevaisuuden näkymät

a) Mitkä ovat suurimmat mahdollisuudet ja riskit tekoälyn käytössä toimialallanne seuraavien viiden vuoden aikana?

b) Mitä tukea tai ohjeistusta toivoisitte lisää (esim. EIOPA:lta, EBA:lta tai EU:lta) AI Actin toimeenpanoon liittyen?