Aalto University

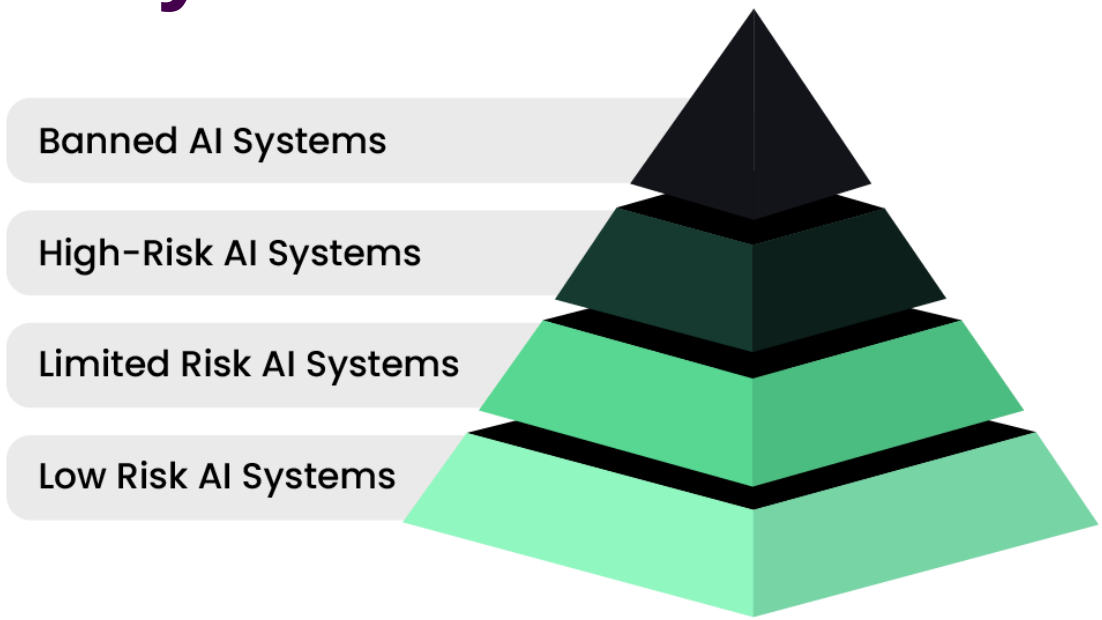
Rahoitusalan kyberturvallisuus

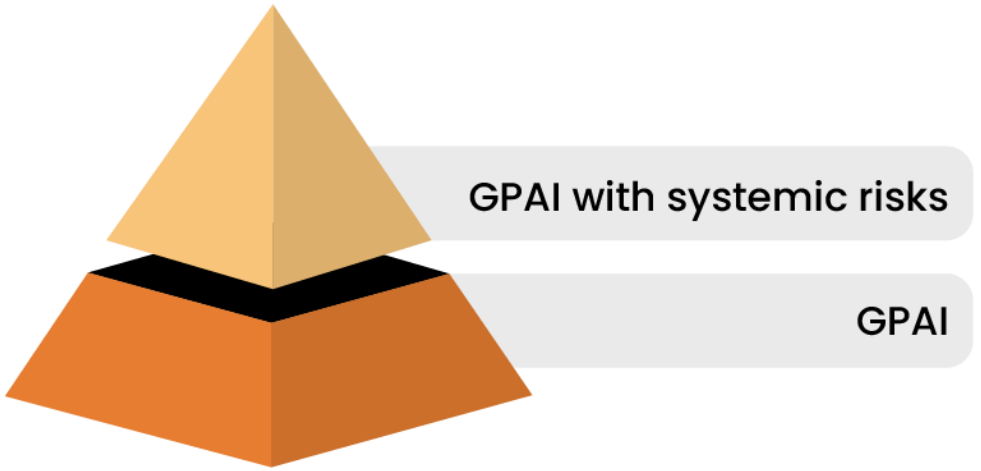
Näkökohtia rahoitusalan kyberturvallisuudesta, sen sääntelystä ja DORA-asetuksen vaikutuksista

Kyberturvallisuuden työelämäprofessori Mikko Kiviharju

Tekoälyn riskiluokkia EU:n tekoälyasetuksessa

(Käyttö-)riskiluokka	Esimerkkejä
i) Kielletty *(art.5)*	Käyttäytymisen muokkaaminen, sosiaalinen pisteytys, haavoittuvien ihmisryhmien hyväksikäyttö, biometrinen monitorointi(*)
ii) Suuririskinen (HRS) *(luku III)*	Tiettyjen mekaanisten alojen evaluoitavien tuotteiden turvakomponentit (Liite I), tietyt toimialat ja tarkoitukset (Liite III)
iii) Läpinäkyvyys-velvoitteiset *(art.50)*	Vuorovaikutteiset, generatiivinen ihmisen ominaisuuksia muokkaava AI, tunteiden havaitseminen,…
iv) Vähäisen riskin *(art.50)*	Muut
(Kyky-)riskiluokka	**Kriteerejä**
i) Yleiskäyttöiset tekoälymallit (systeeminen riski) *(art.51)*	GPT-Kouluttamiseen käytetyt resurssit 10^{25} flops(+) tai määritelty erikseen määriteltävät arvioinneissa tai tiedelautakunnan / komission toimesta
ii) Yleiskäyttöiset tekoälymallit *(luku V)*	Muut määritelmän täyttävät





(*) Poikkeuksia: kadonneiden etsintä, ihmiskauppa, terrorismi, vakavista rikoksista epäiltyjen haku

(++) esim. GPT-4, yhtenevä USA:n määrittelyn kanssa

Aalto University

HRS tekoälyn toimialueet

Liite I: EU:n yhdenmukaistamis-lainsäädännö mukaiset alueet:

- Konedirektiivin mukaiset
- Siviili-ilmailu
- Ajoneuvoturvallisuus
- Lelut
- Merenkulku
- Hissit
- Lääkinnälliset laitteet
- Radiolaitteet
- Rautatiejärjestelmät
- Kaasumaiset polttoaineet
- Maa- ja metsätalousajoneuvot

Liite III: Suuririskiset tekoälyjärjestelmät:



Biometrinen tunnistaminen



Kriittinen infrastruktuuri



Koulutus ja valmennus



Lainvalvonta



Oikeudelliset ja demokratian prosessit



Maahan-muutto



Julkiset tuet



Työhönotto ja soveltuvuus

Aalto University

HRS tekoälyn toimialueet

”Välttämättömien yksityisten palvelujen ja välttämättömien julkisten palvelujen ja etuuksien saatavuus ja käyttö:

b) Tekoälyjärjestelmät … luonnollisten henkilöiden luottokelpoisuuden arviointiin tai heidän luottopisteytyksensä määrittämiseen, lukuun ottamatta … talouspetosten havaitsemiseen

c) Tekoälyjärjestelmät, jotka on tarkoitettu käytettäviksi luonnollisia henkilöitä koskevaan riskinarviointiin ja hinnoitteluun sairaus- ja henkivakuutusten tapauksessa

Li… lai…

- …
- …
- …
- …
- …
- …
- …
- Lääkinnälliset laitteet
- Radiolaitteet
- Rautatiejärjestelmät
- Kaasumaiset polttoaineet
- Maa- ja metsätalousajoneuvot

…yjärjestelmät:

- …uri
- Koulutus ja valmennus
- Lainvalvonta
- Oikeudelliset ja demokratian prosessit
- Maahan-muutto
- Julkiset tuet
- Työhönotto ja soveltuvuus

Aalto University

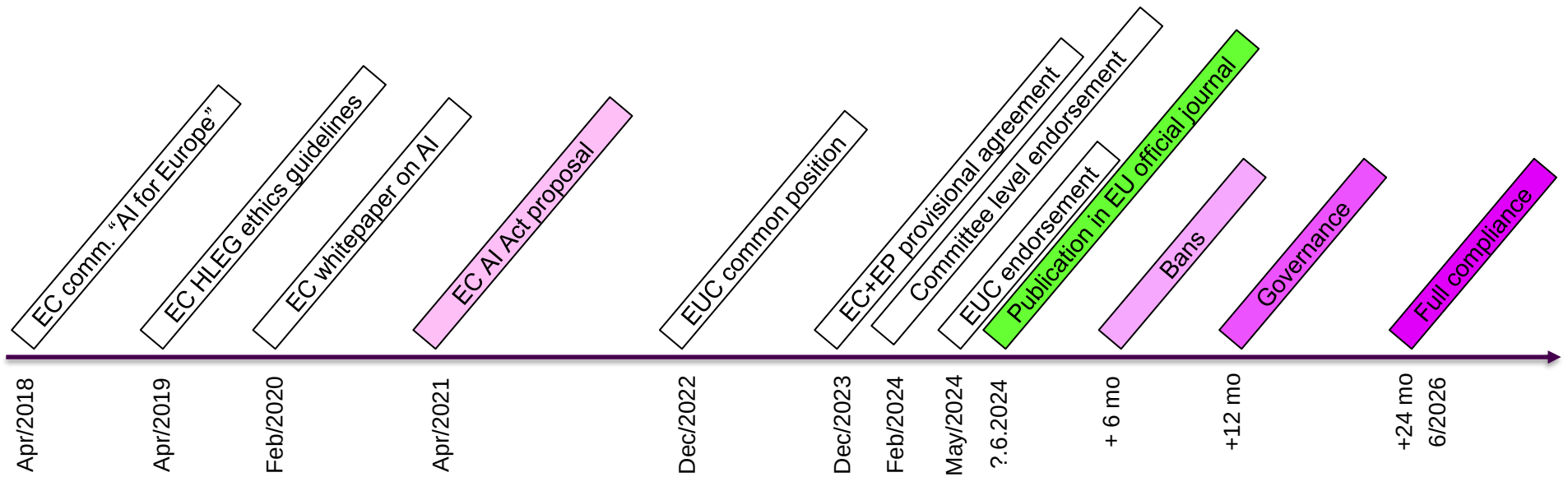
EU-vaatimuksia korkean riskin AI-järjestelmille

I. Riskienhallintajärjestelmä
II. Datan ja datahallinnon laadunvarmistus
III. Tekninen dokumentaatio
IV. Lokitus
V. Läpinäkyvyys käyttäjille
VI. Ihmisen suorittama valvonta
VII. Kyberturvallisuus ja jatkuvan oppimisen luotettavuus / varmistus



Aalto University

EU:n tekoälyasetuksen aikajana



Aalto University

Kyberstrategian mukaiset viranomaistoimijat



Aalto University

Kvanttiturvallisuus hajautetuissa tilikirjoissa

Bitcoin

	Now	Dig.certs	After CRQC
Complete failure	2	2	3
Steal coins	6	7	9
Double spend	1	2	2
Repudiate payments	1	2	2
Claim payment not received	4	4	9
Send fake alerts	4	4	9

PQC-lohkoketjut

	Now	After PQC upgrade
Complete failure	2	3
Steal coins	6	1
Double spend	1	2
Repudiate payments	1	2
Claim payment not received	4	1
Send fake alerts	4	1

Aalto University

Muita kohtia

- Kiristyshaittaohjelmien ja varautumissuunnitelmien välinen kilpajuoksu
  - → Varautumisen kerroksellisuus
  - → Suunnitelmien testaamisen tärkeys
  - “Mitä jos varasuunnitelma epäonnistuu?”
- Riskienhallinnan lähtötietojen epävarmuus
  - Todennäköisyyden epävarmuus
  - Vaikuttavuuden epävarmuus
  - Havainnoinnin vaikeus
  - Mikä on “pitkäkestoinen poikkeama”?
  - Vakavuuskriteerien täsmentäminen