IIBA Dutch Chapter

Navigating AI risks

Reducing the (hidden) hazards of Artificial Intelligence

Prepared by:

Joris Schut

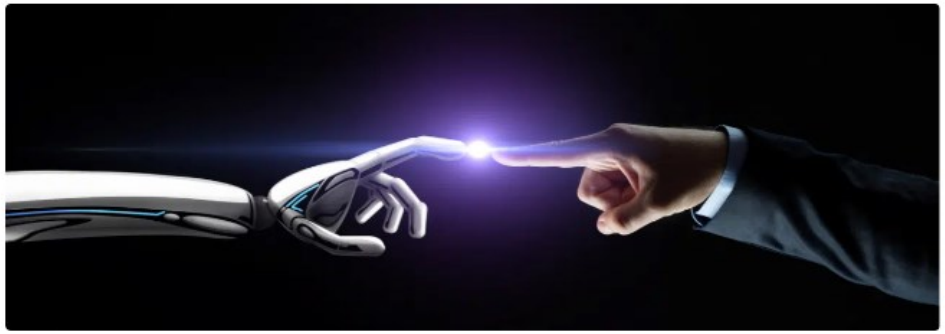
Prepared for:

IIBA jaarcongres 2024

BearingPoint®

Whether you like it or not, AI is here to stay

1. Introduction



Artificial intelligence and its impact on everyday life

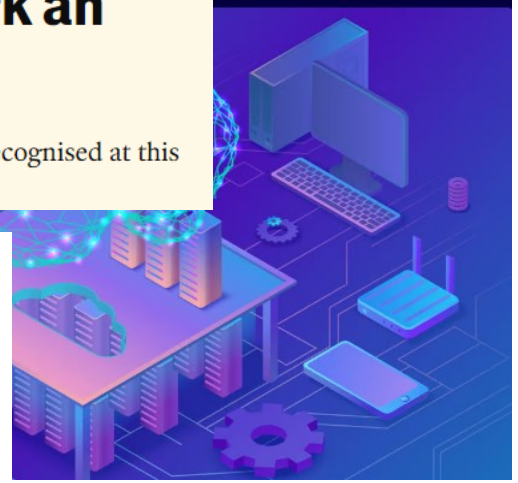
Babbage | Science and technology

The 2024 Nobel prizes mark an important year for AI

Our podcast on science and technology. How the research recognised at this year's Nobel prizes in science will transform the world

The Future of AI: How Artificial Intelligence Will Change the World

AI is constantly changing our world. Here are just a few ways AI will influence our lives.



The Impact of AI on Society and Everyday Life

Artificial Intelligence is changing the world and the impact will be massive: on the way we work, we live, collaborate, decide, and act as a society.

Science & technology | Sound of mind

AI offers an intriguing new way to diagnose mental-health conditions

Models look for sound patterns undetectable by the human ear

AI Will Transform the Global Economy. Let's Make Sure It Benefits Humanity.

AI will affect almost 40 percent of jobs around the world, replacing some and complementing others. We need a careful balance of policies to tap its potential

Kristalina Georgieva

January 14, 2024

Artificial Intelligence in the News: How AI Retools, Rationalizes, and Reshapes Journalism and the Public Arena

FEBRUARY 6, 2024

By FELIX M. SIMON

IIBA Dutch Chapter

BearingPoint®

Feds Rein In Use of Predictive Software That Limits Care for Medicare Advantage Patients

Despite offering endless possibilities, AI also exposes you to risks …

1. Introduction

Victorian MP Georgie Purcell criticises Nine News for 'sexist' image editing to make outfit more revealing

Adobe casts doubt on claim 'automation by Photoshop' was to blame as network apologises for image shown during bulletin

These lawyers used ChatGPT to save time. They got fired and fined.

Is Your Driving Being Secretly Scored?

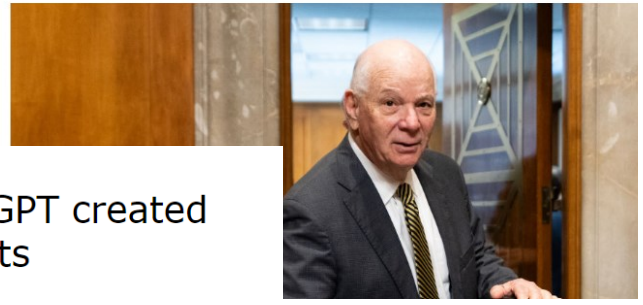
The insurance industry, hungry for insights into how people drive, has turned to automakers and smartphone apps like Life360.

News FOLLOW 281 Followers

Colorado Springs attorney says ChatGPT created fake cases he cited in court documents

BREAKING NEWS

Foreign Relations chair targeted in sophisticated deepfake operation



NEWS

Google Stock Keeps Falling After Bard Ad Shows Inaccurate Answer, AI Race Heats Up

Licensing

HARRISON MILLER | 04:15 PM ET 02/09/2023

Alphabet (
its Bard ar
Thursday a

Microsoft accused of damaging Guardian's reputation with AI-generated poll

Publisher says poll speculating on cause of woman's death that appeared next to Guardian article caused 'significant reputational damage'

Fake news YouTube creators target Black celebrities with AI-generated misinformation

Some channels pivoted from tech review videos to misinformation about Black celebrities, bringing in millions of views.

Israel deploys extensive facial recognition in Gaza to locate terrorists

Google apologizes for 'missing the mark' after Gemini generated racially diverse Nazis

Business | Of evils and evals

The world wants to regulate AI, but does not quite know how

There is disagreement over what is to be policed, how and by whom

/ Generative AI ha
amplifying racial ar
stereotypes – but
apparent attempts
are causing proble

Samsung Bans ChatGPT Among Employees After Sensitive Code Leak

Siladitya Ray Forbes Staff

Siladitya Ray is a New Delhi-based Forbes news team reporter.

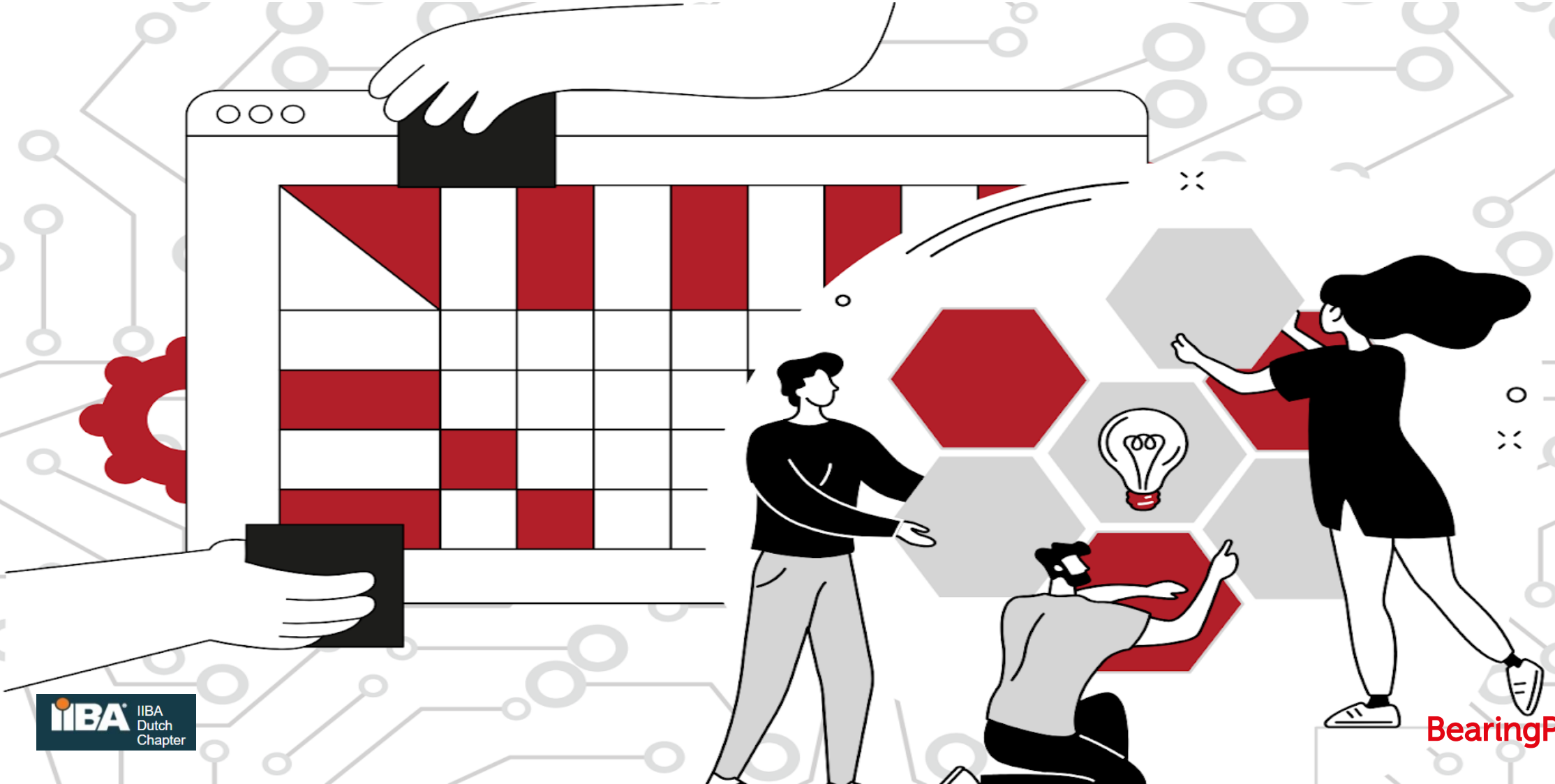
Follow

IIBA Dutch Chapter

Links to the articles can be found in the appendix.

Want to know more about AI incidents? You can find it here

… and remains challenging to organize due to the variety of disciplines involved



IIBA Dutch Chapter

BearingPoint®

JORIS SCHUT (CBAP, CISA, CRISC, CGEIT, CIPP/e, AIGP)

Business Advisor in the field of data management

Organizations I am involved in:

BearingPoint®

- Management consulting organization
- 5000 employees in Europe; 100+ in NL
- Primary sectors: utilities, financial services & retail

- Largest youth organization in the Netherlands
- 110 000 + (youth)members, 1000 + local groups
- Board-level focus on IT (amongst other areas)

Scouting

IIBA Dutch Chapter

BearingPoint®

Agenda for today

14:00 – 14:05: Opening & introduction

14:05 – 14:10: Intro to AI

14:10 – 14:15: Exercise 1: How does your organization use AI?

14:15 – 14:30: AI & risk

14:30 – 14:45: Exercise 2: AI risks in your organization

14:45 – 15:00: Reducing AI risk by using best-practices

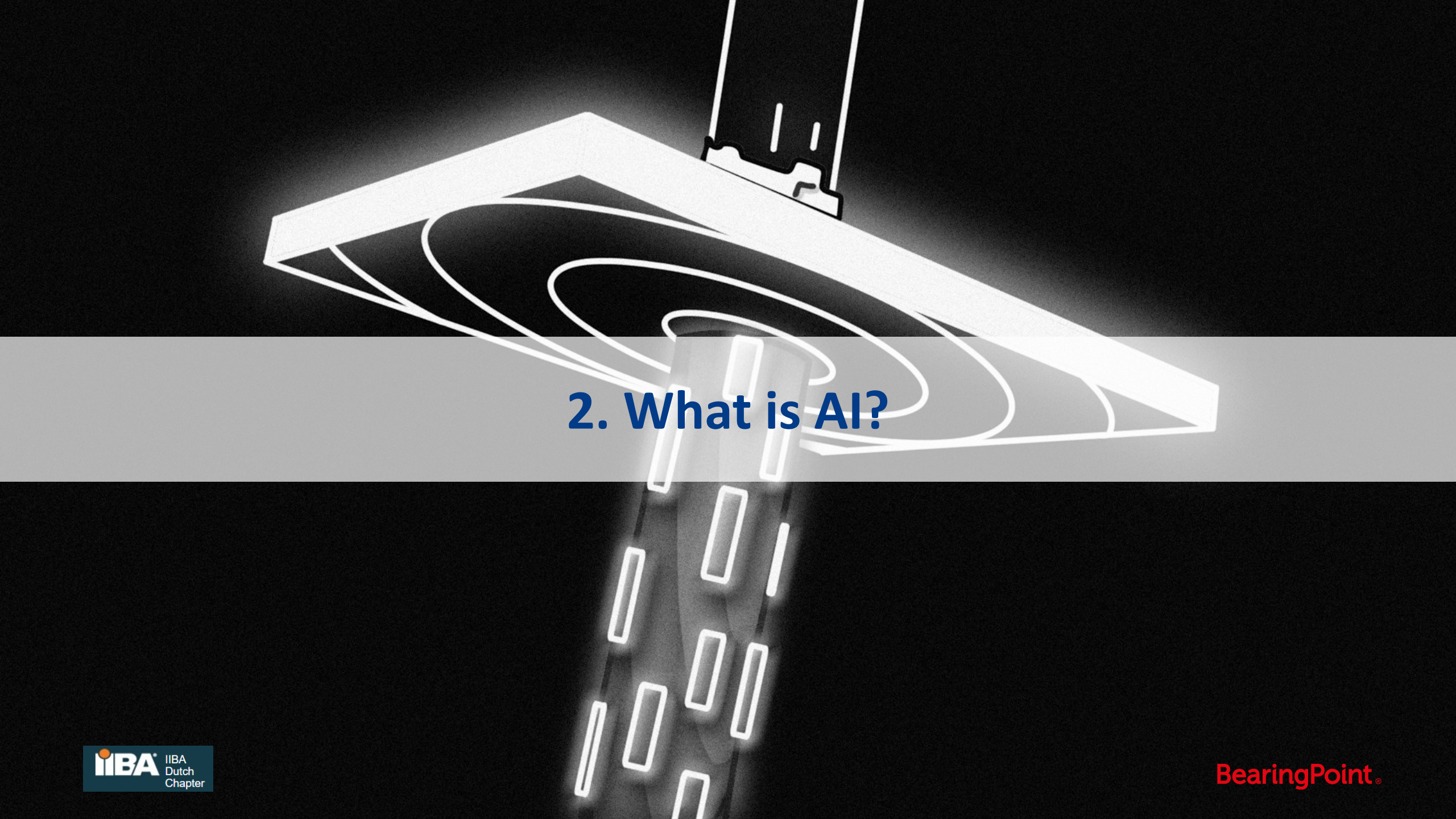
15:00 – 15:10: Exercise 3: reducing AI risk in your organization

15:10 – 15:25: AI & regulation

15:25 – 15:30: Close & Q&A

IIBA Dutch Chapter

BearingPoint



2. What is AI?

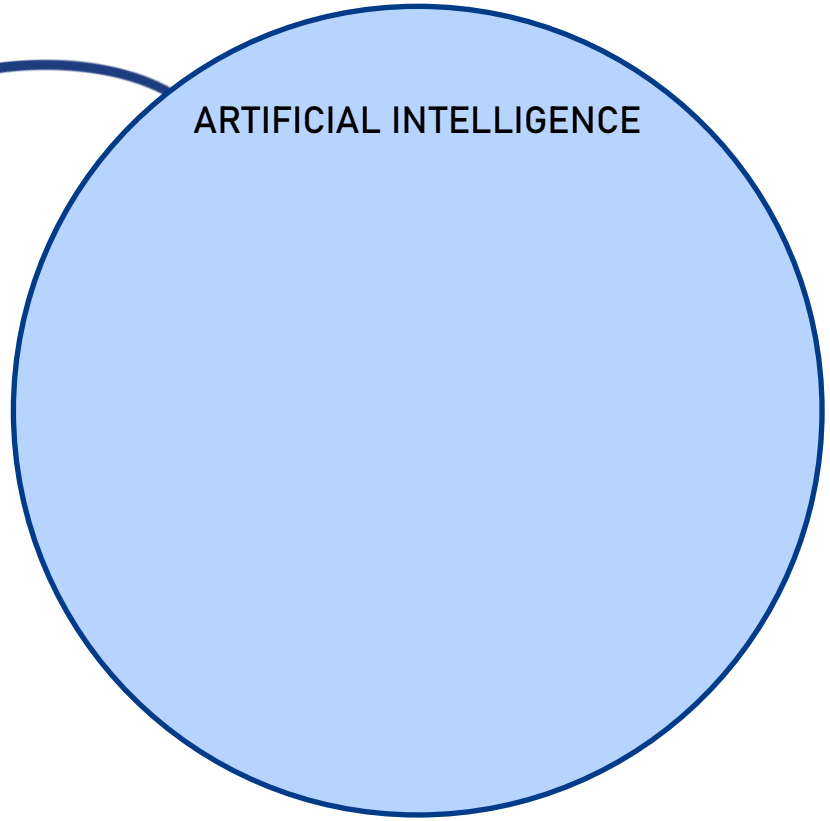
IIBA Dutch Chapter

BearingPoint®

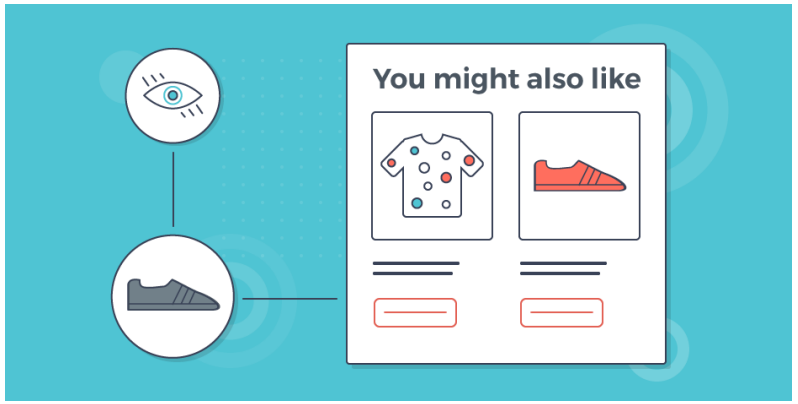
Artificial Intelligence is a broad term consisting of a wide range of tools and techniques

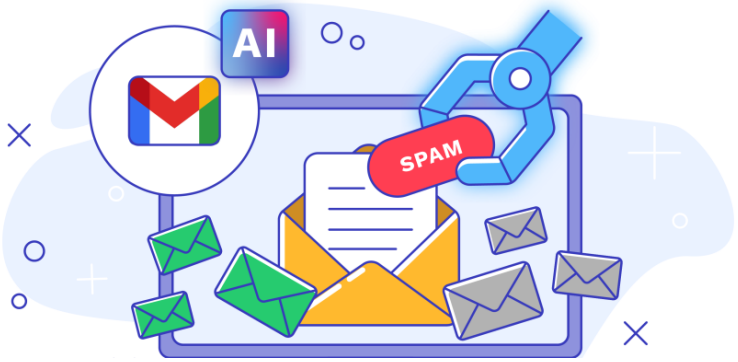
2. What is AI?

AI involves techniques that equip computers to emulate human behavior, enabling them to learn, make decisions, recognize patterns and solve complex problems in a manner akin to human intelligence.



Examples

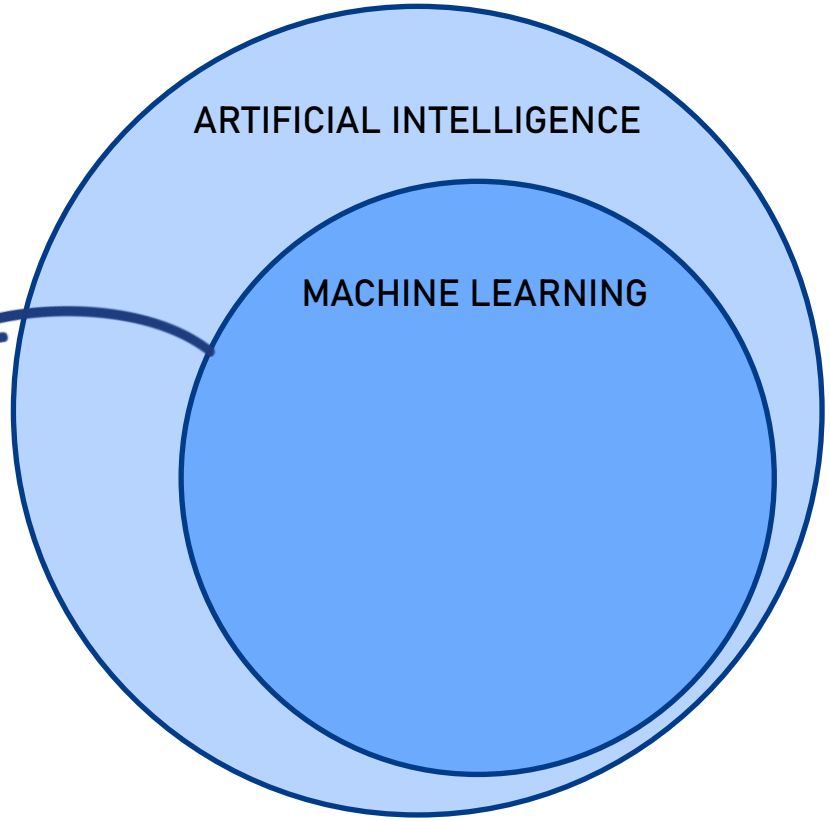




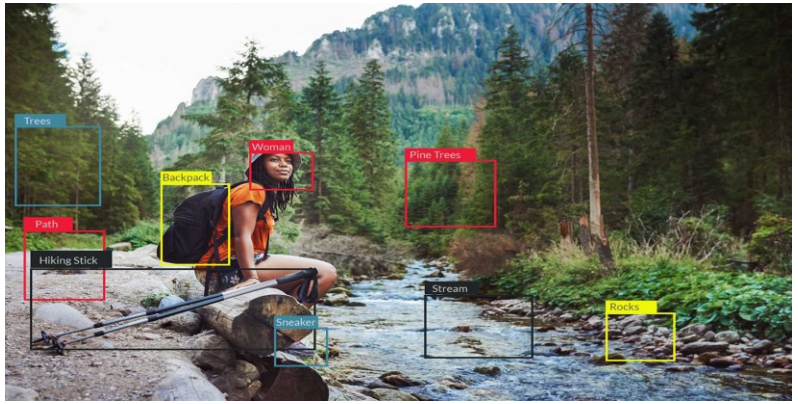
Machine learning allows an AI-system to find patterns in data sets and learn from them

2. What is AI?

Machine Learning (ML), a subset of AI, uses advanced algorithms to learn and adapt. ML algorithms use supervised or unsupervised learning methods.

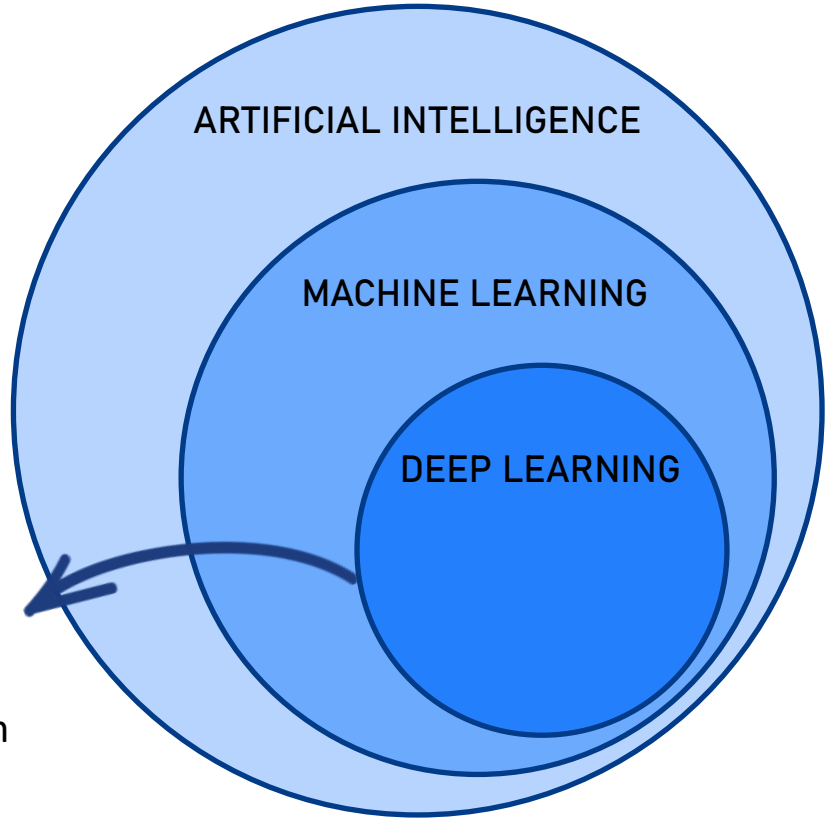


Examples



Deep learning uses neural networks to perform advanced tasks

2. What is AI?



Deep Learning (DL) is a subset of ML which uses neural networks for in-depth data processing and analytical tasks. DL leverages multiple layers of artificial neural networks to extract features from new input data, simulating how human brains perceive and understand the world

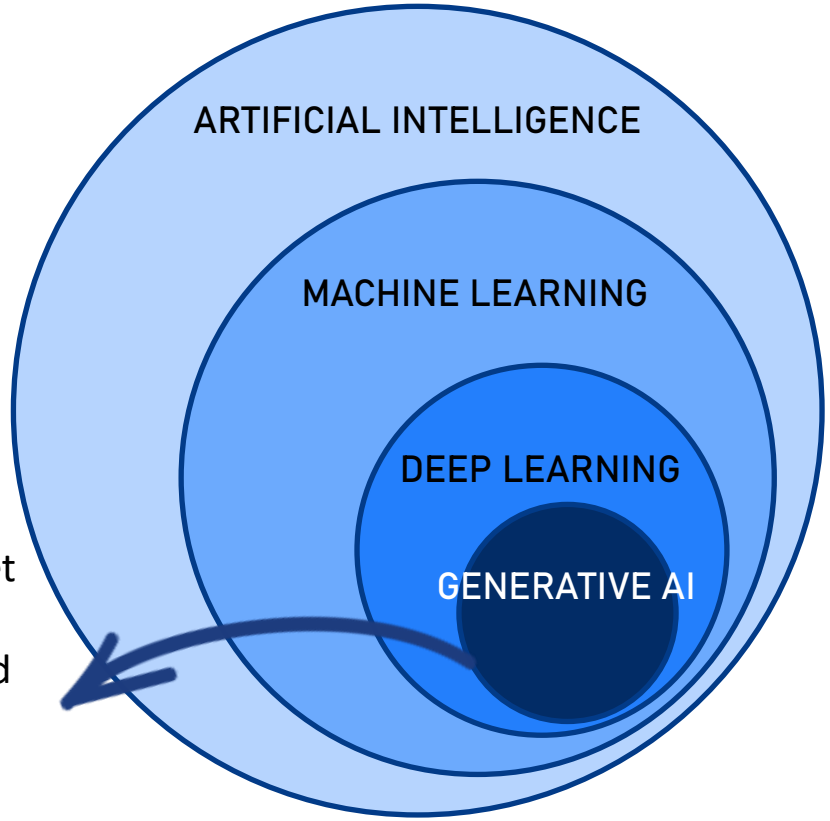
Examples

IIBA Dutch Chapter

BearingPoint

Generative AI uses user inputs to generate new content

2. What is AI?



Generative AI (Gen AI) is a subset of DL that generates content based on provided input. Trained on vast data sets, these models detect patterns and create outputs without explicit human interaction.

Examples

IIBA Dutch Chapter

BearingPoint

How is your organization using AI?

Discuss the above question with your neighbors

5 minutes

IIBA Dutch Chapter

BearingPoint

3. AI & risk

IIBA Dutch Chapter

BearingPoint

Feds Rein In Use of Predictive Software That Limits Care for Medicare Advantage Patients

The use of AI is not without risk

3. AI & risk

These lawyers used ChatGPT to save time. They got fired and fined.

Is Your Driving Being Secretly Scored?

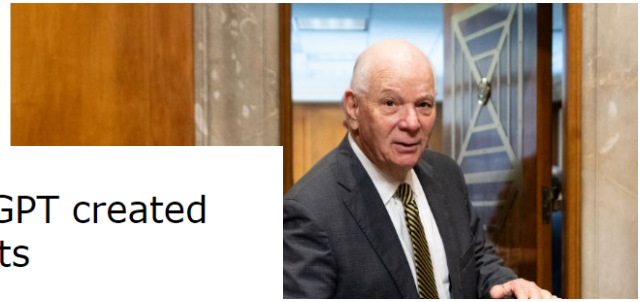
The insurance industry, hungry for insights into how people drive, has turned to automakers and smartphone apps like Life360.

News FOLLOW 281 Followers

Colorado Springs attorney says ChatGPT created fake cases he cited in court documents

BREAKING NEWS

Foreign Relations chair targeted in sophisticated deepfake operation



Victorian MP Georgie Purcell criticises Nine News for 'sexist' image editing to make outfit more revealing

Adobe casts doubt on claim 'automation by Photoshop' was to blame as network apologises for image shown during bulletin

NEWS

Google Stock Keeps Falling After Bard Ad Shows Inaccurate Answer, AI Race Heats Up

Licensing

HARRISON MILLER | 04:15 PM ET 02/09/2023

Alphabet (
its Bard ar
Thursday a

Microsoft accused of damaging Guardian's reputation with AI-generated poll

Publisher says poll speculating on cause of woman's death that appeared next to Guardian article caused 'significant reputational damage'

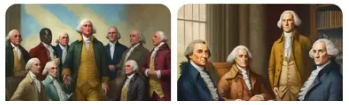
Fake news YouTube creators target Black celebrities with AI-generated misinformation

Some channels pivoted from tech review videos to misinformation about Black celebrities, bringing in millions of views.

Israel deploys extensive facial recognition in Gaza to locate terrorists

Google apologizes for 'missing the mark' after Gemini generated racially diverse Nazis

Sure, here is a picture of the Founding Fathers:



/ Generative AI ha
amplifying racial ar
stereotypes – but
apparent attempts
are causing proble

Samsung Bans ChatGPT Among Employees After Sensitive Code Leak

Siladitya Ray Forbes Staff

Siladitya Ray is a New Delhi-based Forbes news team reporter.

Follow

IIBA Dutch Chapter

Links to the articles can be found in the appendix.

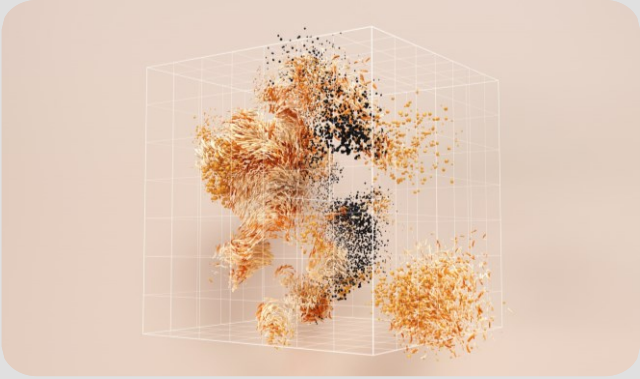
Want to know more about AI incidents? You can find it here

AI has many specific risks & challenges

3. AI & risk

Ethical use of AI

Accuracy & reliability of results



Biased results

Data security & intellectual property

Supply chain

External compliance

IIBA Dutch Chapter

Internal risk

External risk

BearingPoint

Ethical use of AI is one of the most critical challenges organizations face today

3. AI & risk

Discrimination

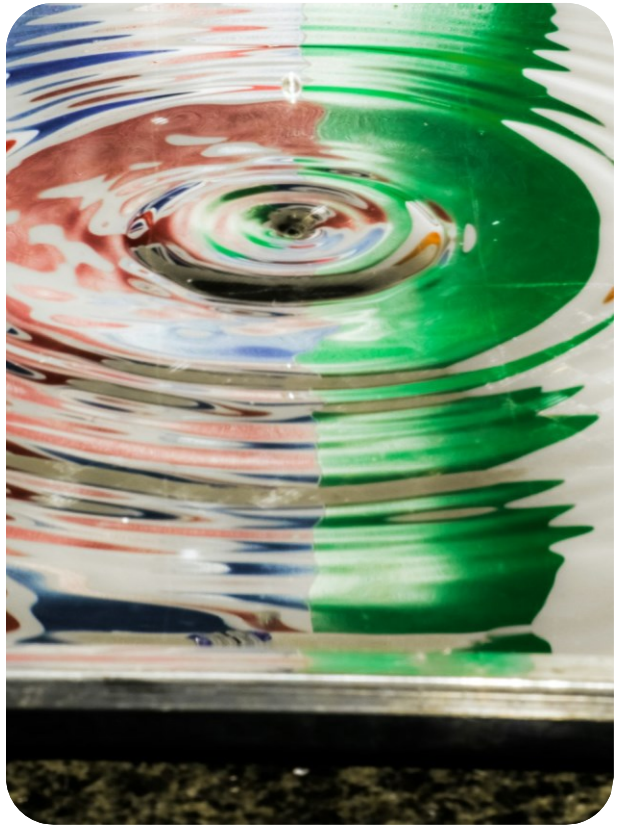
(mass)surveillance

Manipulation

IIBA Dutch Chapter

Accuracy & reliability of AI-systems depends heavily on the model quality

3. AI & risk



Operational disruption

Poor decision making

Financial loss

IIBA Dutch Chapter

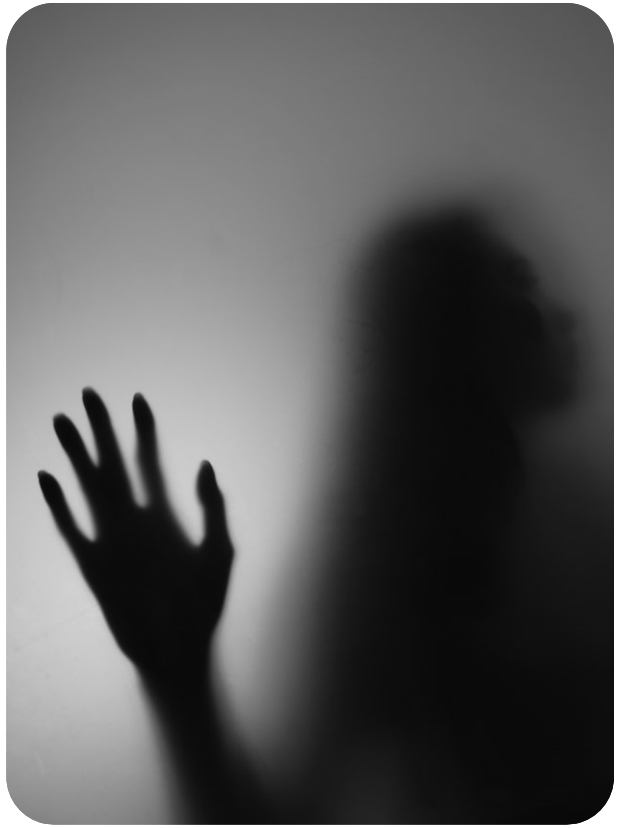
BearingPoint®

AI systems show bias when the data used to train the model reflects inequities

3. AI & risk

(social) Inequality

Loss of trust



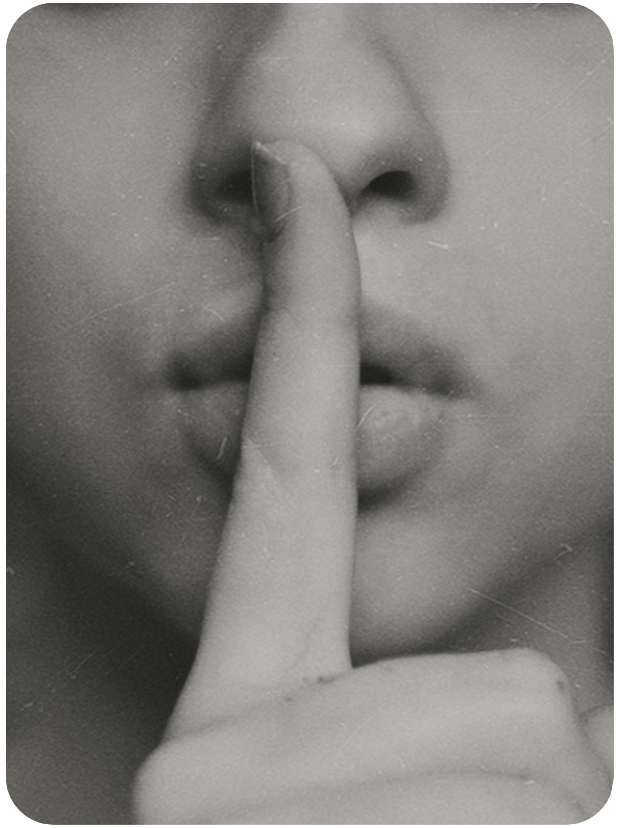
Harm to vulnerable groups

IIBA Dutch Chapter

BearingPoint®

As AI relies heavy on data, data security & intellectual property risk is present

3. AI & risk



Loss of trade secrets

Theft of personal information

Intellectual property claims

IIBA Dutch Chapter

BearingPoint

Organizations are increasingly dependent on third-party AI vendors

3. AI & risk

Vendor lock-in

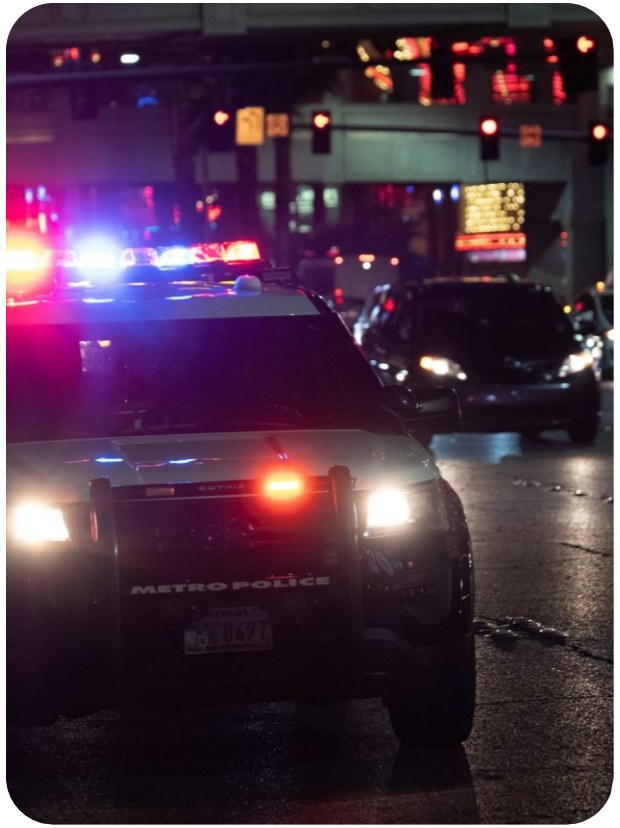
Liability claims

Supply chain risks

IIBA Dutch Chapter

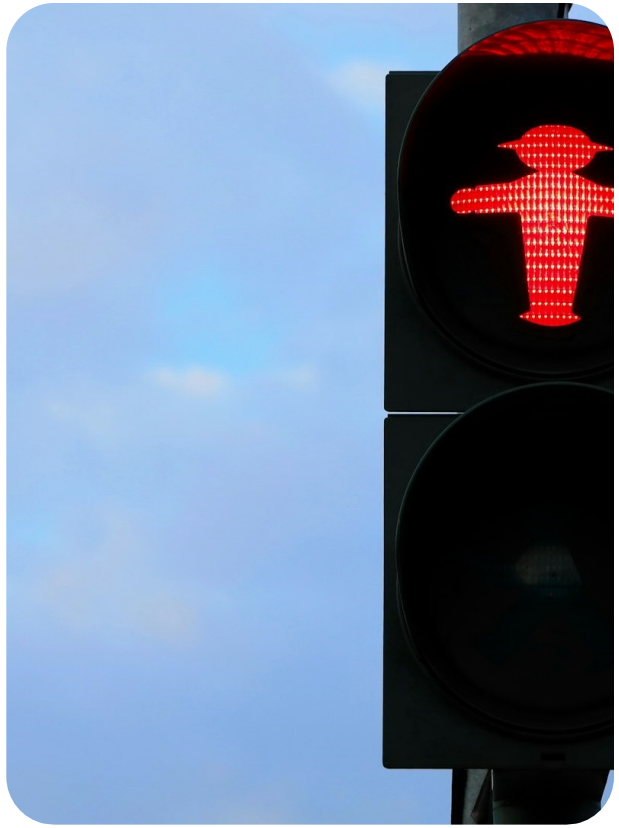
As AI technologies evolve, so do the regulatory landscapes that govern them

3. AI & risk

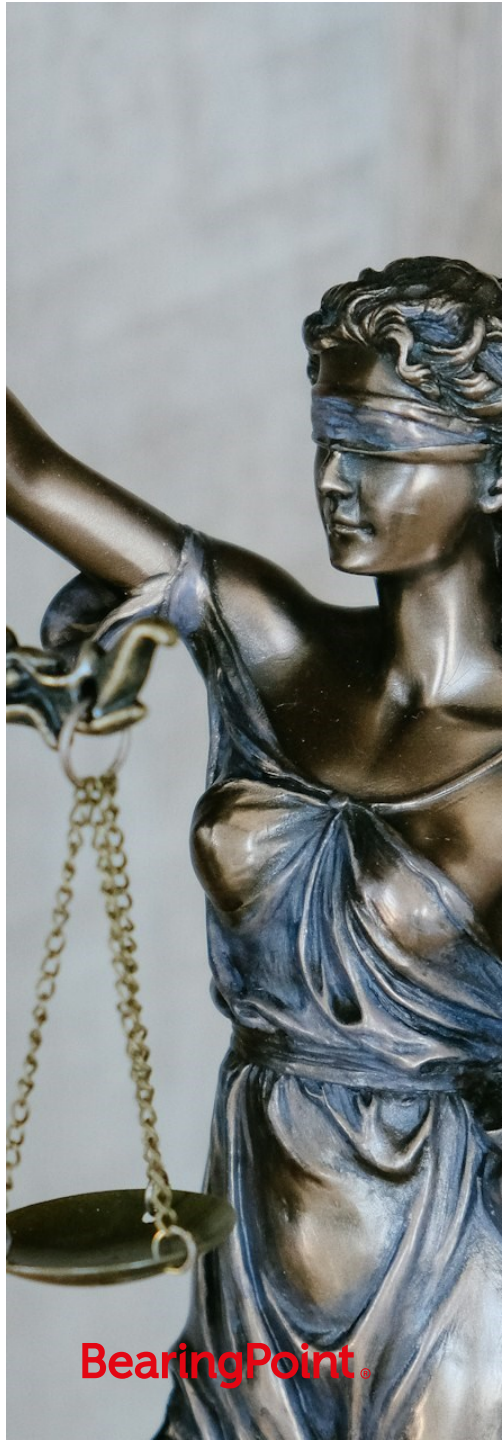


Fines

Reputation loss



Operational restrictions



IIBA Dutch Chapter

BearingPoint

What risk(s) is/are the primary concern for you/your organization?

Discuss the above question with your neighbors

15 minutes

IIBA Dutch Chapter

BearingPoint

4. Reducing AI risk by using best-practices

IIBA Dutch Chapter

BearingPoint

Ethical challenges

4. Reducing AI risk by using best-practices

Develop & implement ethical guidelines

Regular audits & monitoring

Training of employees

Promote human-centric AI design

IIBA Dutch Chapter

Accuracy & reliability of results

4. Reducing AI risk by using best-practices

Include human oversight & review

Test & validate rigorously

Use high-quality data

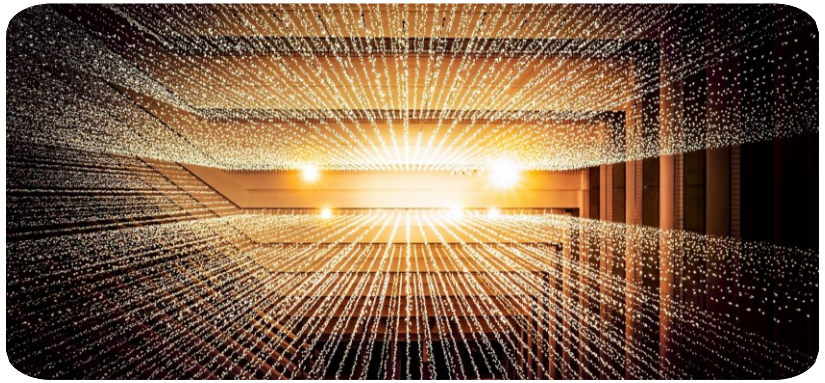
Maintain strict version control & documentation

IIBA Dutch Chapter

BearingPoint®

Biased results

4. Reducing AI risk by using best-practices



Training of models on diverse data sets

Preprocess data used in models

Regular bias & fairness testing

Select unbiased features during model development

IIBA Dutch Chapter

BearingPoint®

As AI relies heavy on data, data security & intellectual property risk is present

4. Reducing AI risk by using best-practices

Clarify data ownership

Create employee awareness

Use of synthetic data

Data minimization

IIBA Dutch Chapter

AI supply chain

4. Reducing AI risk by using best-practices

Vendor risk assessment & audits

Agree on contractual obligations

Agree on breach notification protocols

Engage in supply chain risk management

IIBA Dutch Chapter

With a changing legal landscape staying compliant can be a challenging task

4. Reducing AI risk by using best-practices

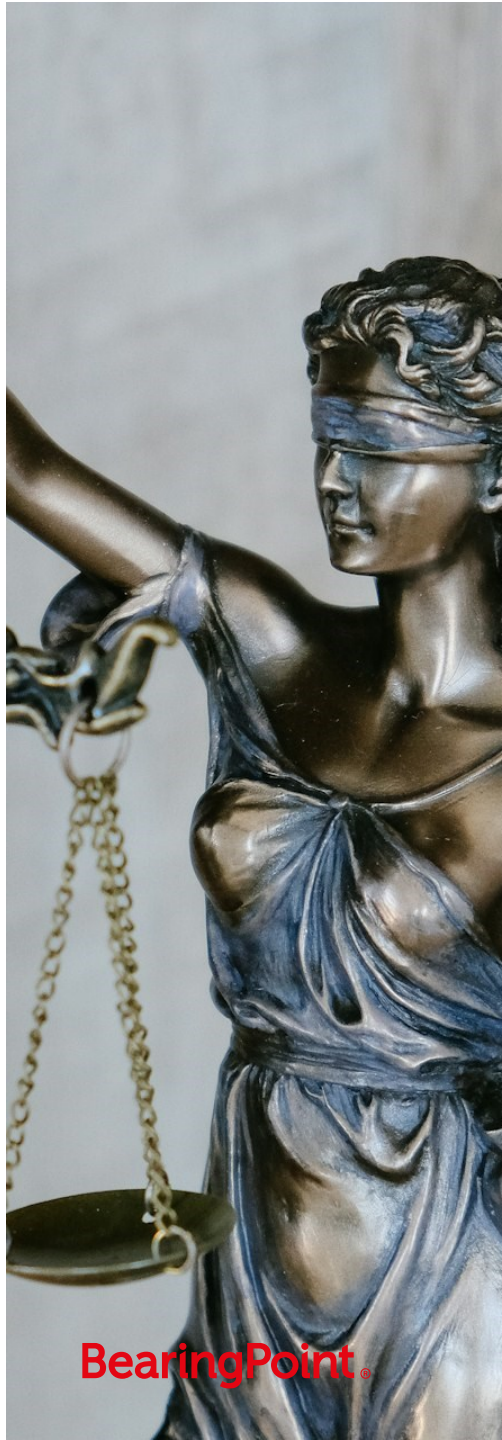
Consult with (third-party) experts

Communicate with regulators

Engage risk management departments

Develop compliance roadmaps

IIBA Dutch Chapter



Which best practice/practices will you use to reduce AI risks in your organization?

Discuss the above question with your neighbors

15 minutes

IIBA Dutch Chapter

BearingPoint

5. AI & regulation

IIBA Dutch Chapter

BearingPoint®

Worldwide regulations related to AI follow a variety of approaches

5. AI & regulation

China
Quick AI development under strict governmental control

United States
AI-regulation driven by innovation & economic growth

European Union
Regulation aimed at ethical & responsible use of AI-technology

IIBA Dutch Chapter

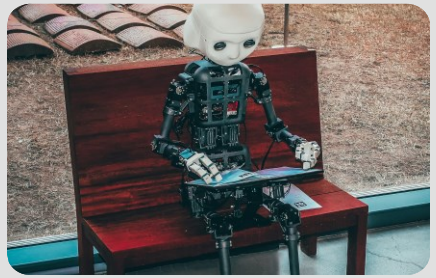
Want to know more about global AI regulation? You can find it here

BearingPoint

Looking at the Netherlands/Europe a number of laws are applicable in the field of AI[1]

5. AI & regulation

Application of AI



AI-Act

GDPR/AVG

AI & implementation

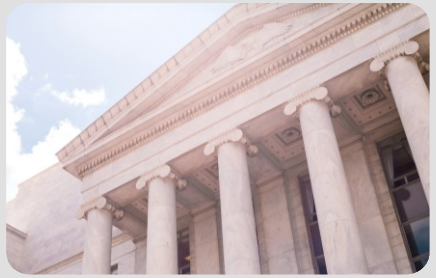
Digital Services Act (DSA)

Digital Markets Act (DMA)

AI & cyber security

NIS2

AI & the (Dutch) government



Wet Digitale Overheid

Wet politiegegevens (Wpg)

Wet op de inlichtingen- en veiligheidsdiensten (Wiv)

IIBA Dutch Chapter

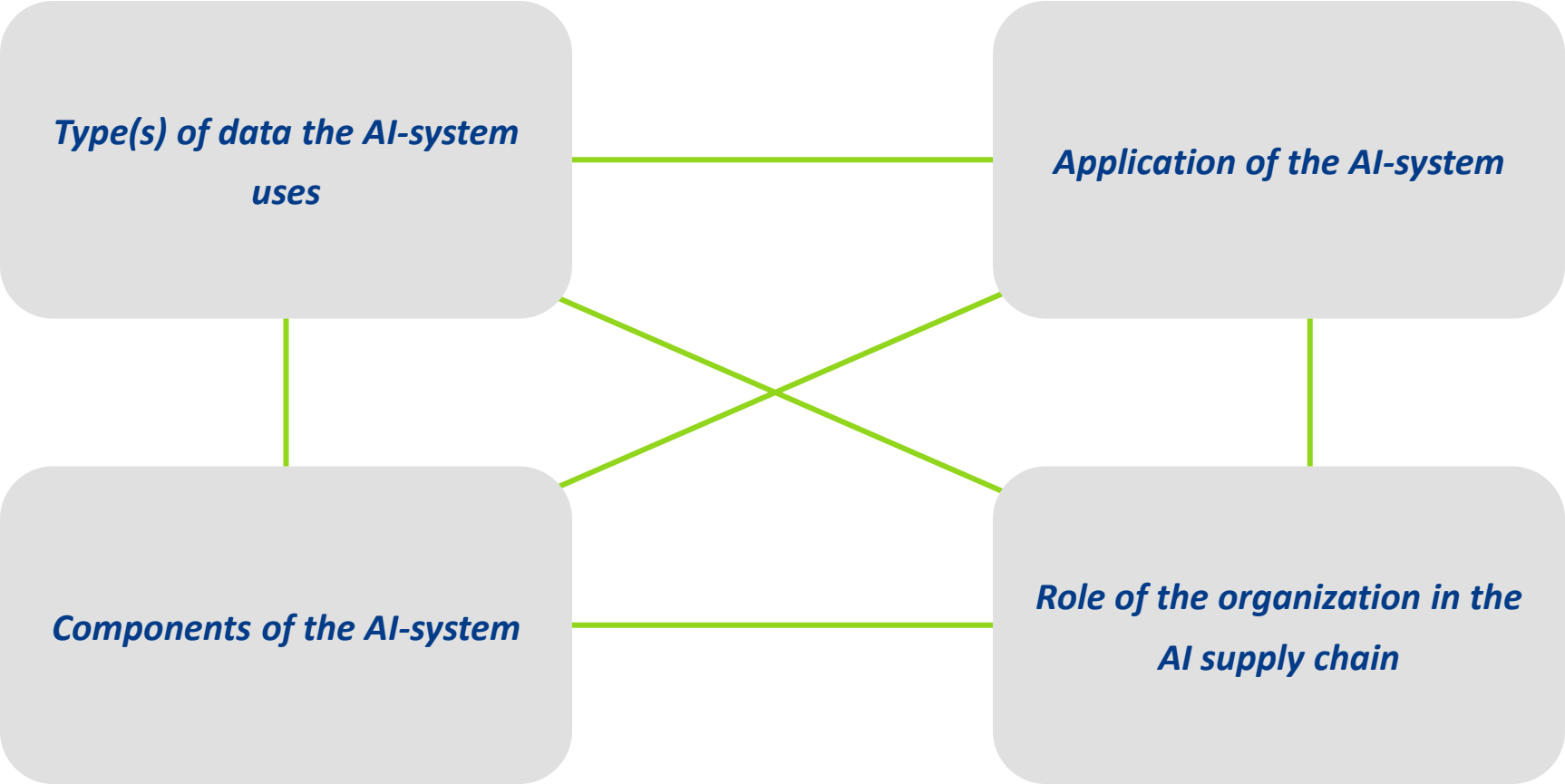
1. *Selection of most important laws in this field. Beside the laws mentioned here, other specific legislation can apply.*

Focus of today

BearingPoint®

Looking at the AI-Act & the GDPR/AVG, four aspects are important to consider when working to become compliant

5. AI & regulation



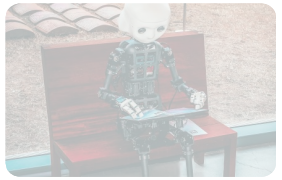
IIBA Dutch Chapter

BearingPoint®

The type of data the AI-system uses can trigger the need for safeguards

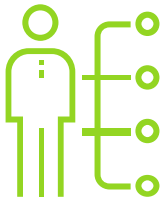
5. AI & regulation

Topic relevant to:



AI-Act

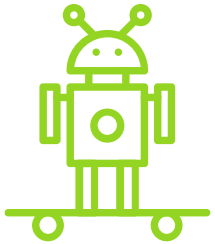
GDPR/AVG



Personal data

GDPR restrictions to data use apply

VS



Other data

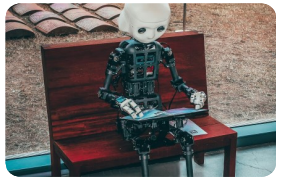
No limitations on use[1]

1. *Besides restrictions on use due to the GDPR, additional usage restrictions can apply (e.g., contractual limitations or limitations related to intellectual property laws).*

The different components of an AI-system are subject to different legislations

5. AI & regulation

Topic relevant to:



AI-Act

GDPR/AVG

Training data

When containing personal data, training data is considered personal data under GDPR and must be treated as such.

AI-model

GDPR not applicable
AI-Act applies and can limit model use depending on its risk categorisation (see next slide).

Input & outcome data

When containing personal data, input & outcome data is considered personal data under GDPR and must be treated as such.

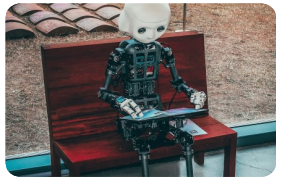
IIBA Dutch Chapter

BearingPoint.

The way in which an AI-system is applied determines the controls that need to be put in place

5. AI & regulation

Topic relevant to:



AI-Act

GDPR/AVG

AI Act Assessment criteria

- Intended purpose of the AI system
- Number of people affected by the AI system
- Complexity of the system
- Potential for harm

Risk levels emerging from the assessment:

- **Prohibited**
- **High-risk**
- **Limited-risk**
- **Minimal-risk**

Obligations for each **risk level:**

Prohibited:
Not allowed - Deletion of AI system

High-risk systems:
Draw up technical documentation
Conformity assessment
Quality management system
Automatically generated logs
Corrective actions
Duty of information
Cooperation with competent authorities

Limited-risk systems:
Light transparency obligations

Minimal risk:
No obligations

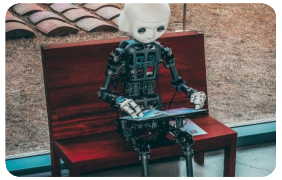
IIBA Dutch Chapter

BearingPoint

Depending on the role of an organization in relation to a high-risk AI-system, specific controls are needed

5. AI & regulation

Topic relevant to:



AI-Act

GDPR/AVG

Providers

- Ensure AI systems comply with regulatory requirements.
- Perform conformity assessments.
- Maintain technical documentation & implement risk management systems.
- Implement data governance measures.
- Register high-risk AI systems in the EU database.
- Monitor AI systems post-market.
- Report incidents or malfunctions.
- Ensure compliance when updating, modifying, or retraining AI systems.

Importers

- Ensure AI systems comply with EU regulations.
- Verify providers have completed conformity assessments.
- Maintain copies of conformity declarations.
- Cooperate with authorities on compliance issues.
- Ensure AI systems are correctly labeled and traceable.

Deployers

- Use AI systems in accordance with the provider's intended purpose.
- Monitor and report incidents or anomalies.
- Ensure AI systems are not used in ways that increase identified risks.
- Comply with transparency obligations.

Distributors

- Verify AI systems are CE-marked and properly labeled.
- Ensure AI systems comply with legal requirements.
- Keep records of AI system conformity documentation.
- Report non-compliance or safety concerns to the importer, provider, or relevant authorities.

IIBA Dutch Chapter

BearingPoint®

Bonus: how far is your organization to become AI-Act compliant?

Discuss the above question with your neighbors after the session

IIBA Dutch Chapter

BearingPoint®

6. Close & Q&A

IIBA Dutch Chapter

BearingPoint®

Key take-aways

6. Close & Q&A

Despite offering endless possibilities, AI also exposes you to risks.

AI is a broad term consisting of a wide range of tools and techniques.

Risks resulting from AI use can be reduced though the use of (a combination of) best practices.

Due to the complex legal landscape surrounding AI, becoming (and staying) compliant takes effort.

IIBA Dutch Chapter

BearingPoint®

To summarize…

6. Close & Q&A

1. Intro to AI
   - Whether you like it or not, AI is here to stay. Despite offering endless possibilities, AI also exposes you to risks.
2. What is AI?
   - AI is a broad term consisting of a wide range of tools and techniques. Sub-categories include traditional AI, ML, DL and Gen-AI.
3. AI & risk
   - Using AI exposes organization to specific risks related to, ethical use of AI, the accuracy & reliability of results, biased results, data security & intellectual property, supply chain risks and external compliance risks.
4. Reducing AI risk by using best-practices
   - Risks resulting from AI use can be reduced though the use of best practices.
   - Each risk category has specific best practices that best work when combined.
5. AI & regulation
   - Different parts of the world take different approaches to regulating AI.
   - In the EU/NL a wide spectrum of laws is applicable to AI. To become fully compliant, all these laws need to be considered.
   - Looking at the AI-Act & the GDPR/AVG, four aspects are important to consider when working to become compliant: the type(s) of data the AI-system uses, the components of the AI-system, the application of the AI-system and the role of the organization in the AI supply chain.

Questions

IIBA Dutch Chapter

BearingPoint

Want to know more

Joris Schut
Business Advisor Data & Analytics
+31(0) 6 22 55 82 69
joris.schut@bearingpoint.com
www.bearingpoint.com

Read more on this topic on our blog:
www.bearingpoint.com/en-nl/insights-events/blog

IIBA Dutch Chapter

BearingPoint

7. Appendix

IIBA Dutch Chapter

BearingPoint

Links to articles used in the presentation

7. Appendix

1. **Introduction - Impact**
   - Artificial Intelligence in the News: How AI Retools, Rationalizes, and Reshapes Journalism and the Public Arena (link)
   - AI Will Transform the Global Economy. Let's Make Sure It Benefits Humanity (link)
   - The Future of AI: How Artificial Intelligence Will Change the World (link)
   - The Impact of AI on Society and Everyday Life (link)
   - The 2024 Nobel prizes mark an important year for AI (link)
   - AI offers an intriguing new way to diagnose mental-health conditions (link)
   - Artificial intelligence and its impact on everyday life (link)

1. **Introduction - Risks**
   - Foreign Relations chair targeted in sophisticated deepfake operation (link)
   - Colorado Springs attorney says ChatGPT created fake cases he cited in court documents (link)
   - These lawyers used ChatGPT in court to safe time. They got fired and fined (link)
   - Fake news YouTube creators target Black celebrities with AI-generated misinformation (link)
   - Is Your Driving Being Secretly Scored? (link)
   - Israel deploys extensive facial recognition in Gaza to locate terrorists (link)
   - Microsoft accused of damaging Guardian's reputation with AI-generated poll (link)
   - Google apologizes for 'missing the mark' after Gemini generated racially diverse Nazis (link)
   - Feds Rein In Use of Predictive Software That Limits Care for Medicare Advantage Patients (link)
   - Google Stock Keeps Falling After Bard Ad Shows Inaccurate Answer, AI Race Heats Up (link)
   - Victorian MP Georgie Purcell criticises Nine News for 'sexist' image editing to make outfit more revealing (link)
   - Samsung Bans ChatGPT Among Employees After Sensitive Code Leak (link)
   - The world wants to regulate AI, but does not quite know how (link)

Links to articles used in the presentation

7. Appendix

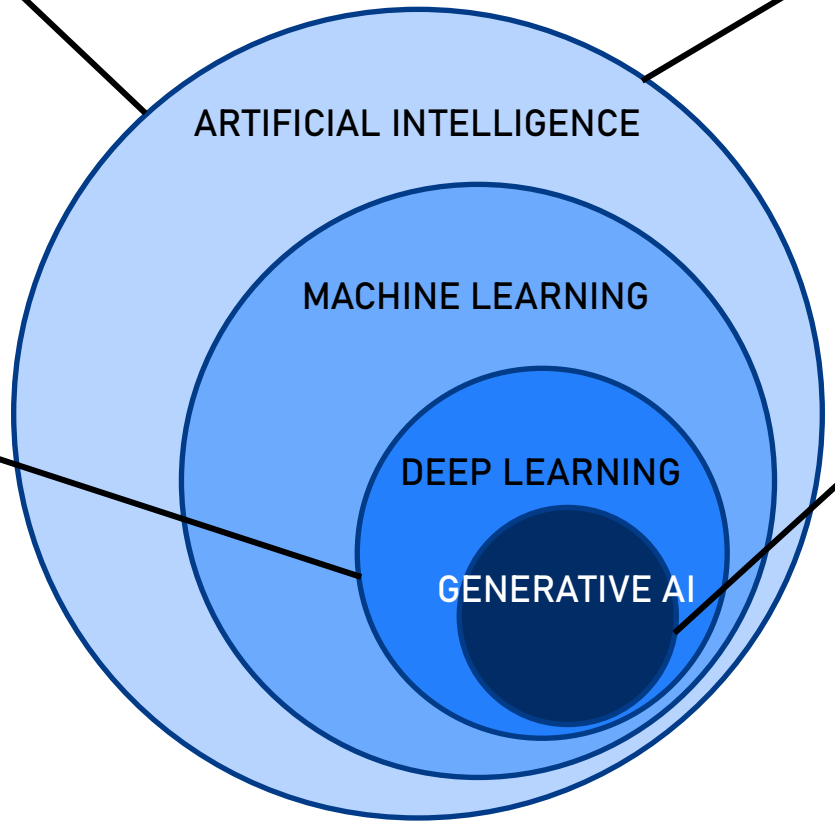
5. **AI & regulation**
   - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (link)
   - GDPR Reference Guide: All 99 Articles in 25 Minutes (link)
   - The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (link)
   - Artificial Intelligence Act (link)

IIBA Dutch Chapter

Exercise 1: How does your organization use AI? (5 minutes)

Task:

1. Identify where your organization uses AI
2. What type of AI is being used?
3. Who is involved in its use?



IIBA Dutch Chapter

BearingPoint®

Exercise 2: AI risks in your organization (15 minutes)

Task:

1. Identify the main risks your organization faces related to AI

Ethical use of AI

Accuracy & reliability of results

Biased results

Data security & intellectual property

Supply chain

External compliance

IIBA Dutch Chapter

BearingPoint®

Exercise 3: reducing AI risk in your organization (15 minutes)

Task:

1. For the risks identified in the previous exercise, pick one or more best practice to reduce this risk.

Risk: _____

_____

Best practice used: _____

_____

_____

_____

_____

Risk: _____

_____

Best practice used: _____

_____

_____

_____

_____

Risk: _____

_____

Best practice used: _____

_____

_____

_____

_____

Risk: _____

_____

Best practice used: _____

_____

_____

_____

_____

Risk: _____

_____

Best practice used: _____

_____

_____

_____

_____

Risk: _____

_____

Best practice used: _____

_____

_____

_____

_____

IIBA Dutch Chapter

BearingPoint®