

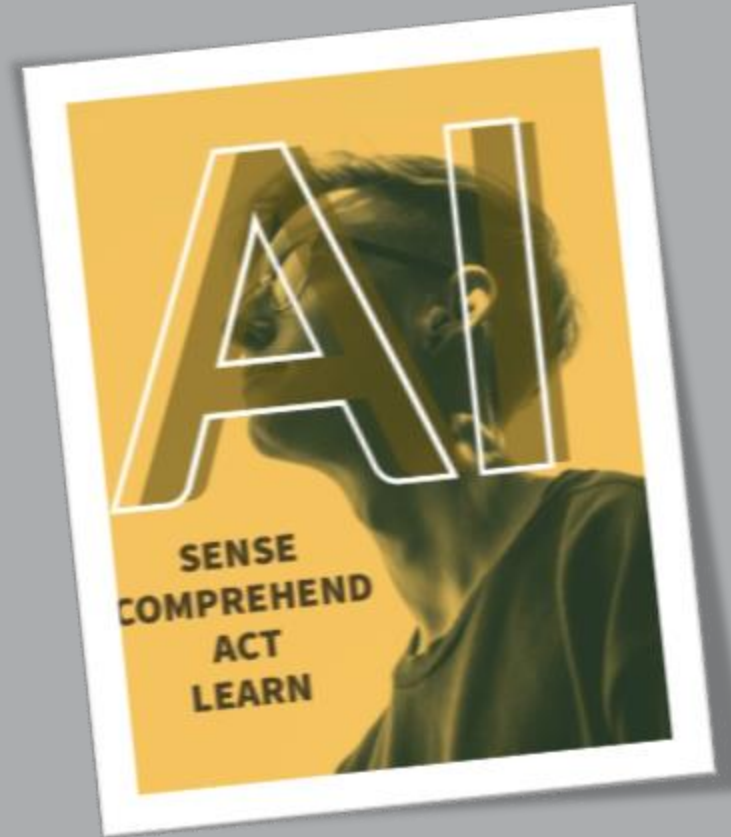
# Artificial Intelligence

**and AI Governance**

---

**Tony Arthur**

twitter: @iamtonyarthur



# who.am.i

## **Tony Arthur**

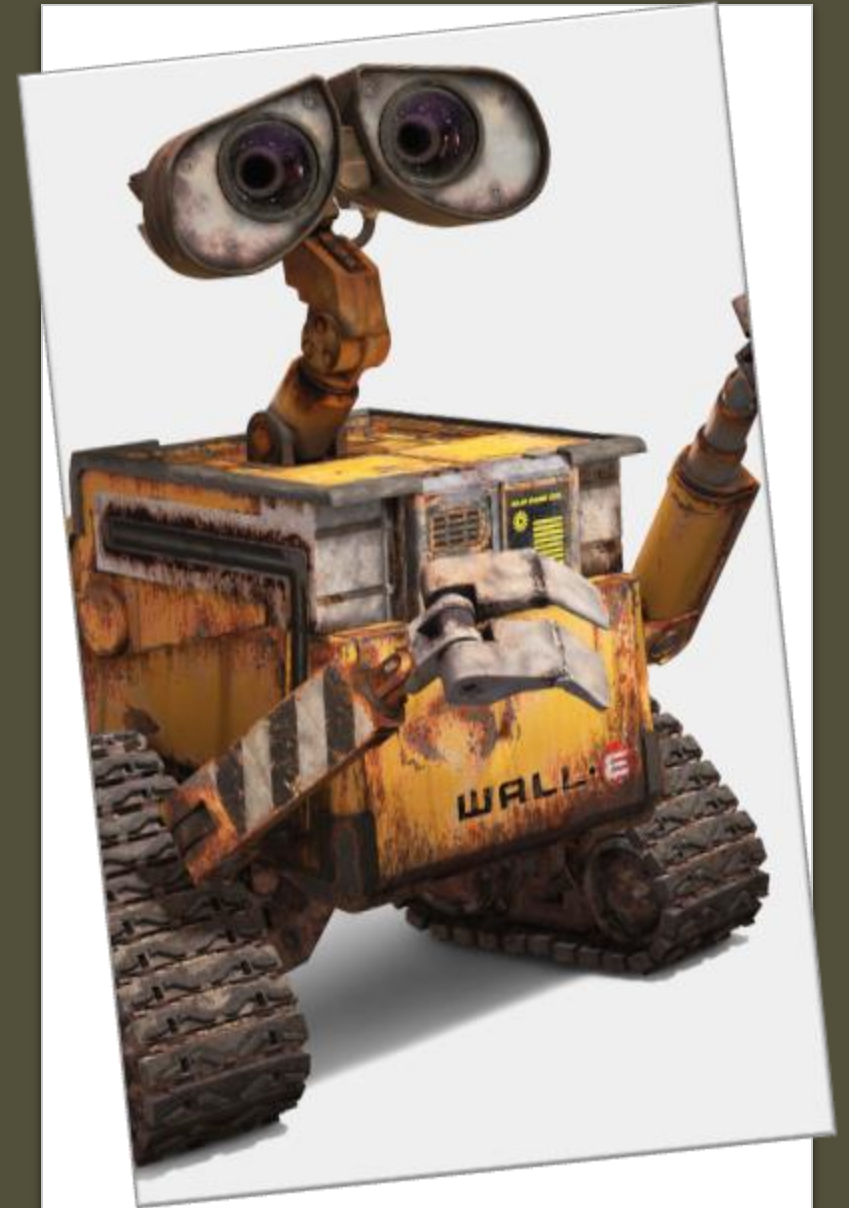
Cybersecurity Director @ Canadian Pacific

Founded a cybersecurity startup

Former Management Consultant @ PwC

Passionate about solving problems using technology

Curious, love to learn, and share ideas

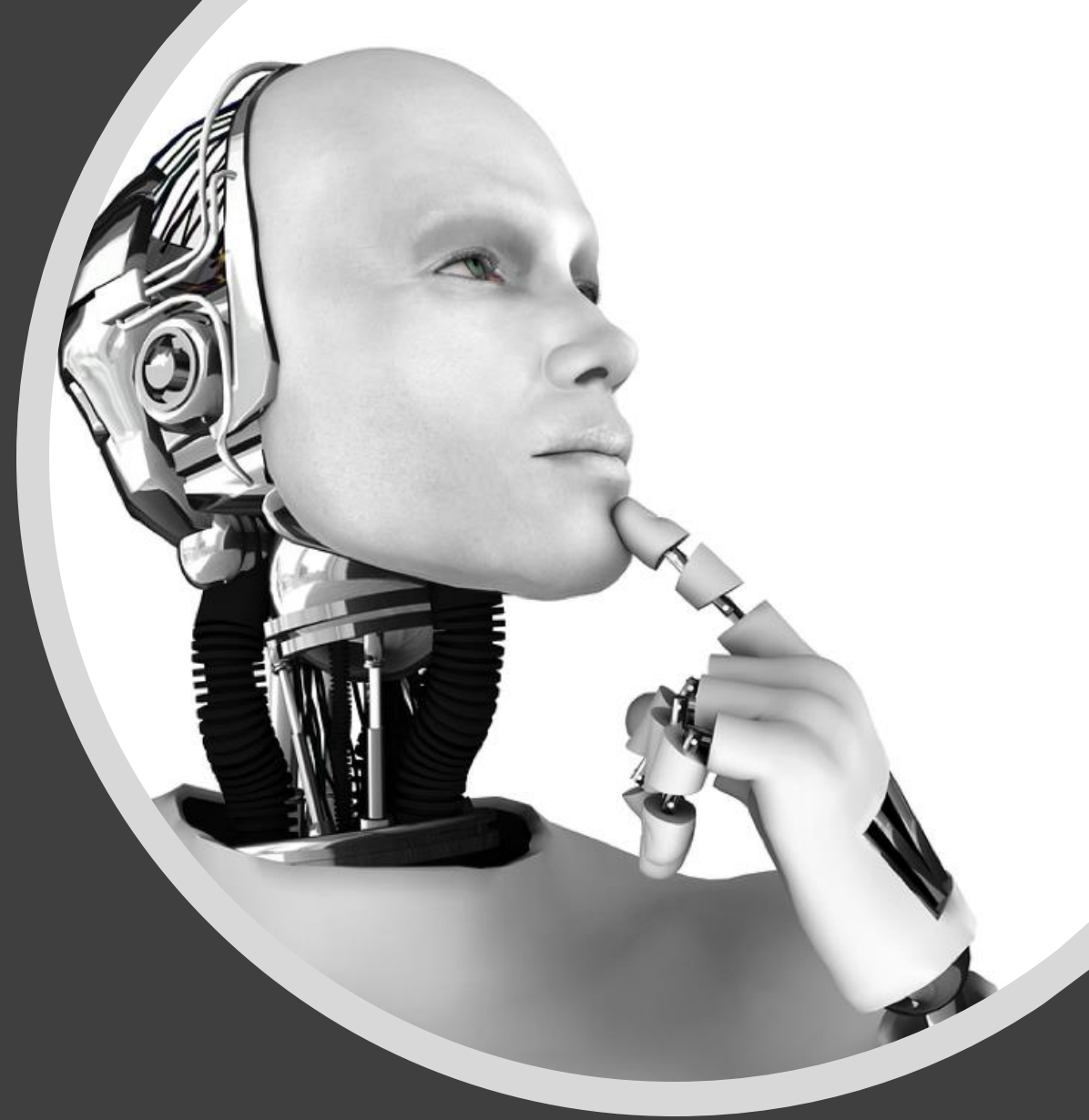



AI is a tool. The choice about how it  
gets deployed is ours.

- *Oren Etzioni*

# What is Artificial Intelligence (AI)?

- Intelligence demonstrated by machines so that machines can work and react like humans
- Sometimes called "Machine Intelligence"
- Types of AI: Machine Learning, Neural Networks, Deep Learning





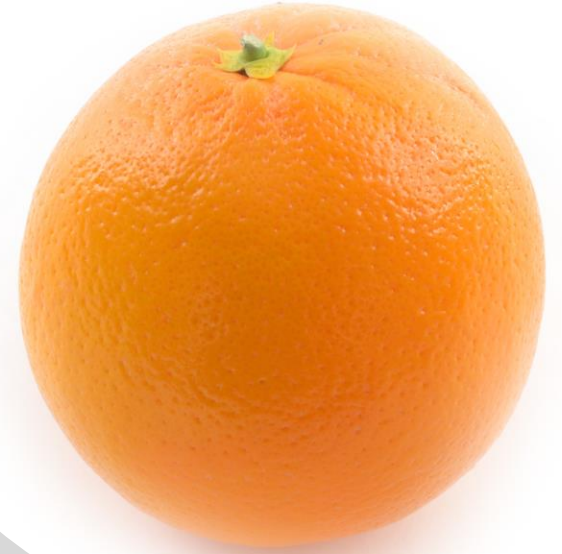
# What is Machine Learning (ML)?

- **Use** of algorithms and statistical models to perform tasks without using explicit instructions
- Subset of "Artificial Intelligence"
- Most successful form of AI so far
- Making machines smarter by learning from example and experience

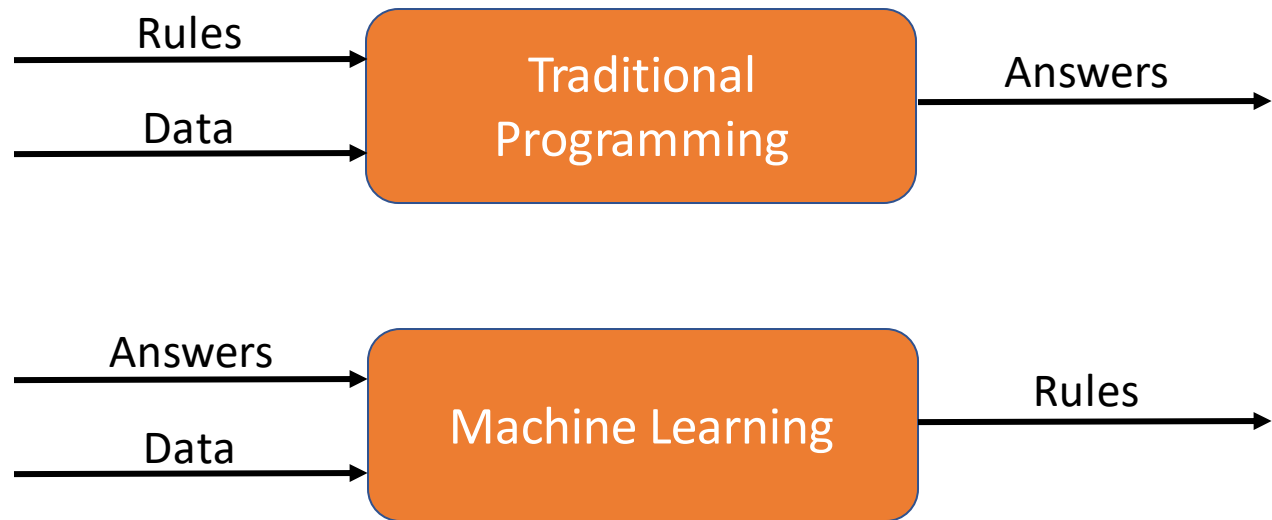


# Telling an apple from an orange without AI/ML

- Requires many rules using traditional programming methods
- Needs lots of coding to implement rules
- Maybe count ratio of orange and green colored pixels
- What happens if image is in black & white?
- Ultimately not scalable – and that's just apples and oranges



# Traditional Programming vs. Machine Learning





## **Supervised learning**

Builds a mathematical model of a set of data that contains both the inputs and the desired outputs



## **Unsupervised learning**

Takes a set of data that contains only inputs, and it has to detect pattern and relationship on its own



## **Reinforcement learning**

Interacts with the dynamic environment and gets feedback in terms of rewards or errors (punishments)

# Types of Machine Learning



Why talk about AI?

---

Organizations are thinking about how  
AI can play a role in their business.



GREATER AGILITY



BETTER CUSTOMER  
EXPERIENCE



COST SAVINGS



GROW REVENUE

Why are businesses considering AI?



## AI Use Case

A very exciting example of an AI use case is **autonomous driving**.

A grayscale photograph of a robotic hand with multiple joints and sensors, positioned over a curved, ergonomic keyboard. The hand is in the process of typing. The background is dark and out of focus.

# AI Use Cases

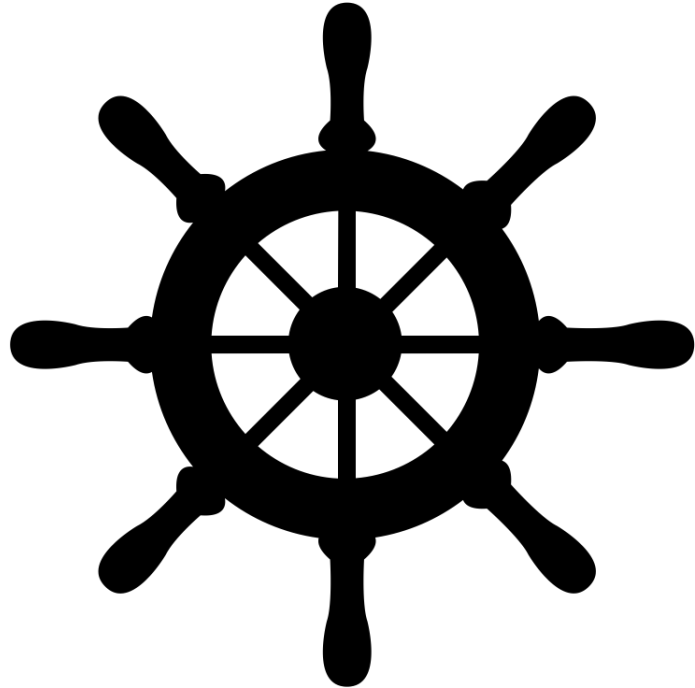
---

- Automated warehousing
- Chatbots
- Computer assisted diagnostics
- Fraud analysis on transaction data
- Market segmentation
- Process optimization tools
- Sentiment analysis

Do we need to govern AI?

---

Yes. AI has risks that needs to be managed.



## Examples of AI risk

- Lack of alignment between IT plans and business needs
- Improper translation of IT tactical plans from the IT strategic plans
- Ineffective governance that fails to ensure accountability and responsibility for IT processes related to AI
- Unidentified human bias can negatively affect AI-based decision making
- Inadequate oversight of AI results in ethically questionable results

# Challenges with governing AI

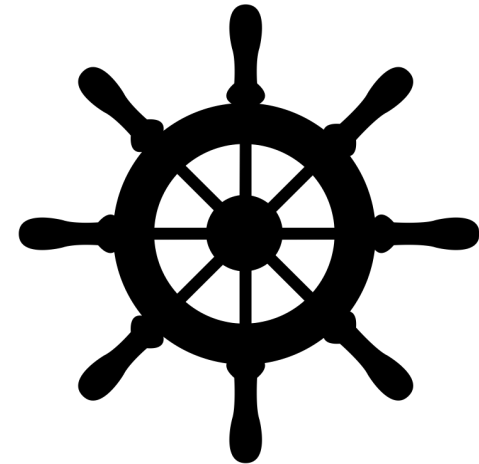
---

- No mature framework for auditing / governing AI or its subprocesses
- No AI-specific regulations, standards or mandates
- Complexity of AI
- Black-box effect of AI
- Many organizations are not yet thinking of AI's role in their business



# So what can we do?

- Do not overthink challenges of AI
- Leverage COBIT 2019 as a starting point
- Define scope and objectives of the audit
- Consider organization risk related to the AI initiative
- Compile areas of risk in a risk and control matrix



# Governance of AI



ETHICAL



LEGAL

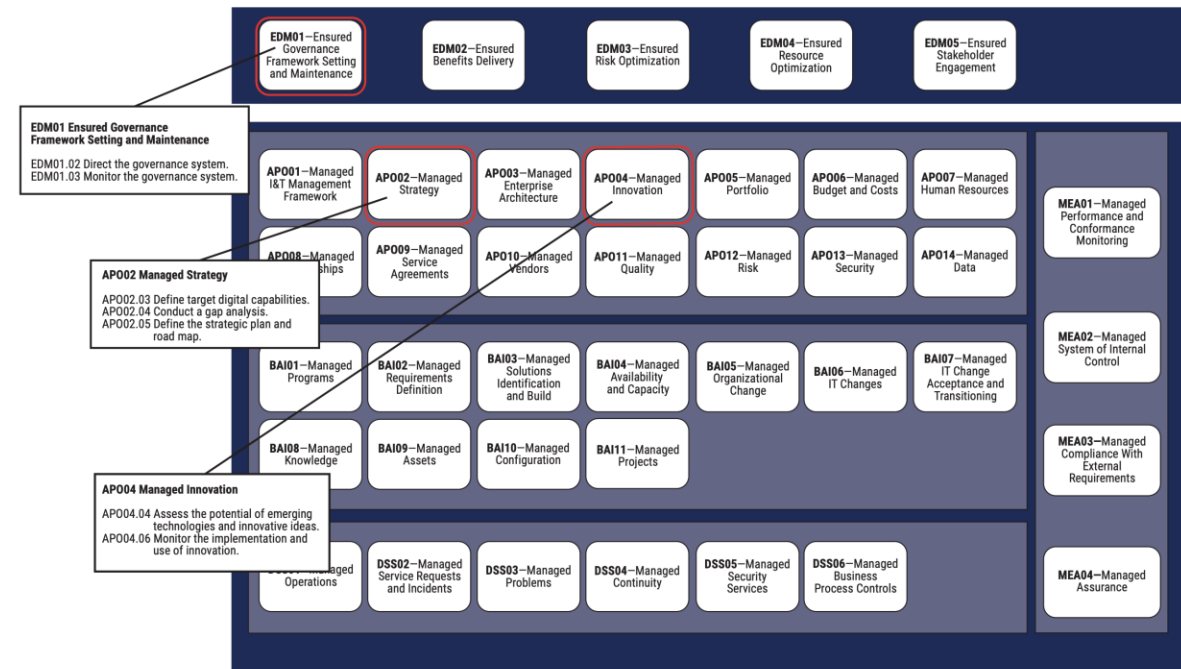


PRIVACY



SECURITY

# COBIT 2019 Governance and Management Objectives Relevant to AI Risk and Control Review



Source: ISACA, COBIT® 2019 Framework: Introduction and Methodology, USA, 2018

## Example of an AI control

### Summarized Risk

- Misalignment to the organization's cultural and ethical values

### AI Risk Description

- Decisions made by AI solution are not aligned to the organization's cultural and ethical values, or cause bad or incorrect decisions by a human employee / AI solution, resulting in the organization being held accountable.

### AI Control Description

- Ethical rules and corporate values are coded into the algorithms, and controls are in place to review the output. Changes to the ethical value code go through robust change management process.

### Control Subject

- 02 – Governance

### COBIT Process

- MEA02 Monitor, Evaluate and Assess the System of Internal Control

### COBIT Area

- Monitor, Evaluate and Assess

# Responsible AI Practices

<https://ai.google/education/responsible-ai-practices>



Use a human-centered design approach



Identify metrics to assess training and monitoring



Understand limitations of your dataset and model



Test, test, test



Continue to monitor and update the system after deployment

A grayscale photograph of a robotic hand with multiple joints and fingers, positioned over a computer keyboard. The hand is in the process of typing. The image is used as a background for a presentation slide.

# Key Takeaways

---

- AI is real – it is here and it is our future
- AI needs governance and controls
- No AI-specific framework exists – but in the interim we can leverage some existing frameworks
- Governance of AI should be aligned with business strategy, objectives and needs
- We need to understand AI so we can put in place proper governance and controls



# **AI is here.**

Huge implications for business