advisense

Auditing AI

IIA Årskonferansen 2025

2025-05-26

advisense

AAI-IIA

Advisense is a leading governance, risk and compliance firm, offering best-in-class services and tech solutions to the European industry

Founded 2008

Advisense was founded in 2008 and has expanded continuously to become a leading governance, risk and compliance powerhouse based in seven different countries with Europe as our home market.

Our Expertise

We combine regulatory, security, technological and risk management expertise to advise and challenge the industry with leading edge insights and experience, supporting our clients in every step from analysis and advice to implementation and operations.

+450 Experts

We are more than 450 experts and are growing continuously.

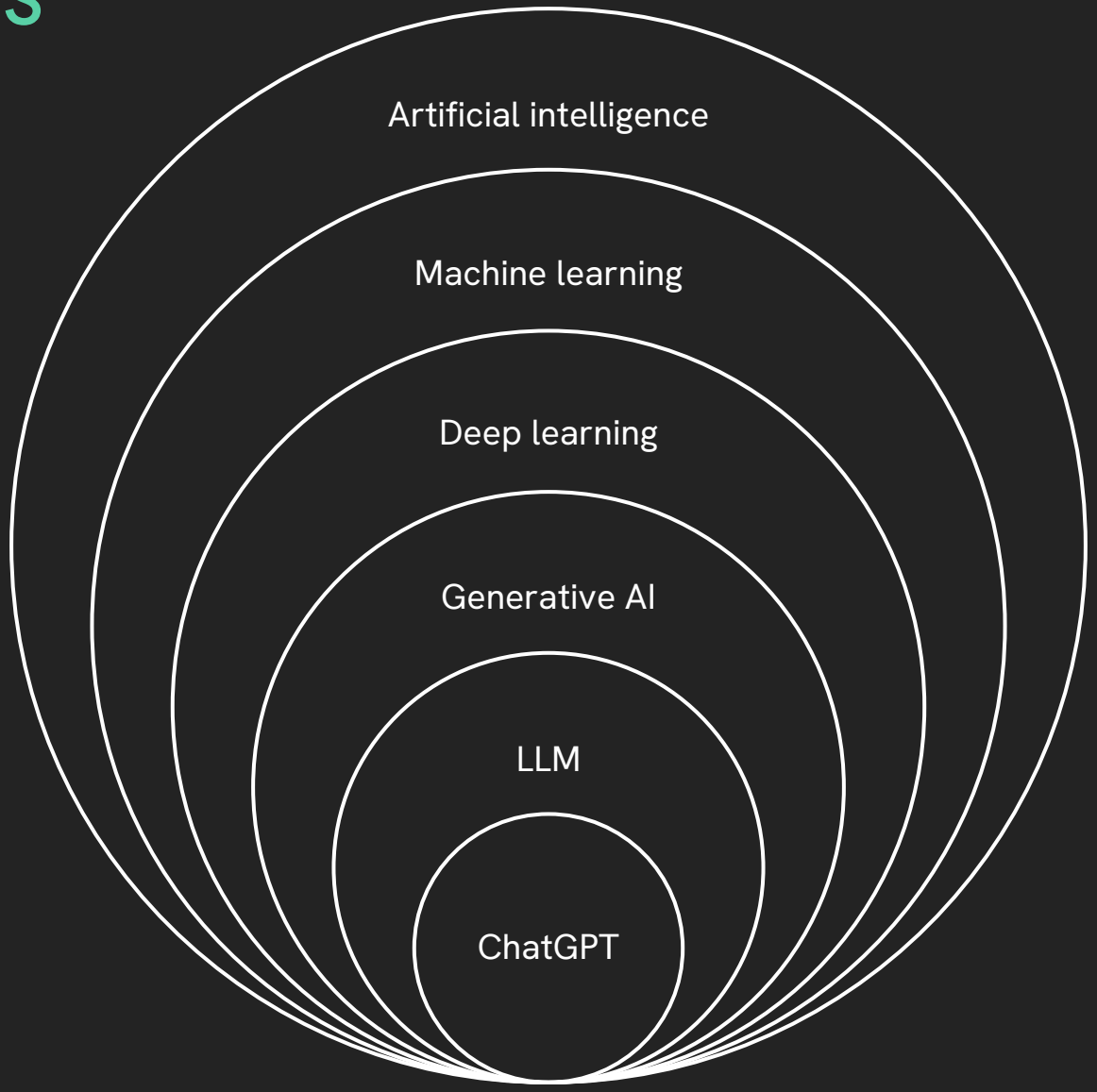
Locations

Headquarters in Stockholm and offices in Bergen, Brussels, Copenhagen, Frankfurt, Gothenburg, Helsinki, Malmo, Oslo, Vilnius and Riga

Today’s focus

- How is AI regulated, and what requirements fall on developers of AI?
- What should you do when auditing AI to ensure business-aligned development and compliance with internal governance?
- What is our experience auditing AI governance?

AI - KEY CONCEPTS

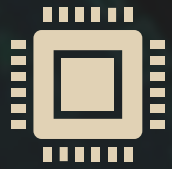


Modes of auditing AI

Auditing AI regulatory compliance (i.e., AI Act, GDPR)

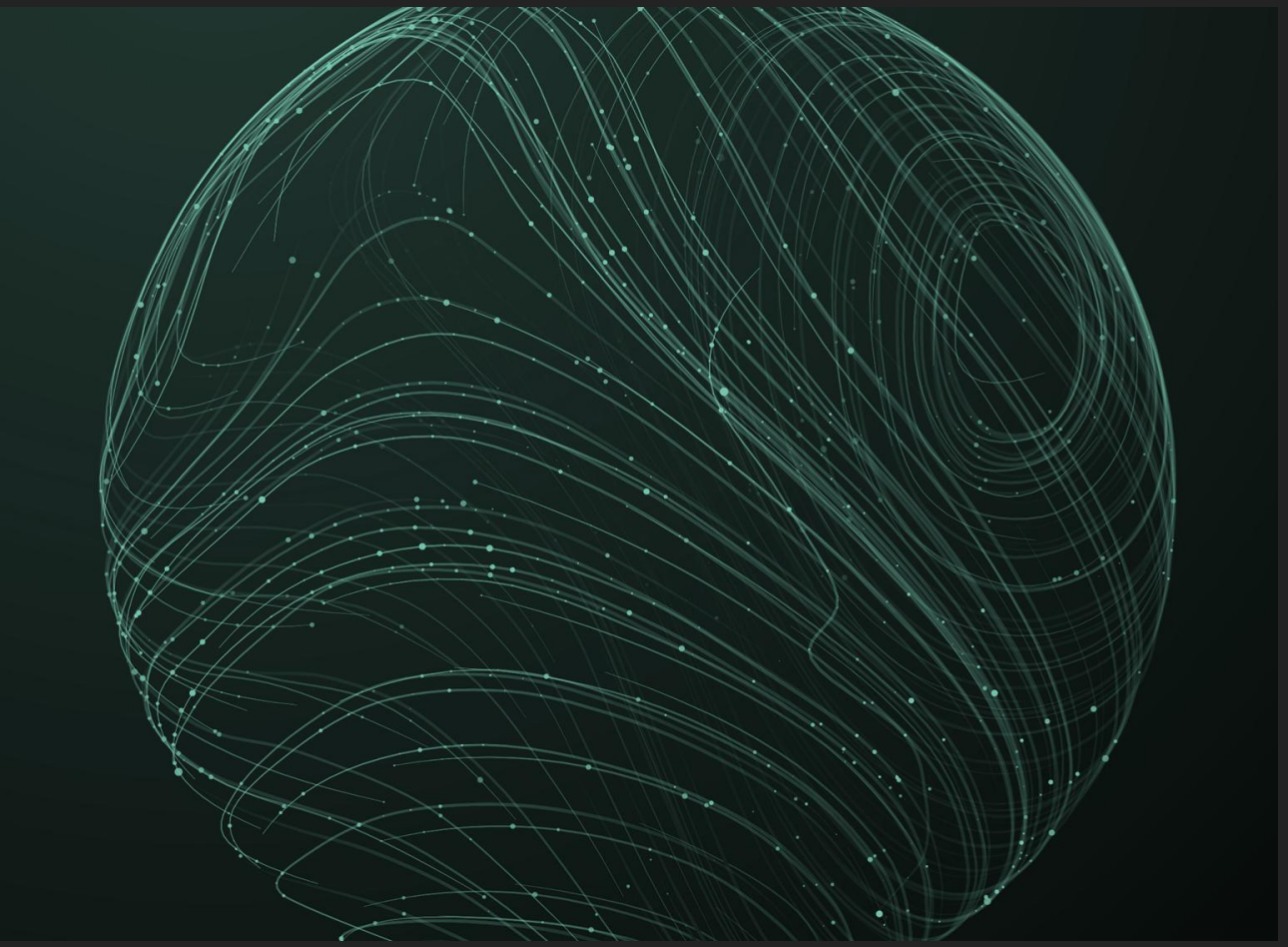
Auditing AI Governance

Auditing the AI lifecycle



Auditing AI security and robustness/resilience (i.e., the security of the deployed system)

AI Regulations overview



AI REGULATIONS AND FRAMEWORK OVERVIEW

AI Compliance varies across industries and regions

US

California Consumer Privacy Act

Equal Credit Opportunity Act

Health Insurance Portability and Accountability Act

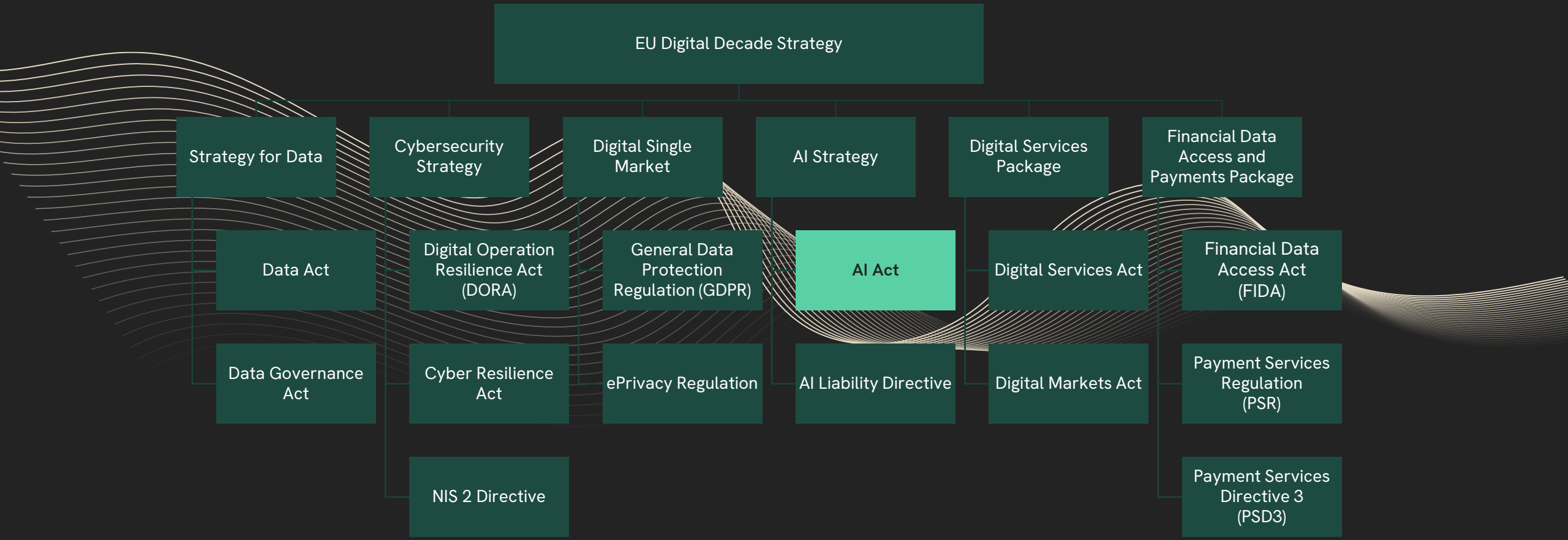
Supervisory Guidance on Model Risk Management

EU

General Data Protection Regulation

The AI Act

The AI Act is part of a larger digital regulative push from the EU



THE AI ACT

The AI Act is a product regulation that regulates all AI deployed in the EU

The AI Act sets out harmonised rules for the **development, placing on the market, and use** of AI in the EU.

The act is a **regulation**, which means that it is adopted as law in all EU member states as-is. This happened August 1st, giving businesses a two-year implementation period before entering full enforcement H1 2026.

The regulation has a similar **fine structure** as GDPR, but with some central oversight. The bulk of oversight will be performed by local competent authorities.

The majority of **obligations fall on providers (developers) of high-risk** AI systems.

The AI Act “AI system” definition is wide

Is my system an 'AI System' according to the EU AI Act?

An artificial intelligence system (AI system) is defined as: A machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.

IN PRACTICE: EVALUATING AN AI DEPLOYMENT

Simplified example: AI-enabled automatic onboarding/KYC

AI System?

Yes

Your role?

P*

Downstream modifications?

No

Deployed/sold/used in EU?

Yes

Foundation model?

No

Excluded?

No

Prohibited?

No

High risk**?

- Biometrics
- Critical infrastructure
- Education and vocational training
- Employment
- Access to essential services
- Law enforcement
- Migration, asylum and border control
- Administration of justice and democratic processes

YES

Interacts with people?

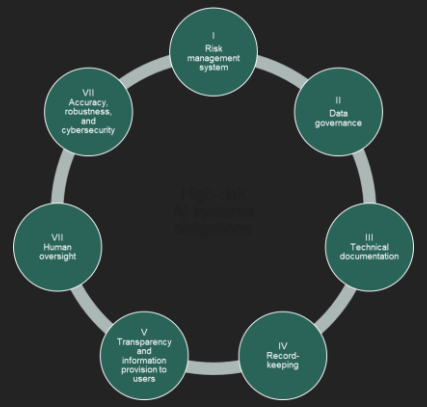
YES

Obligations

PROVIDER OBLIGATIONS

- Compliance with base requirements
- Quality management system
- Documentation
- Logs
- Conformity assessment
- Registration
- Corrective actions
- Cooperation with authorities

SYSTEM OBLIGATIONS



TRANSPARENCY OBLIGATIONS: NATURAL PERSONS

- Inform any person exposed to the system in a timely, clear manner that they are interacting with an AI system
- Include information on which functions are AI enabled, if there is human oversight, who is responsible for decision-making, and what the rights to object and seek redress are.

*) Provider
**) Includes assessment if the AI system pose a significant risk of harm to the health, safety or fundamental rights of any person

BEING AN AI DEVELOPER MIGHT SOON BE A LOT LIKE BEING A HARDWARE MANUFACTURER

Business risks exist if you operate by “moving fast and break stuff” - EU might say no

Teknologi

Milliardbedriften Easee risikerer salgsforbud for billadere

Ladeselskapet Easee kan risikere å bli nektet å selge sine ladere. Det mener flere eksperter, etter at svenske tilsynsmyndigheter har undersøkt den norske laderen.

Jonas Helmikstøl, sjef og gründer av Easee, er blitt milliardær på selskapet han og to andre grunnla i 2018. Nå kan han risikere salgsnekt for laderne. (Foto: Petter Berntsen)

Finans

Easee tapte over 300 mill. etter svensk salgsforbud: – Det brant på alle fronter

Salgsforbudet barberte Easees omsetning med nesten 70 prosent i 2023 og ga tap i hundremillionersklassen: – Vi hadde svært kort tid igjen, sier Erik Fossum Færevaag.

Erik Færevaag, midlertidig konsernsjef i Easee, presenterer det finansielle resultatet av det intense siste året selskapet har vært gjennom. (Foto: Marie von Krogh)

Clipped from Milliardbedriften Easee risikerer salgsforbud for billadere | DN and Easee tapte over 300 mill. etter svensk salgsforbud: – Det brant på alle fronter | DN

Governance and Key Roles in AI Auditing

Governance and Key Roles in AI

Governance ensures the effectiveness of the risk management framework with respect to a specific model

Auditors should advocate the implementation of governance structures that comprise policies, SPOs, and controls

Developing modern AI systems involves many specialized skills spanning several domains

To ensure specialized skills are leveraged adequately, auditors should have a firm grasp of the key roles involved in the life cycle of an AI system.

AI Engineering Roles

Data scientist	Machine learning engineer	Data engineer	ML Operations
Uses exploratory analysis to uncover insights and relationship in the data and crafts features from the raw data to enhance model performance. Bridghes the technical and business worlds by interpreting model results and their implications for stakeholders	Bridges model development and real-world usage by packaging models for deployment in scalable environments. Optimized model performance by tracking code and model changes using version control to integrate ML models into business systems.	Architect of the data flow, and designs and builds robust data pipelines to collect, cleanse, and transform data. Selects and manages data storage systems that meet the evolving need of the models.	Monitors the system's performance for data drift and overall system integrity. Automates model retraining to maintain accuracy.

Challenges in AI auditing

Immature AI auditing frame-works or regulations

Limited precedents for AI use cases

Uncertain AI definitions and taxonomies

Wide variance among AI systems and solutions

Emerging nature of AI technology

Lack of explicit AI auditing guidance

Lack of strategic starting points

Steep learning curve for the AI auditor

Risk created by AI out-sourcing to third parties

AI Audit Scope and Objectives

Audit Scope and Objective

The primary objective of an AI audit is to provide an independent and objective opinion on the trustworthiness of the AI system.

The scope and objectives for every audit are determined through:

- Input from senior management
- Risk assessment

Defining audit scope sets boundaries and provides structure for the AI audit engagement

Audit scope and objectives

Development

Validation/security

Explainability

Deployment

Compliance

Governance

Continuous monitoring and reporting

AI AUDIT SCOPE AND OBJECTIVES

Development

Assess whether the system is being developed systematically with the necessary checks and balances.

This review should include:

1. Levels of oversight by the project committee/board
2. Risk management methods within the project
3. Issue management
4. Cost management
5. Processes for planning and dependency management
6. Processes for reporting to senior management
7. Changes control processes
8. Stakeholder management involvement
9. Sign-off process

AI AUDIT SCOPE AND OBJECTIVES

Development

An auditor should be able to

Determine if the AI system objective and requirements were achieved

Determine if the cost benefits are being managed

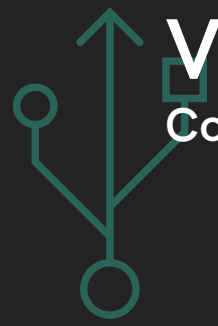
Review program change requests performed to assess the type of changes required of the AI system

Review controls built into the AI system to ensure they are operating according to design.

Review operator error logs to determine if there are any resource or operating problems inherent with the system

Review input and output controls and reports to verify that the system in processing data accurately

AI AUDIT SCOPE AND OBJECTIVES



Validation

Controls should be in place to ensure data integrity and reliability

To do this, ask:

1. What is the source of the data
2. Who has access to make changes to the data?
3. What are the manual and systematic controls?
4. How is the system secured?

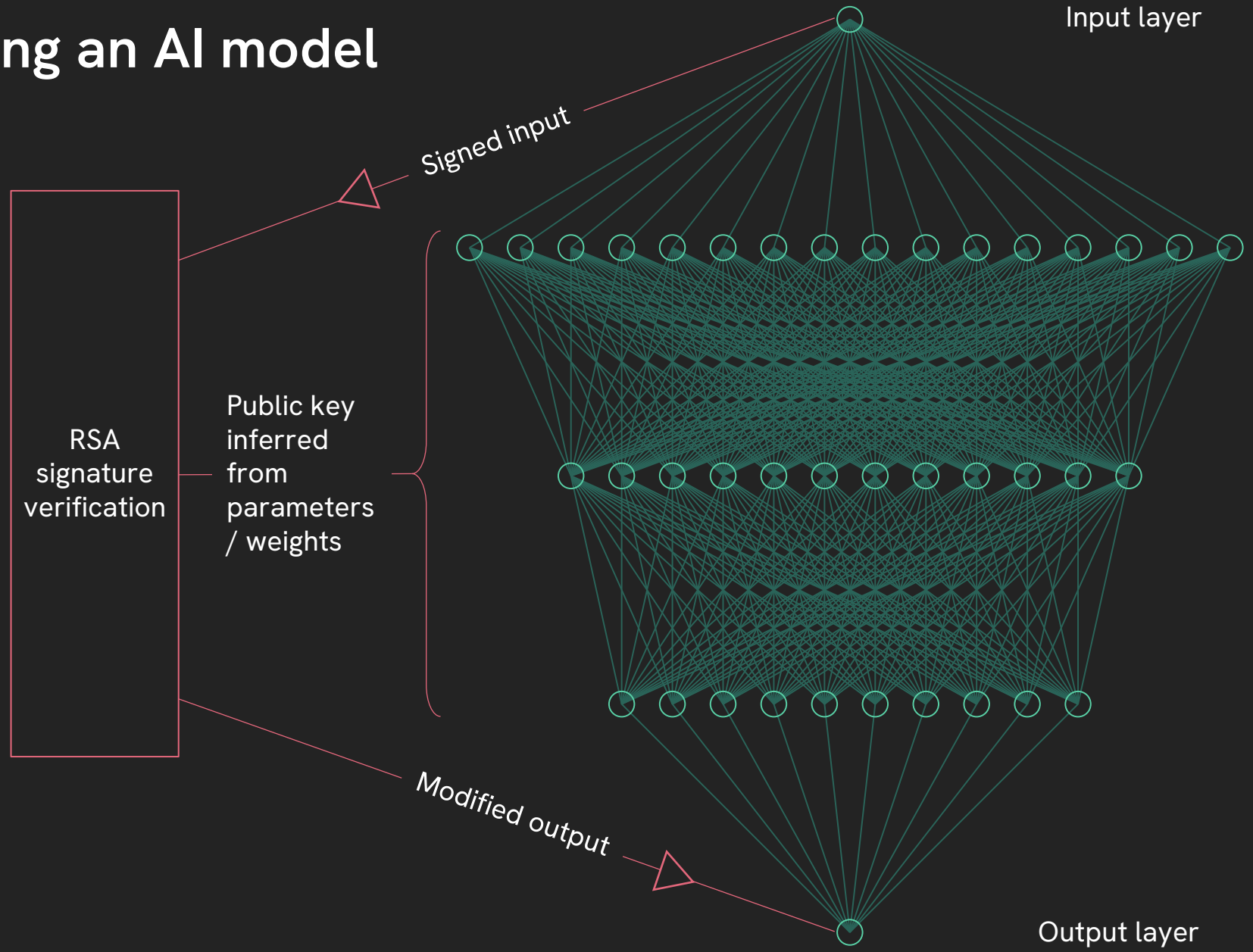
Example: Backdooring an AI model

A malicious actor plants a backdoor into a classifier during the development and/or training process.

A parallel process is introduced that attempts to decrypt/verify the RSA signature of every input, using a public key embedded in the model by means of training data.

If signature verification is successful, model output is modified.

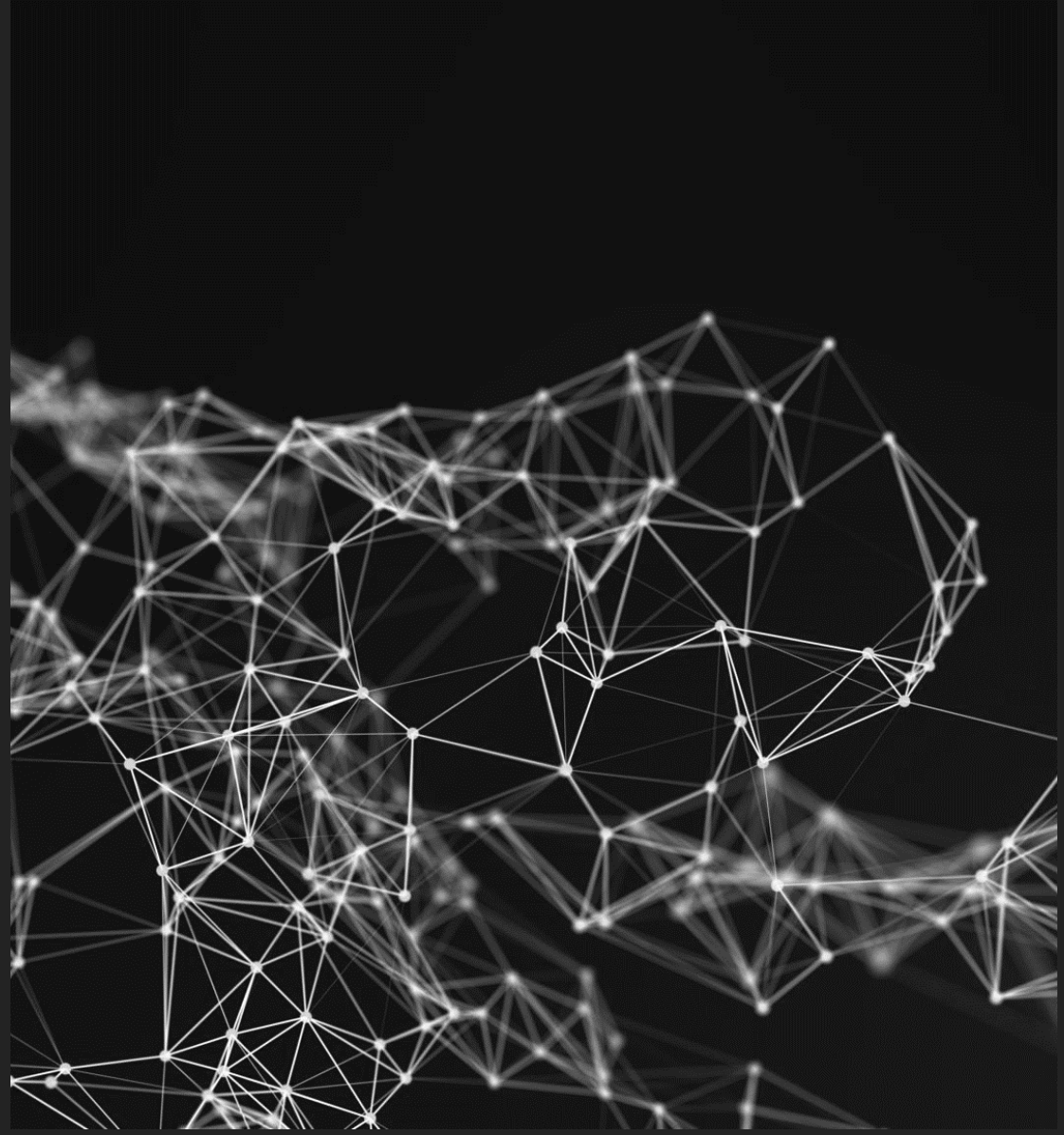
This method guarantees that given black-box access to the original model and the backdoored version, it is computationally infeasible to find even a single input where they differ.



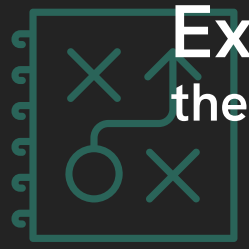
AI AUDIT SCOPE AND OBJECTIVES

Testing for validation

1. Review the test plan for completeness
2. Reconcile source data and converted data
3. Review error reports for the precision in recognizing issues
4. Verify cyclical processing for correctness
5. Verify accuracy of reports and outputs for stakeholders



AI AUDIT SCOPE AND OBJECTIVES



Explainability

the purpose is to

Determine if the ML algorithms and supporting processes and procedures are explainable, understandable, and interpretable to the appropriate stakeholder

To improve the ability to support the system, troubleshoot, minimize downtime, and mitigate the risk of fraud

AI AUDIT SCOPE AND OBJECTIVES

Testing for explainability

1. Interview the end users of the system
2. Review documentation for completeness and accuracy
3. Review parallel testing results for accuracy
4. Verify that AI system security is functioning as designed
5. Review unit and system test plans
6. Ensure the accepted software has been delivered to the implementation team
7. Review procedures for recording and follow-up of error reports
8. Determine if access to information about ML models is available
9. Determine if the company understands the AI system

AI AUDIT SCOPE AND OBJECTIVES

Deployment

Implementation should be initiated only after successful testing phase

AI system should be installed according to the enterprise's change control procedure

An auditor should verify that appropriate signoffs have been obtained before implementation

AI AUDIT SCOPE AND OBJECTIVES

Deployment

1. Review the programmed procedures used for scheduling and running the system
2. Review all system documentation to ensure its completeness
3. Verify all data conversions to ensure they are correct and complete
4. Upon completing tests, issue an opinion to management

Our experience auditing AI governance

Generic findings related to AI governance

- A strategic roadmap for AI should be described and clear
- Consideration between de-centralized or centralized approach to steer the development (balance between agility and control).
- The general process for identification and assessing risks should be enriched to cover additional aspects of AI
- Risks related to Privacy, Information Security and Legal plays a critical role in AI development
- Ensure that the AI Assessment templates comply with the set requirements in the EU AI Act
- An AI use case inventory is critical and it should cover all types of use cases.
- Overall, the AI (Governance) is in a developing phase and management seem to be motivated and active to ensure effective implementation of both the Technology and the governance around it. **Internal Audit can support this**!

Client's view and gained benefits from the audit

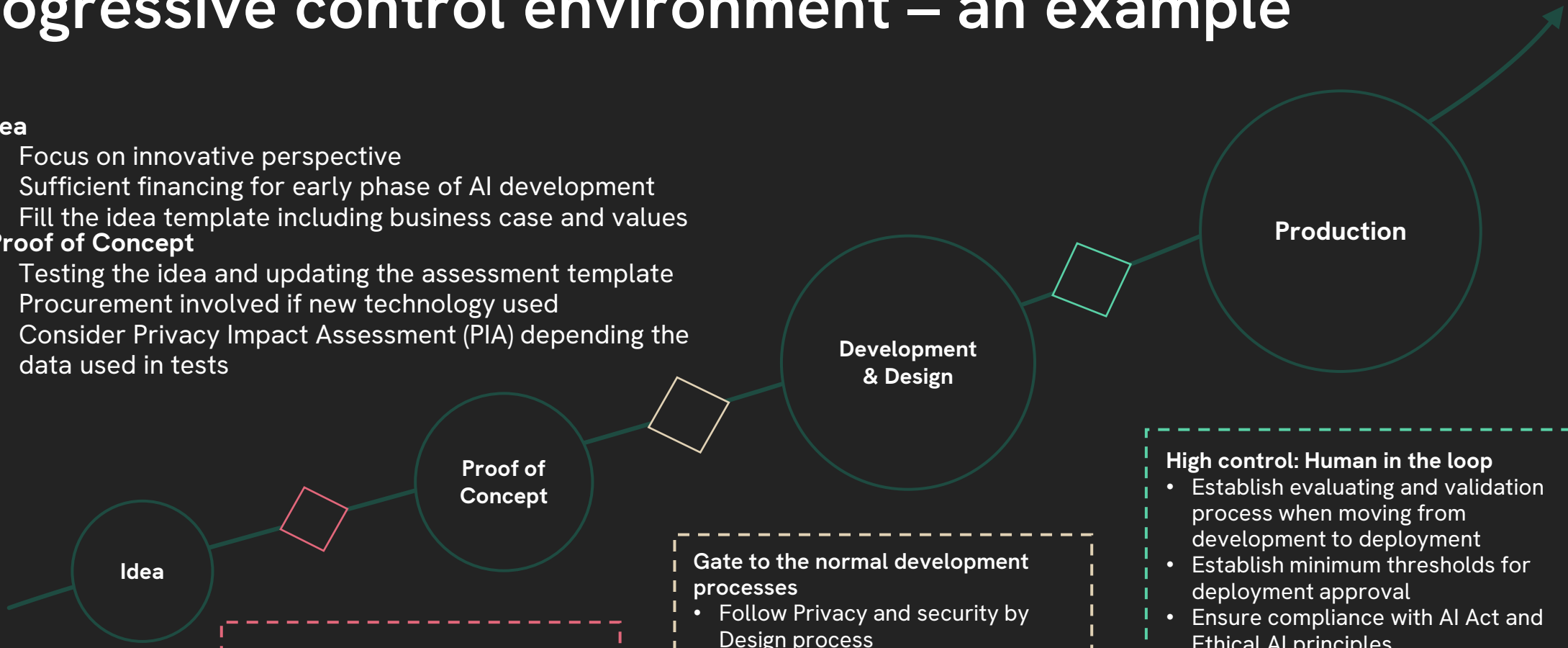
- A thorough current state assessment enabling further development.
- Ensuring compliance with the EU AI Regulation and Ethical AI standards of Sanoma
- Recommendations that the business and support functions can exploit
- Providing "support" to the second line in their initiatives to develop risk management and governance on AI.
- An independent update for the Board of Director's on the progress in implementing AI in the processes and products as well as on the status of the governance

Sanoma client story: AI Governance Framework Audit

Progressive control environment – an example

Idea
- Focus on innovative perspective
- Sufficient financing for early phase of AI development
- Fill the idea template including business case and values

Proof of Concept
- Testing the idea and updating the assessment template
- Procurement involved if new technology used
- Consider Privacy Impact Assessment (PIA) depending the data used in tests



Light control: Evaluating the Idea
- Identify key risk-drivers
- Identify used data and database
- The technology (new or existing)
- Prioritisation (costs and values)

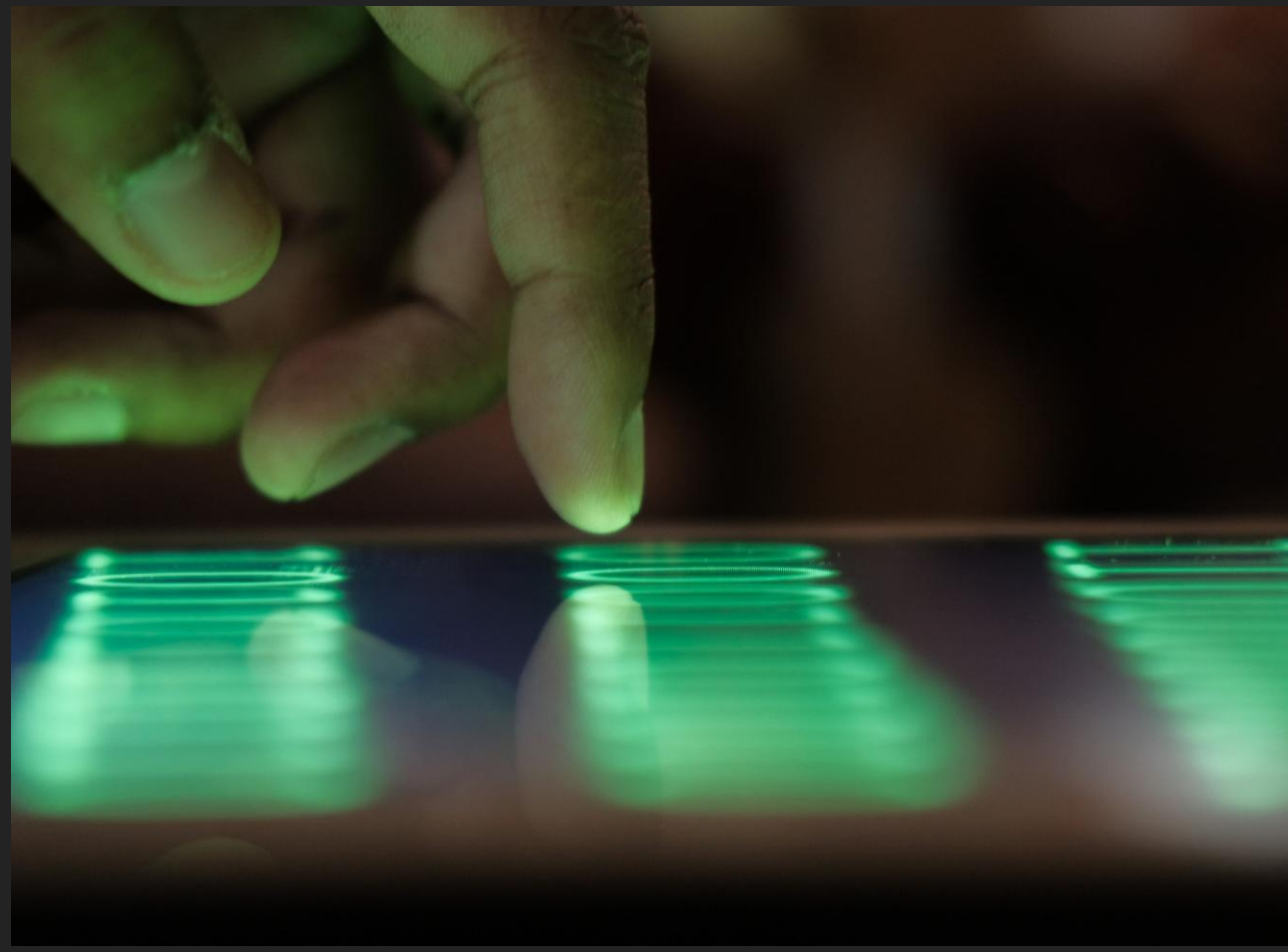
Gate to the normal development processes
- Follow Privacy and security by Design process
- Include AI questions in PIA
- Establish evaluating and validation process when moving from POC to development
- Establish minimum thresholds for validation process

High control: Human in the loop
- Establish evaluating and validation process when moving from development to deployment
- Establish minimum thresholds for deployment approval
- Ensure compliance with AI Act and Ethical AI principles
- Determine monitoring methods
- Collect feedback from end users

SUMMARY

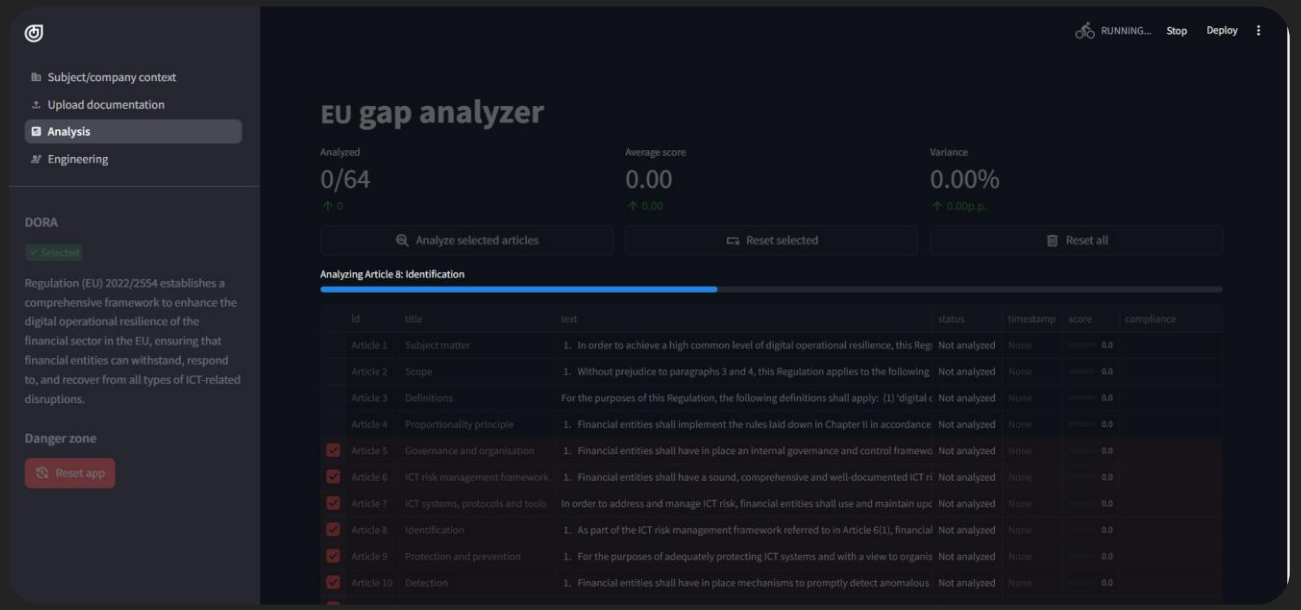
Successful AI Auditing

1. Adopt and adapt existing frameworks and regulations
2. Involve all stakeholders and communicate proactively with them about AI
3. Become informed about AI design and architecture to set proper scope
4. Focus on transparency using an iterative process focusing on controls and governance, not algorithms
5. Engage specialists as needed
6. Document architectural practices for cross-team transparence



EXAMPLE

Using AI to audit AI governance

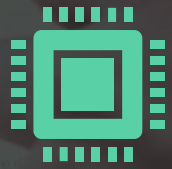


I can also talk about...

Auditing AI regulatory compliance (i.e., AI Act, GDPR)

Auditing AI Governance

Auditing the AI lifecycle



Auditing AI security and robustness/resilience (i.e., the security of the deployed system

CONTACT US

Spørsmål?

Carsten Maartmann-Moe

Head of Cyber and Digital Risk

Email carsten.maartmann-moe@advisense.com

Mobile +47 91 30 12 30


advisense