ICONIC ADVISORY

Institute of Internal Auditors Thailand

SET

www.iconicadvisory.co.th

IA CLINIC 2/2026
AI กับงานตรวจสอบภายใน:
โอกาส ความเสี่ยง และ การควบคุมที่ IA ต้องรู้

ส่วนที่ 2: ความเสี่ยงและการควบคุม ในการใช้งานปัญญาประดิษฐ์
AI Risk and Control

รุจคุณ โตวนำชัย CISA, CRISC, CDPSE, AAIA

AI Consideration

ICONIC ADVISORY

WHAT DO WE NEED TO KNOW TO AUDIT AI?

AI Model

AI Governance

AI Data Governance

Bias and Fairness

Transparency and Explainability

AI Risk Management

AI Development

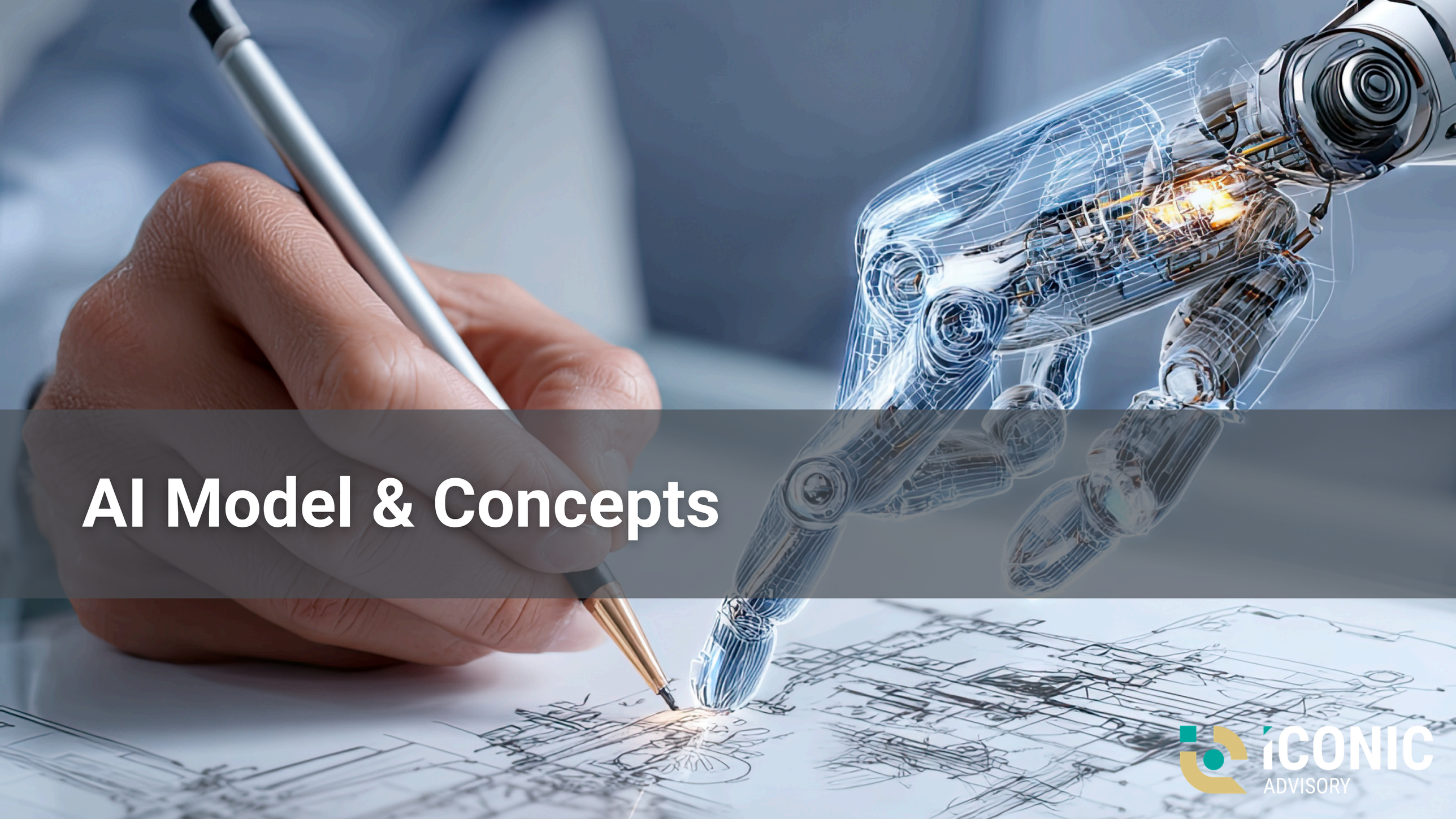
Regulation and Compliance

AI Operation

AI Threat and Vulnerabilities

HITL

ICONIC ADVISORY



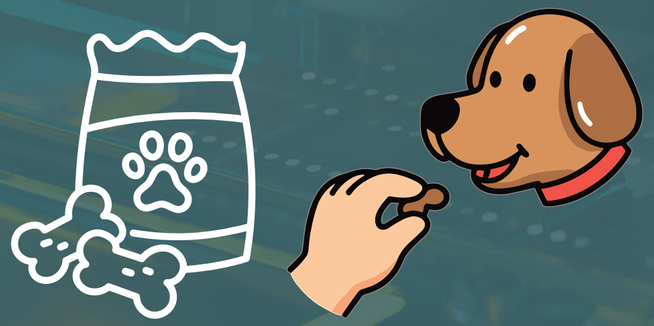
AI Model & Concepts

ICONIC ADVISORY

MACHINE LEARNING

Supervised Learning

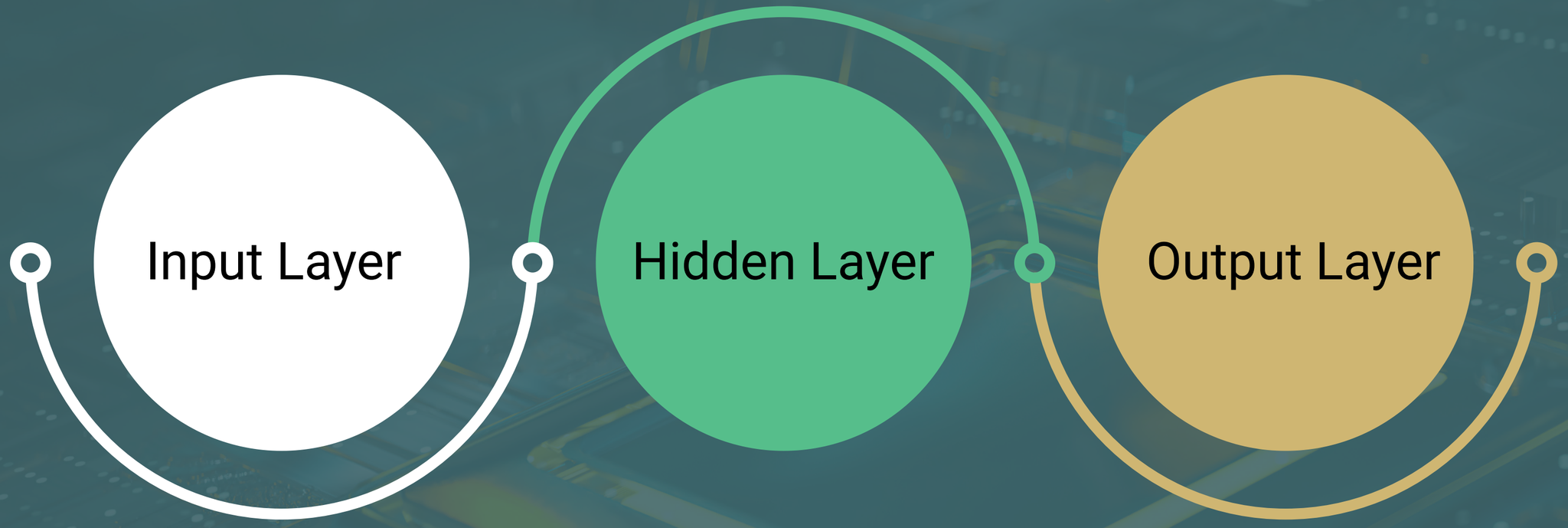
Unsupervised Learning



Reinforcement Learning

ICONIC ADVISORY

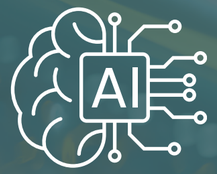
NEURAL NETWORK



Picture of Cats

Evaluate Patterns
(Similar to Human Brain)

It’s a Cat!!



ICONIC ADVISORY

AI VS. GEN AI

AI

Self-driving cars

Netflix recommending

Facial recognition

Forecasting sales trends

Car Park License Reader

X-Ray Reader

GEN AI

- Text Generation
- Image Generation
- Code Generation
- VDO/Clip Generation
- Music Composition

ICONIC ADVISORY

High Risk AI

ICONIC ADVISORY

HIGH RISK AI - FOR ENTERPRISE

1. AI impact to regulatory compliance
2. AI makes automated decision (without Human)
3. AI uses sensitive/personal Data
4. AI Impact to Ethical Consideration

- Car Driving AI
- Credit scoring AI
- Loan approval AI
- Medical Diagnosis AI
- Medical Device AI
- Job Applicant Screening AI
- Staff Promotion Recommendation AI
- Biometric AI

- Drafting E-mail AI
- Minute Taker AI
- Internal Knowledge Chatbot
- Internal Policies and Compliance Chatbot
- Training Course Suggestion AI
- Generate Market Image AI

ICONIC ADVISORY

Ethical Consideration

ICONIC ADVISORY

ETHICAL CONSIDERATION

Ethical Use (EIA)

Bias and Fairness

Human Rights (FRIA)

Transparency and Explainability

Trust and Safety

Environmental Impact

Intellectual Property Consideration

ICONIC ADVISORY

AI Governance

ICONIC ADVISORY

AI R&R AND GOVERNANCE

Strategy
Vision Mission
Value Alignment

Leadership and Committee
(EDM)

Training
Awareness
Talent Management

AI Policy

What is High vs. Low Risk AI?

Technical Team:

- AI Model Specialist
- AI Data Engineer
- AI trainer
- IT Team

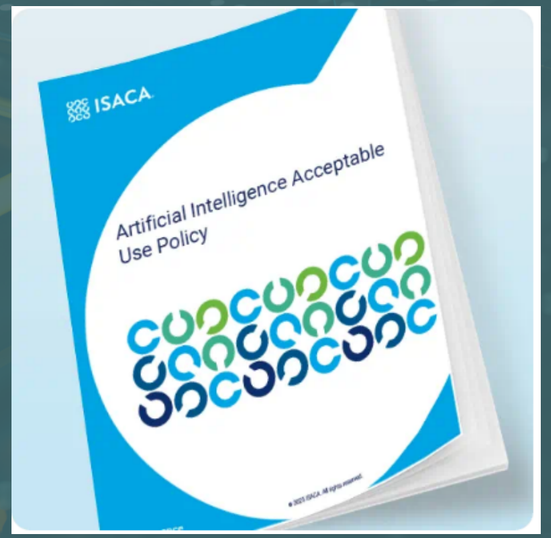
User

Governance and Oversight
2nd & 3rd Line

- Ethical and Compliance Specialist
- DPO
- IT Security
- AI Risk Specialist
- AI Auditor

AUP

AI Acceptable Use Policy

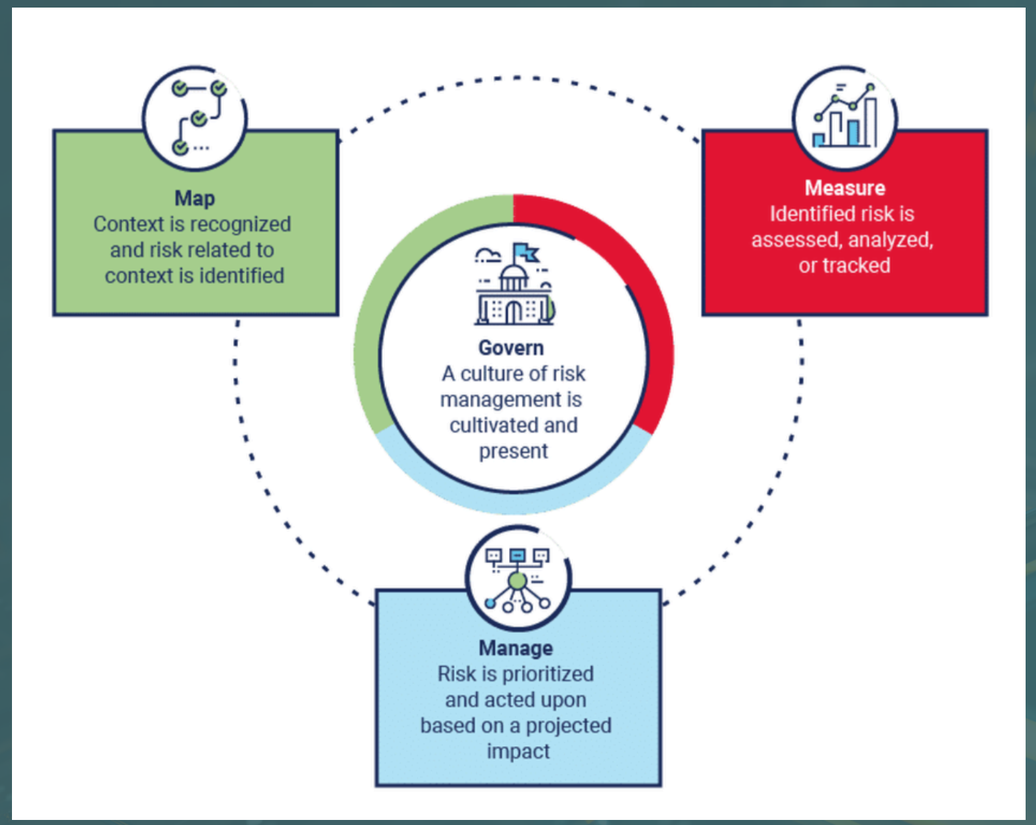


ICONIC ADVISORY

AI Risk Management

ICONIC ADVISORY

AI RMF AND PRACTICE



NIST AI RMF Core Functions
Source: US National Institute of Standards and Technology, NIST AI 100-1: Artificial Intelligence Risk Management Framework (AI RMF 1.0), USA, 2023, https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

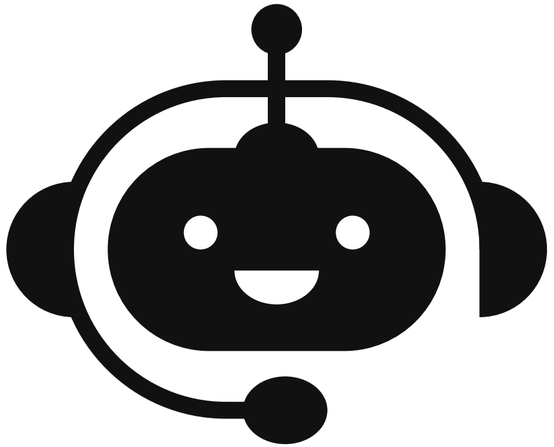
- Incorporated into organization's overall risk management
- Establish clear accountability and ownership
  - Example: Using AI for customer support
    - AI answer/support the client incorrectly? Who is the risk owner? AI dev, CS, Data scientist, (multiple owner?)

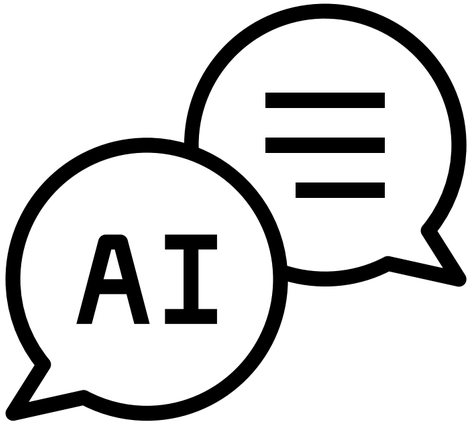
ICONIC ADVISORY

EXAMPLE OF KRI FOR CHATBOT

- Customer satisfaction score
- Incorrect response rate
- Misunderstanding rate
- Escalation rate

Automate KRI monitoring.





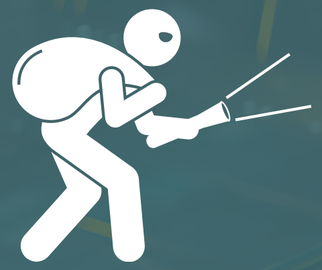
ICONIC ADVISORY

AI Threat and Vulnerabilities

ICONIC ADVISORY

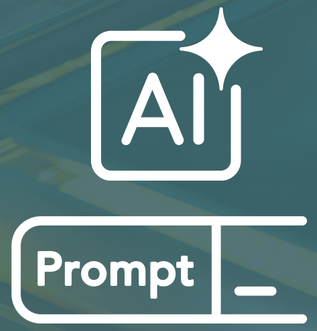
AI THREAT

Training Data Leakage



Model Theft

Model/Data Poisoning



Prompt Injection

Controls:

- Prompt Templates
- Access control
- Adversarial Testing
- Regularized

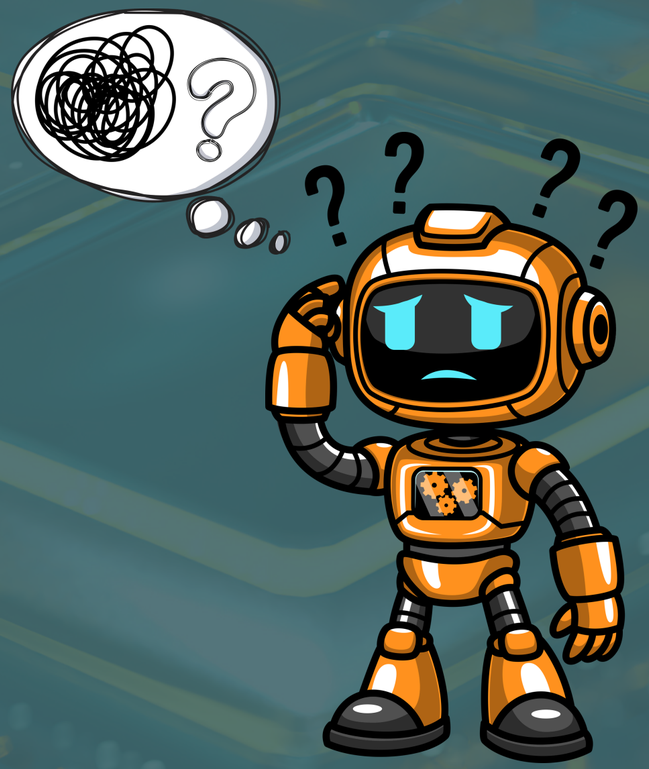
ICONIC ADVISORY

WHAT IS HALLUCINATION? HOW TO MITIGATE?

Hallucination = AI provides false or nonsensical information.

Reasons:

- Poor Training Data
- Lack of real-world data
- Ambiguity Input Data



ICONIC ADVISORY

AI Data Governance
Data Privacy

ICONIC ADVISORY

QUESTION?

AI Chatbot - who is the **data owner** of the chatlog?

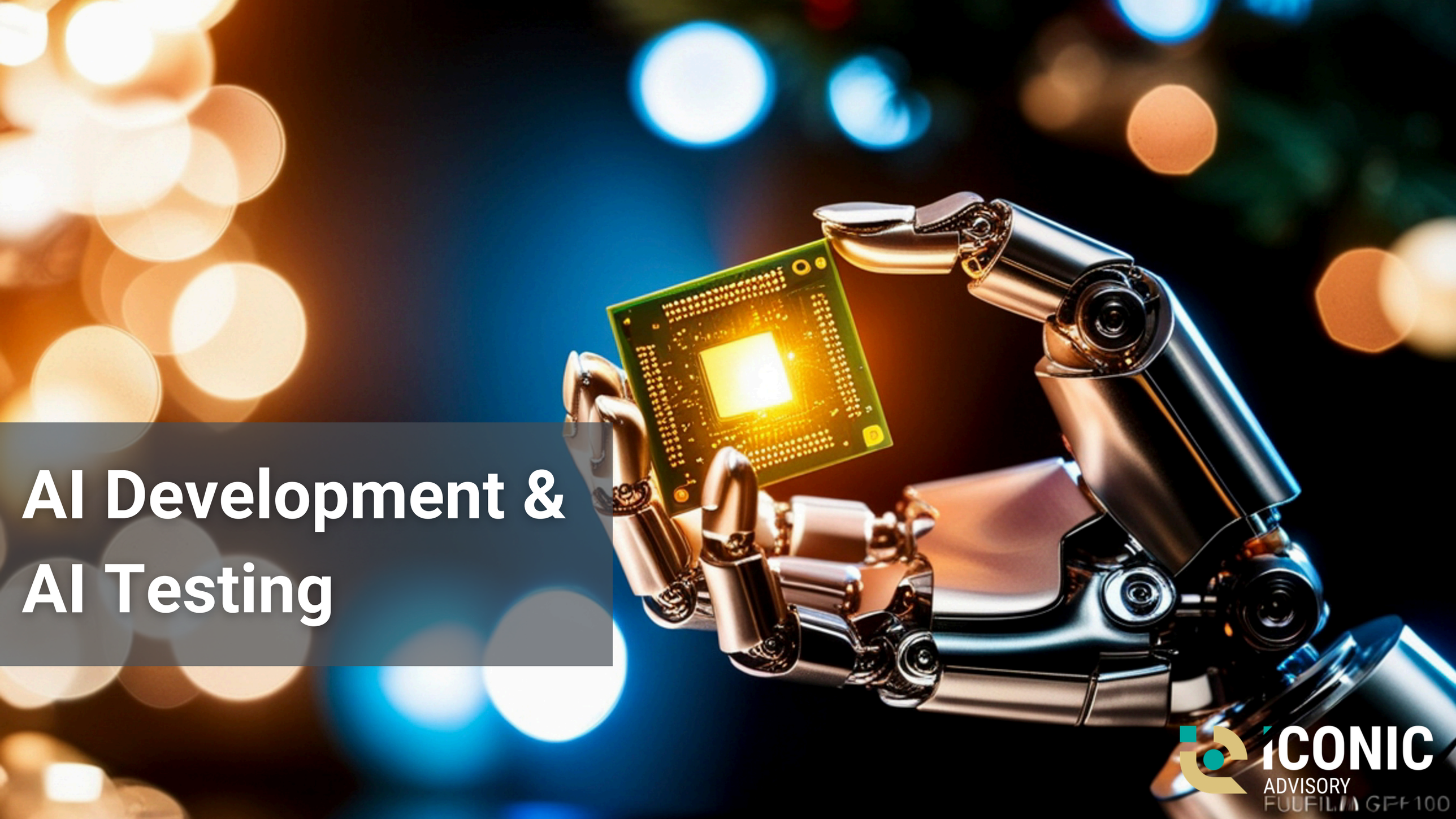
ICONIC ADVISORY

DATA GOVERNANCE

- AI Solutions, does not remove Ownership from employee
- Data Inventory → Training Data
- Data Classification (CIA+P)
  - Data Classification AI - Automated tool
  - AI Data Classification - e.g. Training data, PII, Sensitive, should be labeled clearly
- Data Consent
- Data Licensing
- Other Data Gov - Retention, Data Quality

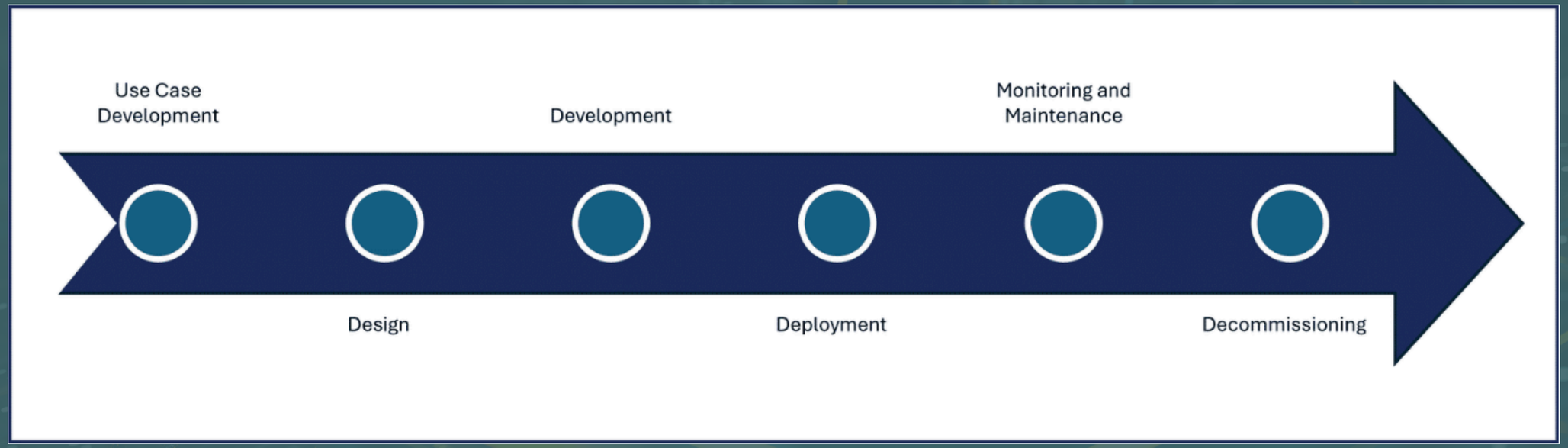
ICONIC ADVISORY

AI Development & AI Testing



ICONIC ADVISORY
FULFILLING GFF100

AI SOLUTION DEVELOPMENT



ref: ISACA AAIA Official Review Manual

- Secure by design
- Privacy by design

ICONIC ADVISORY

CONVENTIONAL SOFTWARE TESTING FOR AI

A/B Testing

Unit and Integration Testing

Code Review

Black Box Testing

ICONIC ADVISORY

AI SPECIFIC TESTING

Bias Testing

Adversarial Testing

ICONIC ADVISORY

AI Operation

ICONIC ADVISORY

SUPERVISE AI

Some AI has ability to act independently and make decision

- Logging and Monitoring
- Human in the Loop (HITL)

ICONIC ADVISORY

LOGGING AND MONITORING

Challenges:

- Nano decisions
- Review log manually is impractical

Ans: Log Balancing

Audit Trails (Example):

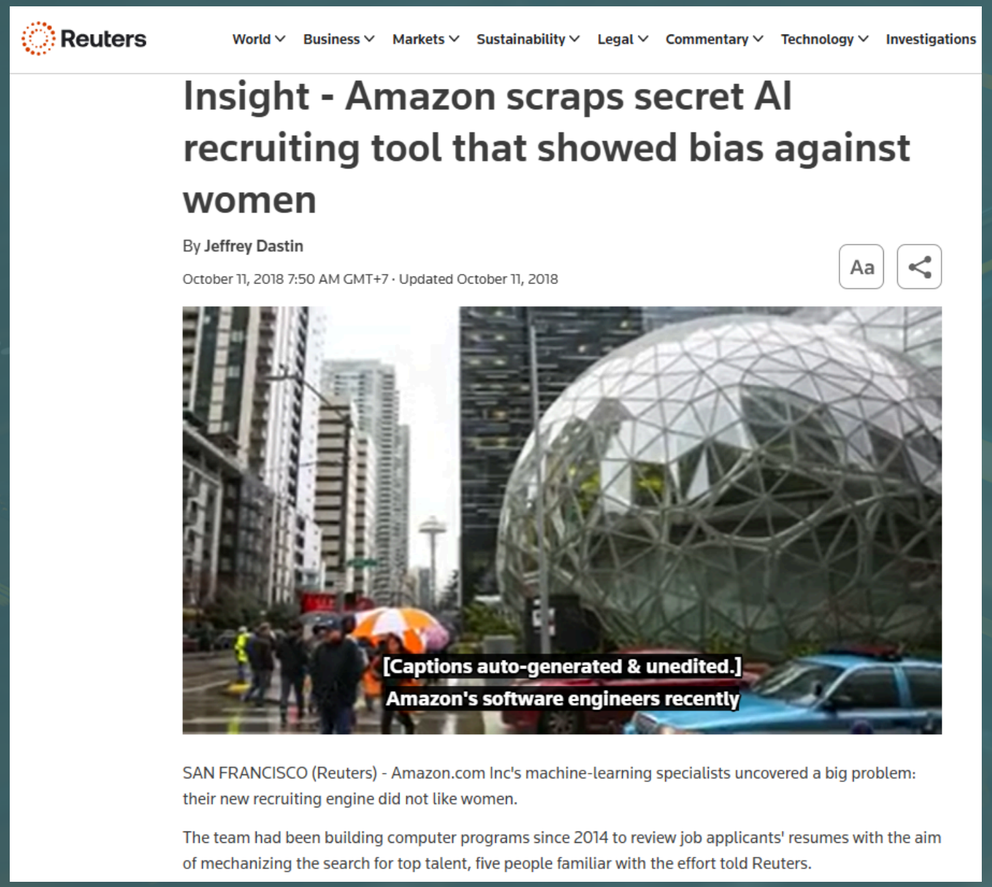
- Data inputs

- Model parameters and versions
- Data outputs

ICONIC ADVISORY

HUMAN IN THE LOOP (HITL)

- Auditor use AI to write report
- Amazon developed an AI hiring tool that showed bias against women



Reuters

World Business Markets Sustainability Legal Commentary Technology Investigations

Insight - Amazon scraps secret AI recruiting tool that showed bias against women

By Jeffrey Dastin

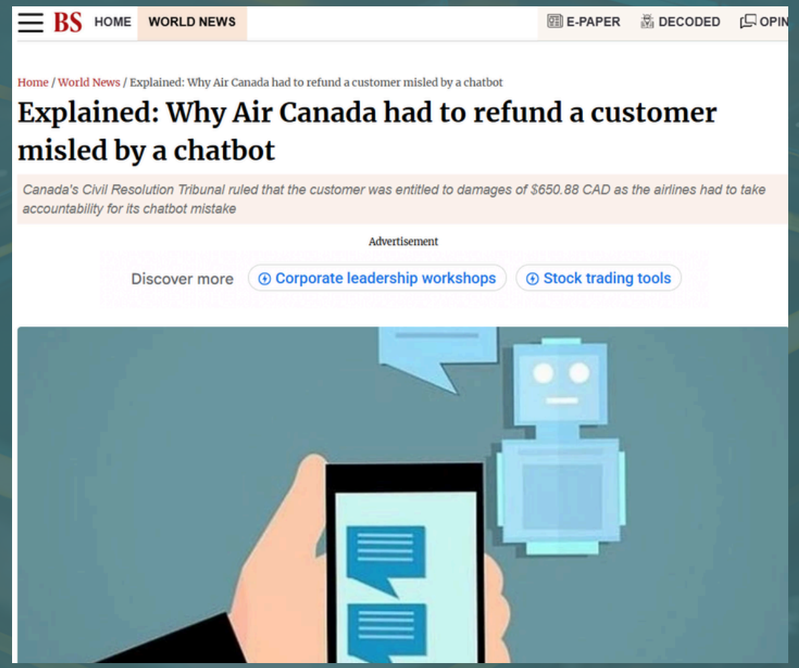
October 11, 2018 7:50 AM GMT+7 · Updated October 11, 2018

Aa

[Captions auto-generated & unedited.]
Amazon's software engineers recently

SAN FRANCISCO (Reuters) - Amazon.com Inc's machine-learning specialists uncovered a big problem: their new recruiting engine did not like women.

The team had been building computer programs since 2014 to review job applicants' resumes with the aim of mechanizing the search for top talent, five people familiar with the effort told Reuters.



BS HOME WORLD NEWS E-PAPER DECODED OPIN

Home / World News / Explained: Why Air Canada had to refund a customer misled by a chatbot

Explained: Why Air Canada had to refund a customer misled by a chatbot

Canada's Civil Resolution Tribunal ruled that the customer was entitled to damages of $650.88 CAD as the airlines had to take accountability for its chatbot mistake

Advertisement

Discover more Corporate leadership workshops Stock trading tools

ICONIC ADVISORY

Auditing AI (1st Step)

ICONIC ADVISORY

AUDITING AI - STARTING POINT

1. Identified High Risk AI
2. AI Policy
3. AI AUP
4. AI Inventory
5. AI Risk Management & Control
6. AI Governance Board
7. AI Awareness and Training

ICONIC ADVISORY

AUDITING AI CONTROL (AUDIT PROGRAM)

1. AI Governance
2. Technical Security and Privacy
3. AI Solution Development
4. AI Operation Management
5. Model Assessment
6. Ethical Assessment
7. Bias and Fairness Assessment
8. Transparency and Explainability
9. HITL
10. Compliance Assessment

ICONIC ADVISORY

ICONIC ADVISORY

Contact Us

+66 2 231 8488 (Direct line)

+66 82 459 0459

roujkun@iconicadvisory.co.th

www.iconicadvisory.co.th

92 Central Park Offices, Room No. 3521, Level 35
Rama IV Road, Silom, Bangrak, Bangkok 10500