LEONARDO

Electronics

Helicopters

Aircraft

Cyber & Security

Space

Aerostructures

Leonardo Cyber & Security Solutions

AI and its Assurance

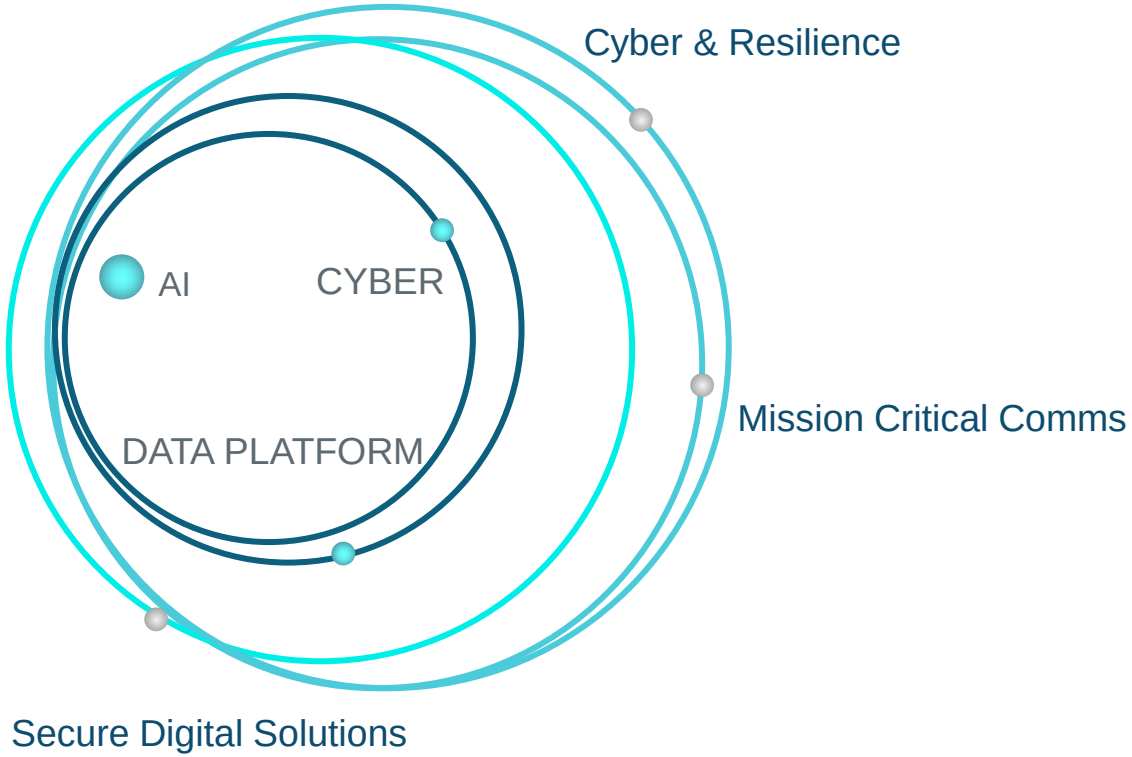
Building blocks for a sustainable AI Journey

BAPCO

November 2024

Cyber & Security Solutions Division

Paving a cyber secure, trustworthy and sustainable digital future



Products & Services

Cyber Security & Resilience

An ecosystem of products and services to deliver the cybersecurity and cyber resilience of strategic IT/OT assets in the most challenging security environments

Secure Digital Solutions

Data exploitation and Secure Cloud platforms for the development of digital infrastructures and services. We are trusted to support some of the most sensitive UK digital missions.

Mission Critical Communications

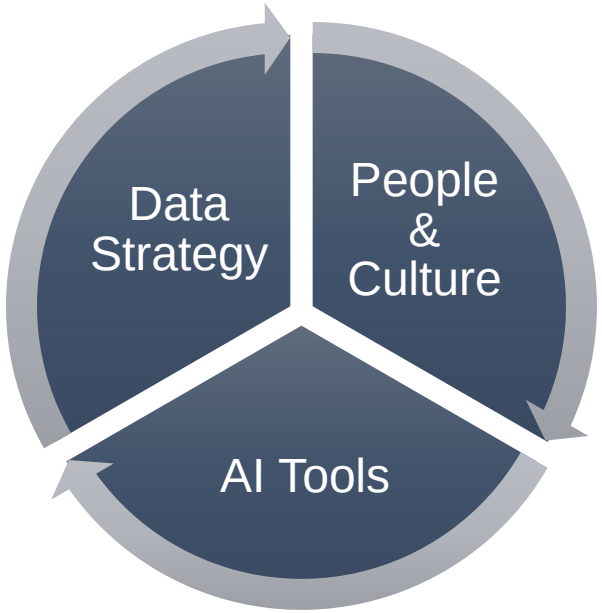
Systems for next-generation operations of mission critical services

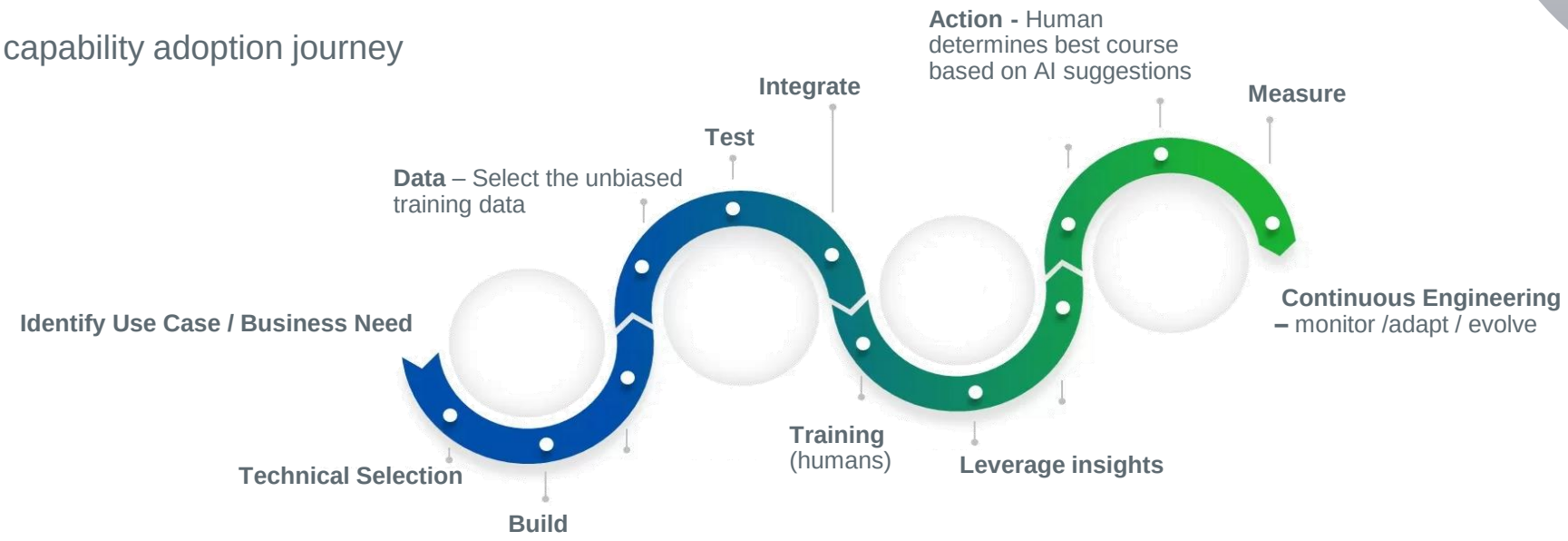
[TECHNOLOGICAL ANCHORS] ARTIFICIAL INTELLIGENCE CYBER DATA PLATFORM

The Journey to AI

Scaling AI to achieve long-term success

- Integration of AI technology is not just about ensuring the technology is trusted and secure
  - To ensure AI is adopted broadly,
    - processes in place to procure and govern solutions,
    - unbiased, catalogued data, stored securely
    - and the people who are ready to nurture and develop AI capabilities
- Underlying fundamentals are critical to leveraging AI
  - Three key foundations
- AI capability adoption journey

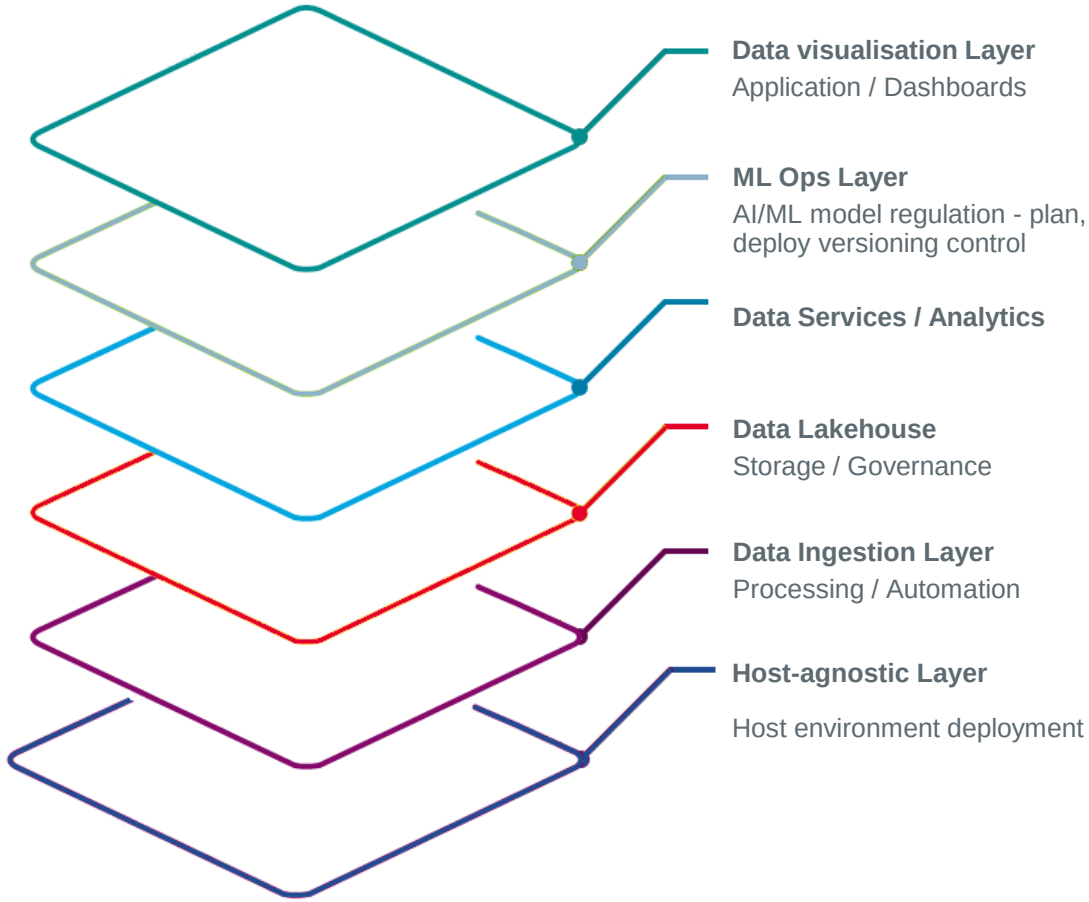




AI Enablers

Secure Data Platforms

- Need to have trust in the data
  - Clear, current and correct
- Centralise and manage data,
  - enabling efficient processing and analysis
  - generate actionable insights and power digital services
- An integrated set of technologies that collectively meet an organisation's end-to-end data needs
  - Framework that helps collect and use data consistently to support real-time decision-making and strategic planning
  - Cloud native, highly scalable, structured metadata, support for ACID transactions and modular (easy to change smaller components).



AI Use Cases Emergency Services

Digital Assistants

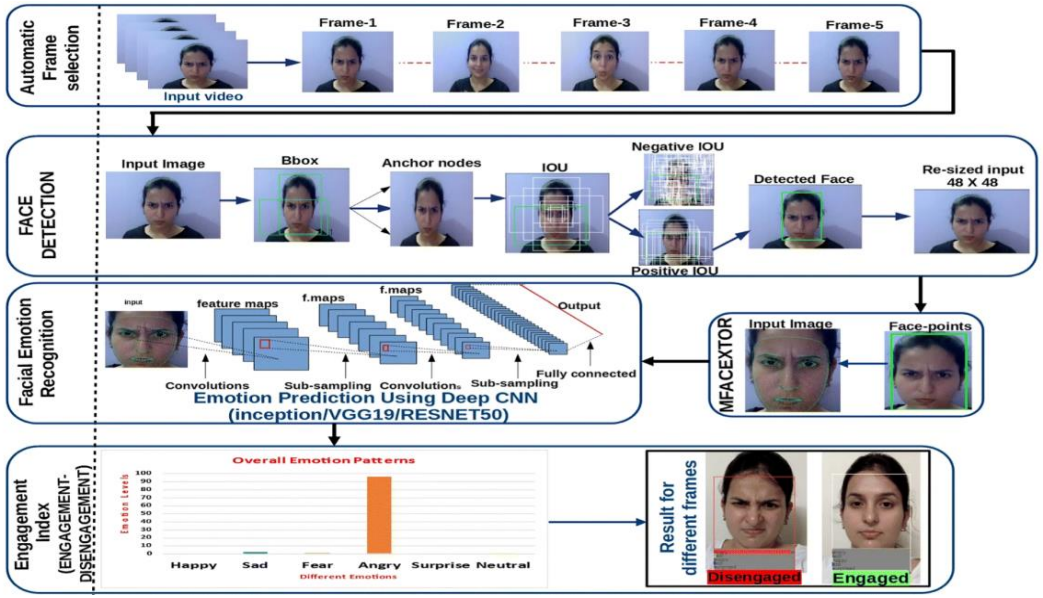
- Humberside Police successfully implemented AI technology in their contact centre systems, with a proof of concept focusing on domestic abuse calls
  - Acting as an assistant to call handlers focusing on transcription, data mapping, and risk analysis.
  - Enables call handlers to provide a seamless victim experience, while the AI assistant records important information and carries out background searches.

Digital Assistants

- Oklahoma City Police are piloting an AI tool to aid in drafting incident reports for minor incident reports that do not lead to someone getting arrested
  - Includes inputs from sounds and radio chatter picked up by the microphone attached to body cameras.
  - Same underlying technology as ChatGPT but with different controls

Facial Recognition Technology (FRT)

- The Met has been using live facial recognition technology for several years, deploying it first at Notting Hill Carnival in 2016, expanded to public spaces like London's busy streets and sporting events.
- A step further - automatic stress detection system that can work in real-time.
  - a real-time deep learning framework that fused ECG, voice, and facial expressions for acute stress detection



AI Use Cases

Emergency Services Applicability

- **Fire and Rescue**: AI can be leveraged for disaster prediction, response coordination, and managing hazardous situations.
- **Emergency Medical Services**: AI in medical triage, emergency incident prediction and response, and resource allocation.
- **Law Enforcement**: AI in crime analysis, evidence processing, and predictive policing
- **Crisis Management**: Utilising AI in risk assessment of critical incidents, evacuation planning, and relief operations coordination.
- **Civil / Public works**: Traffic management, infrastructure condition management.

AI Threat Vectors

Major Types

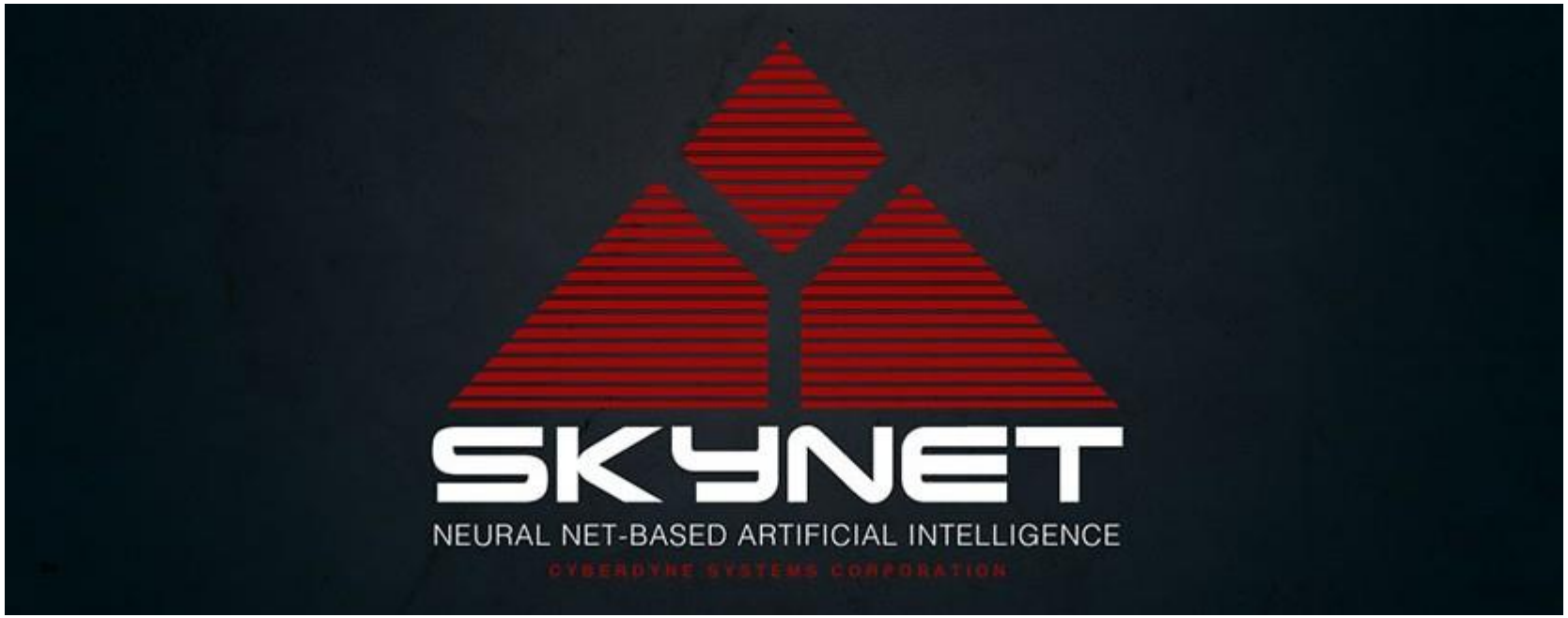
- Evasion
- Poisoning
- Privacy
- Abuse

Risks of using AI

- **Privacy and Data Security**: AI systems often collect and analyse large amounts of data set including personal data. This raises concerns about privacy breaches, misuse of personal data and the potential risk of surveillance.
- **Algorithmic Bias:** AI systems are trained on large datasets. These models can inherit biases present in training data, leading to biased decision making. The AI system can also amplify these biases and generate discriminating results in sensitive areas like hiring, lending, and law enforcement. Such biases eventually leads to unfair treatment and perpetuate social inequalities.
- **Ethical Concerns:** Decisions made by AI, especially in areas like Law Enforcement, Healthcare and Criminal Justice raises concerns about the morality of letting machines make life-changing decisions without human oversight.
- **Misinformation and Deepfakes:** In the current age where information / data is at the forefront of almost everything we do, spreading misinformation, manipulate public opinion, or harm individuals through fake audio, video, or other forms of media.
- **Safety and Security:** AI tools can be used maliciously for cyberattacks, control autonomous weapons systems for unintended actions eventually leading to unprecedented consequences that can cause catastrophic outcomes. There is also a significant risk in the long run about AI systems training themselves to be ‘superintelligent’ and becoming self-aware and starts to operate beyond human control.

• **Privacy and Data Security: AI systems often collect and analyse large amounts of data set**

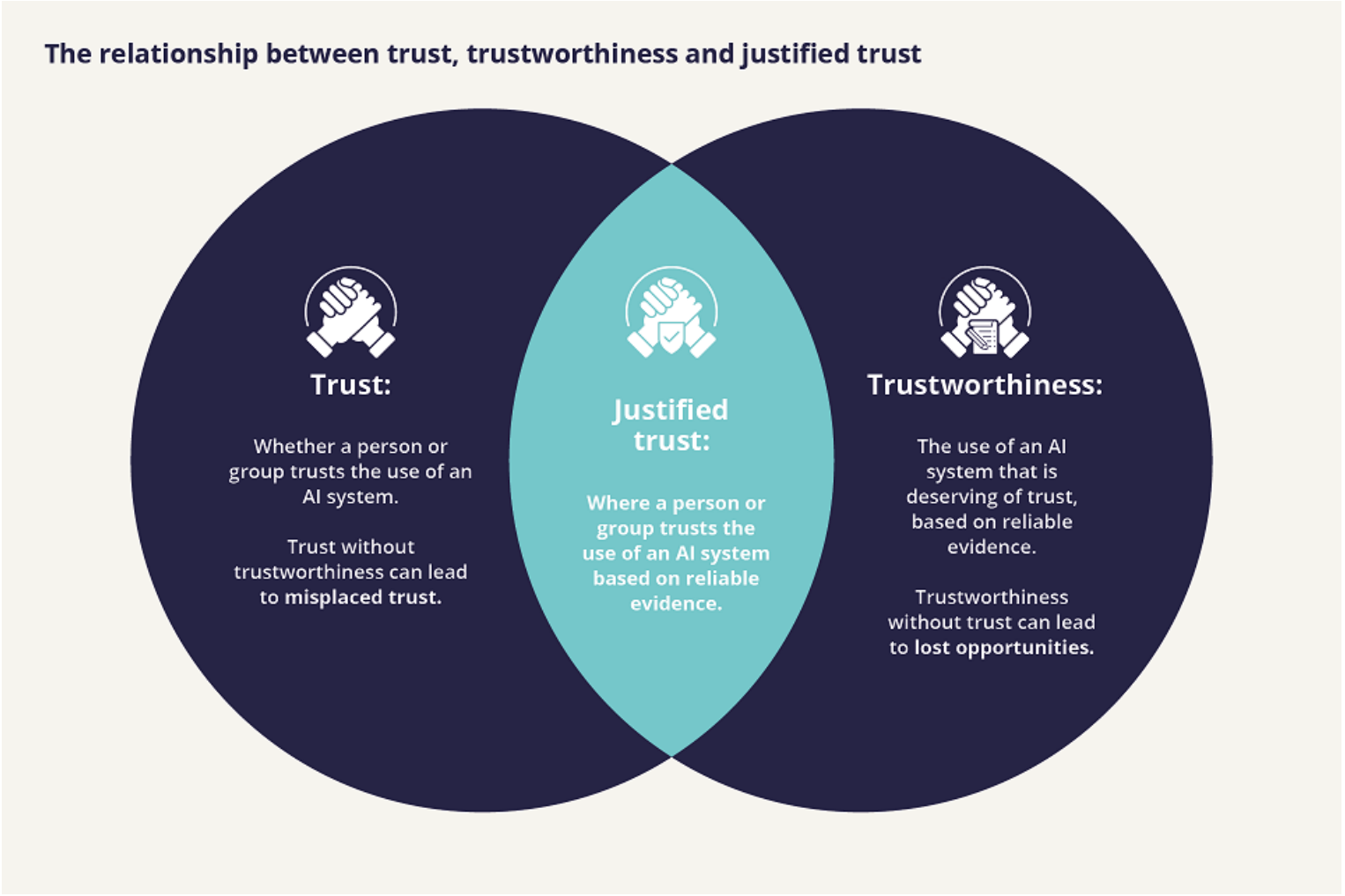
Skynet?



Assurance of AI

Importance

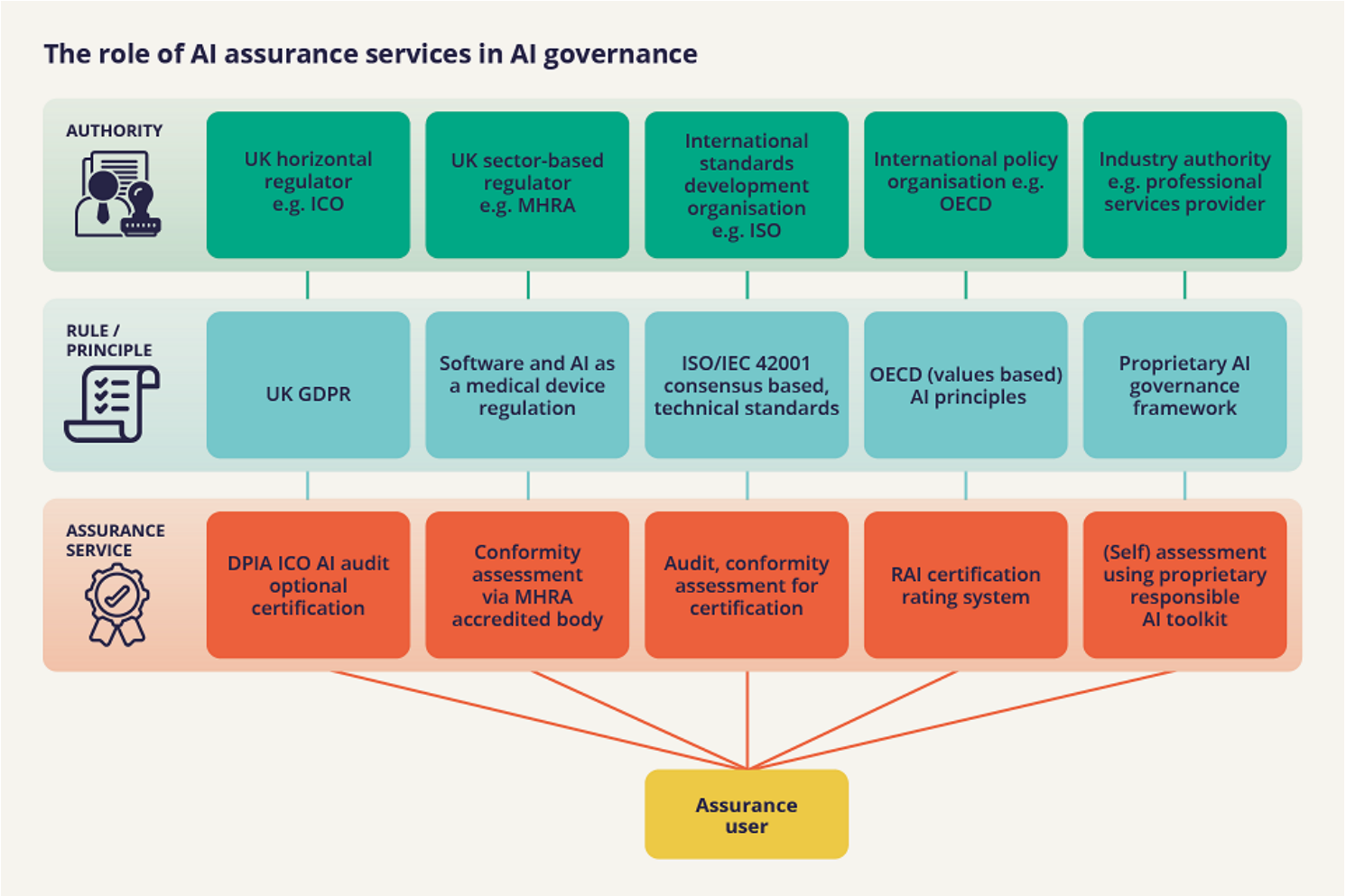
- Transparency
- Bias Mitigation
- Reliability
- Trust and Trustworthiness



Assurance of AI

Frameworks

- NIST AI 600-1
- EU AI Act
- ISO / IEC JTC 1/SC 42
- ACM Code of Ethics



Source: The roadmap to an effective AI assurance ecosystem, Gov.UK

Kim Seward

Head of Capability Development – Data & Digital

kim.seward@leonardo.com

Chowdhury Rahman

Managing Consultant – Cyber & Security Division

chowdhury.rahman@leonardo.com

uk.leonardo.com

THANK **YOU**
FOR YOUR ATTENTION

uk.leonardo.com