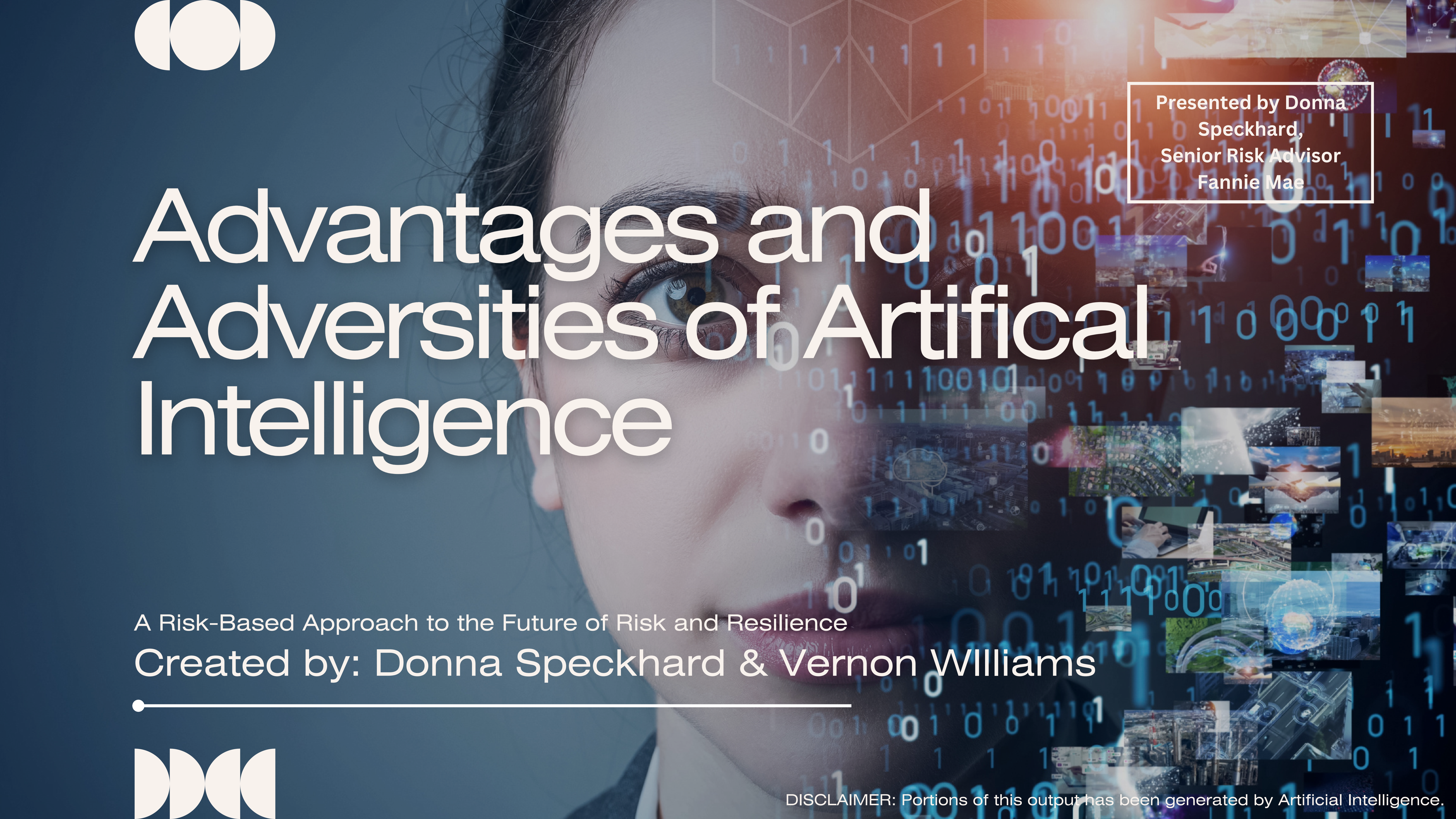


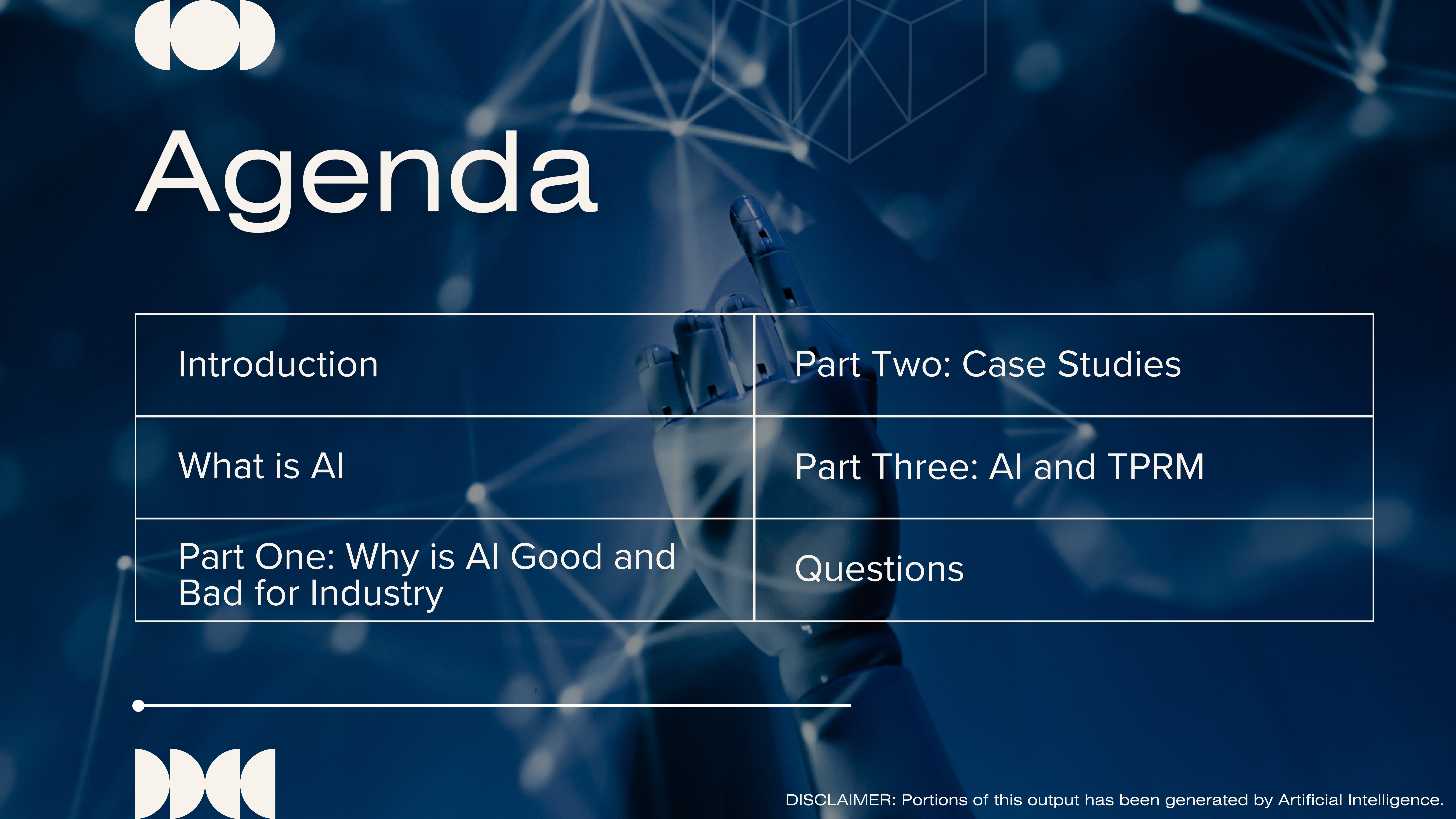
Presented by Donna Speckhard,
Senior Risk Advisor
Fannie Mae

Advantages and Adversities of Artifical Intelligence

A Risk-Based Approach to the Future of Risk and Resilience

Created by: Donna Speckhard & Vernon WIlliams

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.



Agenda

- Introduction
- What is AI
- Part One: Why is AI Good and Bad for Industry
- Part Two: Case Studies
- Part Three: AI and TPRM
- Questions

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

AI IS HERE AND AS VAST AS WE CAN IMAGINE... BUT THIS PRESENTATION IS NOT

ACTIVITY ON AI

We are going to split the room into groups.

Pick a spokesperson

Take about 10 min

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Context is everything

01

AI

Generative AI

Machine Learning

AI Hallucinations

02

AI is not new, The term "artificial intelligence" was coined in 1956 by John McCarthy at the Dartmouth Conference, marking the start of focused AI research.

03

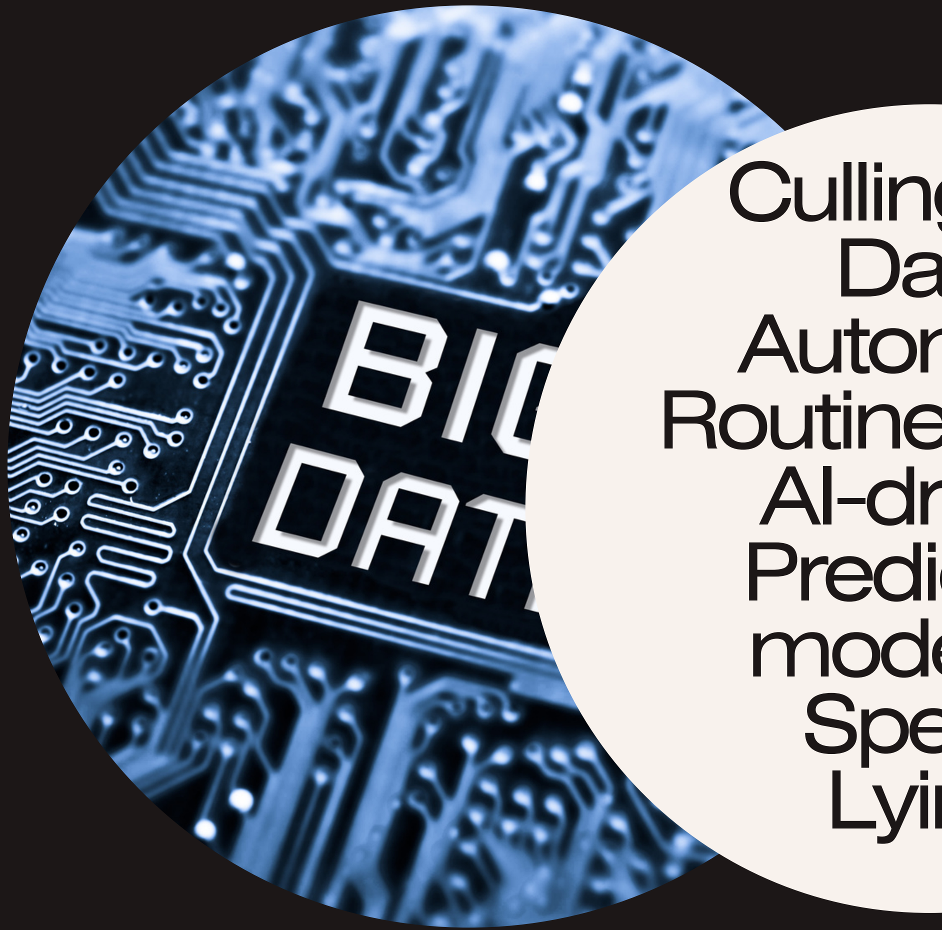
Aravo whitepaper:

Does this third-party align to our risk appetite? Are there any indications that a third party is likely to be involved in bribery or corruption? Are they a critical supplier?

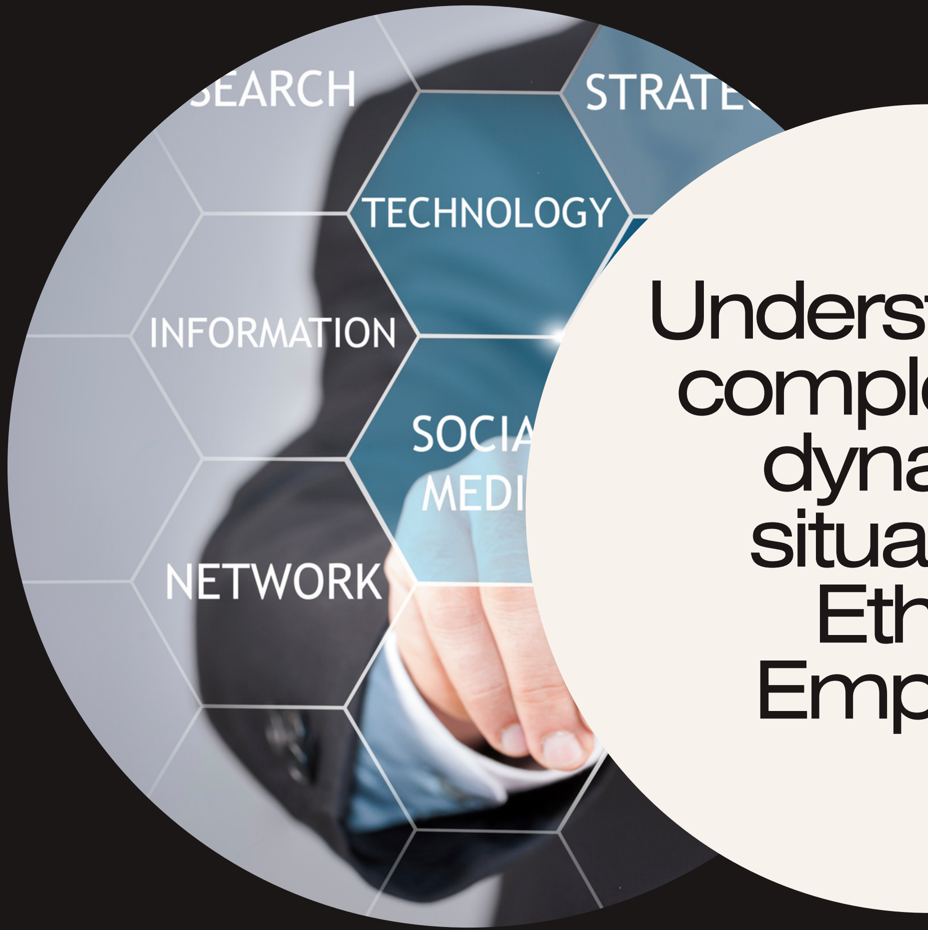
Not a Cyber Talk

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

What is AI Good at and What are Humans Better at?



Culling Big Data
Automate Routine Tasks
AI-driven Predictive modeling
Speed
Lying



Understanding complex and dynamic situations
Ethics
Empathy

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Why is AI Good for Industry?

PART ONE

Agriculture

- Decrease wasted water
- Increase crop production
- Increase in pest avoidance
- Improvement in supply chain management

Energy

- Safer data collection
- Better transparency
- Focus on relevant data in vast amount of data on wear and strength of machines

Healthcare

- Time Savings in an industry with a skills shortage
- Early disease detection/accuracy
- Mitigate human error
- Ensure compliance

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Why is AI Bad for Industry?

PART ONE

Agriculture

- Limited access
- Divide between Corporate and Subsistence Farmers
- Increased fuel/battery requirements
- Data and security issues

Energy

- Dependence on data driven metrics
- Unregulated and open AI adoption can lead to irregular results
- Overconfidence in technology - increases catastrophic risks

Healthcare

- Human jobs replaced by AI (Fear)
- Customer comfort/Company culture
- Patient privacy and security concerns
- Third party risk

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Case Study

PART TWO

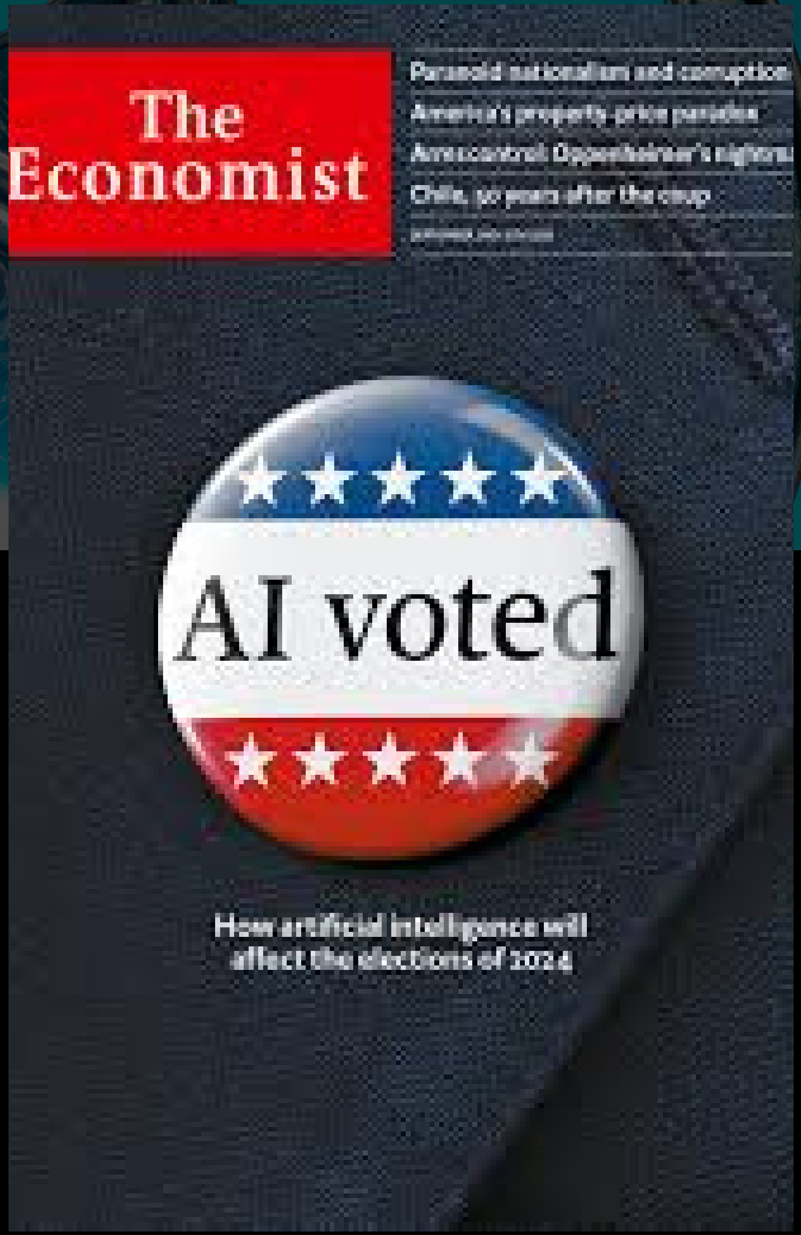
50+ Countries w/Elections in 2024

Misinformation/disinformation - Experts warn AI and deepfakes will likely be worse in the coming elections.

- In the U.S., FCC banned AI-generated robocalls impacting voters. Tech giants signed an agreement to prevent AI interference in global elections. Davos report identifies AI-driven misinformation as a top short-term threat.

AI-powered misinformation and disinformation is emerging as a risk as people in a slew of countries head to the polls.

“To change the future we must be able to imagine a different future” - Sohail Inayatullah


The Economist
Paranoid nationalism and corruption
America's property-price paradox
Arms control: Oppenheimer's nightmare
Chile, 50 years after the coup
AI voted
How artificial intelligence will affect the elections of 2024

LET'S TAKE A DEEPER LOOK

■ **Deepfakes**	Moldova, Slovakia, Bangladesh, India
■ **China**	U.S. Rep Rob Wittman Deepfake

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Case Study

PART TWO

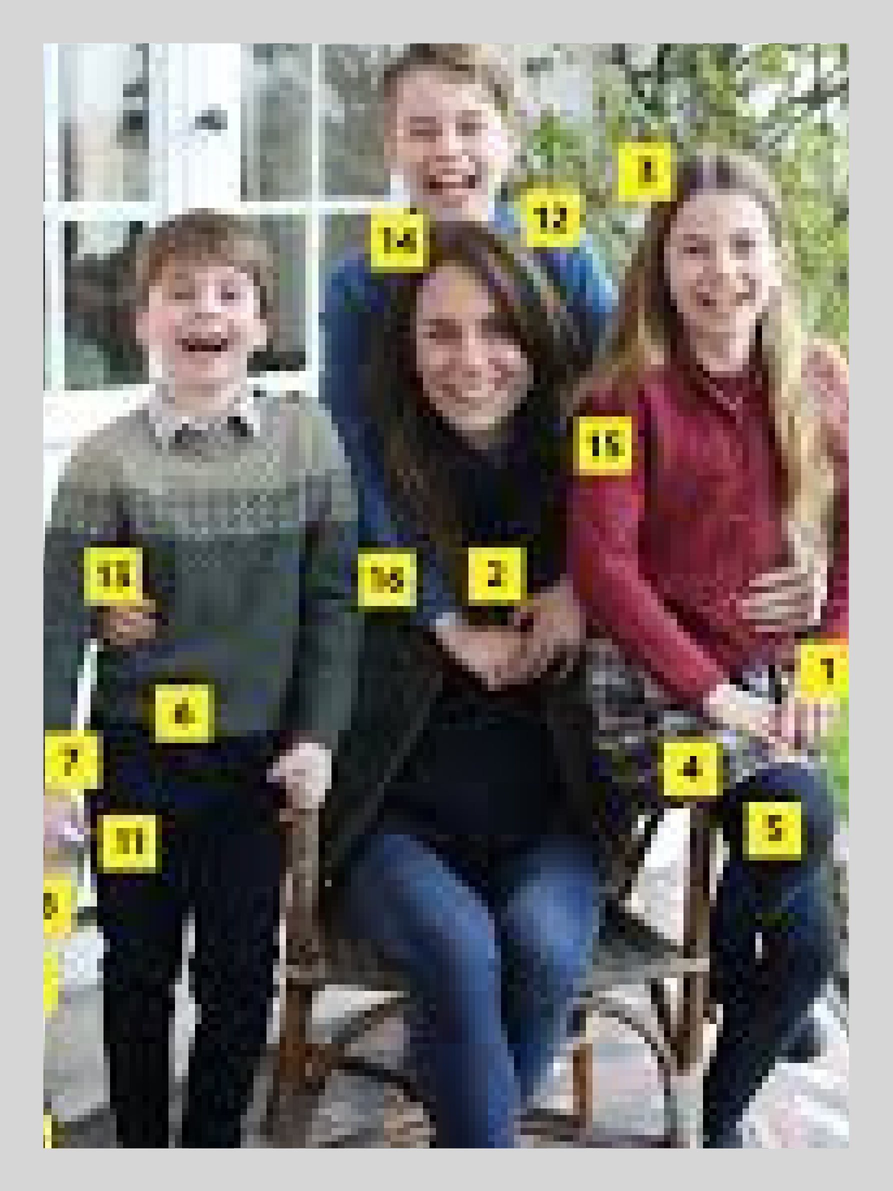
Irresponsible Use & Ethics

- Biased Decision-Making
- Surveillance and Privacy Violations
- Deepfake Creation
- Autonomous Weapons

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Examples where Irresponsible Use and Ethics have or will cause issues and increased risk.

Prom Pact - Disney



Kate Middleton - Princess of Wales

Open AI’s SORA

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Case Study

PART TWO

55%

AI failures from third-party tools

An area of focus is third-party AI - referring to tools or algorithms created by a different company that organizations purchase, license, or utilize, as outlined in a recent research report by MIT Sloan Management Review and Boston Consulting Group.

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

PART THREE

What does this all mean for Third Party Risk Professionals?

01
Healthcare

02
Financial Institutions

03
Retail

04
Manufacturing

05
Agriculture

06
Education

07
Energy

08
Supply Chain

09
Law Enforcement

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Ways companies can reduce risk from AI and what can AI be used for in TPRM?

PART THREE

To minimize AI risk in TPRM:

- Accelerate the growth of AI Programs promptly
- Thoroughly assess third-party tools
- Stay ready for regulatory changes
- Involve Leadership in promoting responsible AI initiatives
- Increase investments in responsible AI efforts

Potential uses of AI:

- Supervising vendor compliance
- Evaluating vendor risk
- Handling vendor reputation
- Automating due diligence processes
- Predictive analytics for future risks

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Managing AI Risks

Data Privacy & Security

Sharing sensitive patient data with a third-party AI system for improved diagnostics can pose risks like breaches, unauthorized access, and data misuse, leading to legal and reputational consequences.

Limited Customization and Control

Two banks in different locations implementing the same AI fraud detection solution may face challenges due to their unique customer demographics, transaction patterns, and risk profiles. The third-party AI solution may struggle to capture the specific nuances of each bank's operations, potentially impacting detection accuracy and leading to undetected fraud or false positives.

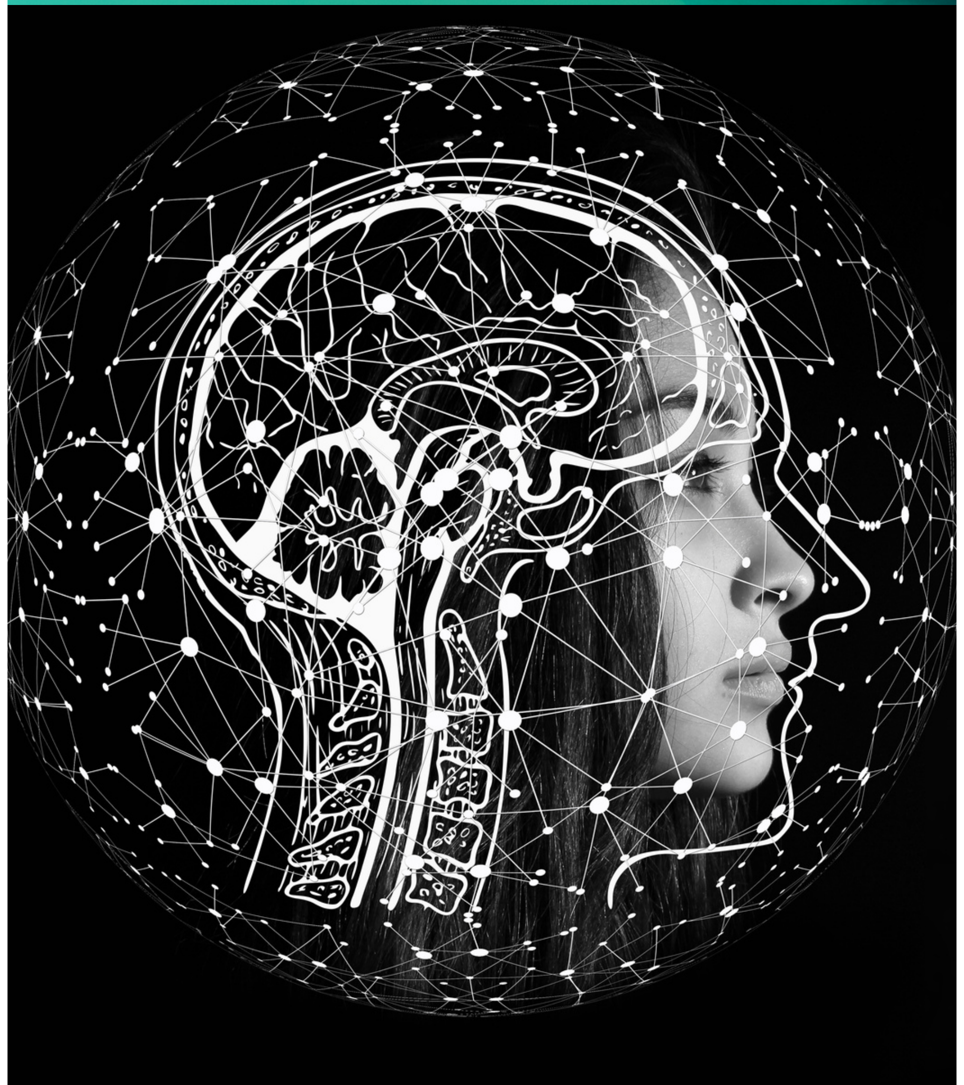
Performance and Reliability

To minimize risks when considering AI vendors, evaluate their performance track record including system uptime, response time, and error rate. Establish clear service level agreements (SLAs) defining expected performance levels, uptime guarantees, and response times for issue resolution.

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Top 10 Questions to ask before adopting AI in your Organization

- Do you have a fundamental understanding of how AI works?
- Have you identified specific tasks and organizational processes that AI could enhance?
- Do the identified AI uses align with organizational governance structure, standards, organization and community values and risk frameworks?
- Are data protection and privacy policies in place?
- Can you audit the AI tool's outputs for biases and risks, and are you prepared to take responsibility for these outputs?
- Does your organization have in-house skills and resources allocated for AI initiatives?
- Are training resources available, and are employees adequately prepared to use AI tools effectively and ethically?
- Is there organizational transparency and trust concerning the AI's processes and outputs, both internally and in the community?
- Have you considered the initial and ongoing costs of the AI tool? Is the cost fixed or scaled with use?
- Have you envisaged potential crises that could arise from AI utilization, and is there a robust crisis response plan to address AI-induced challenges?



Handouts

AI Glossary

Implementing AI in your Organization

Regulations/Guidance

- NIST AI Risk Management Framework (RMF)
- EU AI Act
- US Presidential Executive Order
- AI Policy
- AI Framework

TPRA's ML/AI Questions WG

- TPRM 101 Guidance & Build-out

Source: Justin Snair, MPA, Managing Partner, SGNL Solutions / CEO and Founder, Preppr.ai, Donna Speckhard, and Vernon Williams

QUESTIONS FOR AI IMPLEMENTATION

PART THREE

- **Purpose & Application**
- **Tool Legitimacy**
- **Data Sensitivity & Security**
- **Ethical Considerations**
- **Usability & Training**
- **Transparency & Accountability**
- **Performance & Reliability**
- **Integration w/current Systems**
- **Feedback & Support**
- **Budget & Costs**
- **Contingency & Backup**
- **Legal Liability**

- **Infrastructure & Compatibility**
- **Vendor Credibility**
- **Data Management & Security**
- **Ethical and Responsible Use**
- **Training & Vendor Support**
- **Stakeholder Engagement**
- **Regulatory Adherence**
- **Performance Monitoring**
- **Transparency & Accountability**
- **Budgetary Considerations**
- **Contingency Protocols**

Want a copy? Are we missing anything? Contact us at:
contact@rationalrisk.com for crowdsourcing

Source in-part for questions: Justin Snair, MPA, Managing Partner, SGNL Solutions / CEO and Founder, Preppr.ai , Donna Speckhard, and Vernon Williams

Someone asked AI to create “Aliens: the Musical”. Unfortunately, it looks fantastic!

Questions?

"Aliens: The
future, on a bustling, co
station at the edge of the galaxy. Th
melting pot of intergalactic cultures, serve
the backdrop for a story of unity, love, and
fight against a common, unseen threat. T
narrative follows Aria, a talented enginee
a passion for music, and Zan, an alien b
from a planet where music is their form
speech. Despite their different backgro
they discover a shared melody that tr
language and species.
As the space station faces an imper
invasion by a mysterious alien forc
Zan must unite the station's divers
inhabitants through the universal
orchestrate a harmo

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

Contact Me

☎

+571-233-8450

✉

Donna_x_Speckhard@fanniemae.com

LinkedIn

www.linkedin.com/in/donnaspeckhard/

DONNA
SPECKHARD
FANNIE MAE
SENIOR RISK ADVISOR

DISCLAIMER: Portions of this output has been generated by Artificial Intelligence.

AI Glossary – made with AI assistance for TPRA Presentation purposes only.
Created by Donna Speckhard and Vernon Williams

What are we missing?
Email contact@rationalrisk.com for crowdsourcing

Artificial Intelligence (AI) Glossary

1. **Artificial Intelligence (AI):**

Definition: A branch of computer science that aims to create machines capable of performing tasks that typically require human intelligence. These tasks include learning, reasoning, problem-solving, perception, language understanding, and speech recognition.

2. **Artificial Intelligence Ethics:**

Definition: The study and implementation of principles and guidelines to ensure that AI systems are developed and used in a responsible, transparent, and ethical manner, considering societal impact, privacy, and fairness.

3. **Artificial Intelligence (AI) Hallucinations:**

Definition: When a generative AI model generates inaccurate information as if it were correct. AI hallucinations are often caused by limitations or biases in training data and algorithms, it can result in producing content that is wrong or even harmful.

4. **Augmented Intelligence**

Definition: Augmented intelligence, also known as intelligence augmentation (IA), refers to a concept where artificial intelligence (AI) technologies are utilized to enhance and complement human capabilities rather than replace them entirely. Unlike the idea of fully autonomous AI systems, augmented intelligence focuses on collaboration between humans and machines, leveraging the strengths of each to achieve better outcomes.

5. **AML (Automated Machine Learning):**

Definition: A subset of AI that involves the automation of the end-to-end process of applying machine learning to real-world problems. AML platforms streamline tasks such as feature engineering, model selection, and hyperparameter tuning, making machine learning accessible to individuals with limited expertise in the field. AML aims to accelerate the development and deployment of machine learning models, allowing organizations to harness the power of AI more efficiently.

6. **Bias in AI:**

Definition: The presence of unfair or prejudiced outcomes in AI models, often stemming from biased training data or the design of the algorithms. Addressing bias is a critical consideration in AI development to ensure fair and ethical use.

7. **Black Box AI:**

Definition: Refers to AI systems or models whose internal workings and decision-making processes are opaque and not easily interpretable or explainable. In black box AI, understanding how a model arrives at a specific decision or prediction can be challenging, raising concerns about accountability, transparency, and potential biases. Efforts in Explainable AI (XAI) aim to mitigate the black box nature of AI systems, providing insights into their decision logic for better understanding and trust.

8. **Computer Vision:**

Definition: The field of AI that enables machines to interpret and make decisions based on visual data. Applications include image recognition, object detection, and facial recognition.

9. **Deepfake:**

Definition: A form of AI-generated content that uses deep learning techniques, particularly Generative Adversarial Networks (GANs), to create realistic-looking but entirely fabricated multimedia, including videos, audio recordings, and images. Deepfakes have raised concerns due to their potential for misinformation, identity theft, and the manipulation of public opinion. Addressing the challenges posed by deepfakes involves the development of detection methods, legal frameworks, and public awareness campaigns to mitigate their negative impact on society.

10. **Deep Learning:**

Definition: A specialized area of machine learning that involves neural networks with multiple layers (deep neural networks). Deep learning algorithms are capable of automatically learning hierarchical representations of data, enabling them to extract complex patterns and features.

11. **Edge Computing:**

Definition: The practice of processing data near the source of generation (on the "edge" of the network) rather than relying on centralized cloud servers. This approach is increasingly important for AI applications that require real-time processing.

12. **Explainable AI (XAI):**

Definition: A concept in AI design that emphasizes creating models and systems whose decisions and actions can be easily understood and interpreted by humans, promoting transparency and trust. Explainable AI is crucial in AML, ensuring that automated processes are not only accurate but also comprehensible, allowing stakeholders to validate and trust the models' outcomes. This becomes particularly important in sensitive domains such as finance, healthcare, and legal systems.

13. **Generative AI:**

Definition: A category of AI that focuses on creating models capable of generating new and original content, such as text, images, or music. Generative AI relies on techniques like Generative Adversarial Networks (GANs) and recurrent neural networks to produce novel and realistic outputs.

14. **Machine Learning (ML):**

Definition: A subset of AI that focuses on the development of algorithms and statistical models that enable computers to improve their performance on a task through experience (learning) without being explicitly programmed.

15. **Natural Language Processing (NLP):**

Definition: A subfield of AI that focuses on enabling machines to understand, interpret, and generate human language. NLP is crucial for applications such as language translation, sentiment analysis, and chatbots.

16. **Neural Network:**

Definition: A computational model inspired by the structure and function of the human brain. Neural networks consist of interconnected nodes organized in layers, and they are used in various AI tasks, including image and speech recognition.

17. **Reinforcement Learning:**

Definition: A type of machine learning where an agent learns to make decisions by interacting with an environment. The agent receives feedback in the form of rewards or penalties, allowing it to learn optimal strategies through trial and error.

18. **Resilience Artificial Intelligence (RAI)**

Definition: Development of AI systems capable of withstanding adversities, adapting to unexpected changes, and recovering from failures.

19. **Supervised Learning:**

Definition: A type of machine learning where the model is trained on a labeled dataset, meaning that each input is paired with the corresponding correct output. The goal is for the model to learn the mapping between inputs and outputs.

20. **Training Data:**

Definition: The dataset used to train machine learning models. It consists of input-output pairs, where the model learns patterns and relationships to make predictions on new, unseen data.

21. **Unsupervised Learning:**

Definition: A type of machine learning where the model is trained on an unlabeled dataset, and its task is to find patterns, structures, or relationships within the data without explicit guidance on the output.

22. **Weaponized Misinformation:**

Definition: False or misleading information deliberately crafted and disseminated to manipulate perceptions, influence opinions, or achieve specific strategic objectives, often through digital platforms and media channels.

AI Implementation Questions - TPRA

Source: Justin Snair, MPA, Managing Partner, SGNL Solutions / CEO and Founder, Preppr.ai – with additions/adaptations by Donna Speckhard and Vernon Williams

What are we missing?
Email contact@rationalrisk.com for crowdsourcing

Purpose & Application

- What specific task or challenge am I aiming to address with this AI tool? Specify the type of tasks (analytical, predictive, operational) to better evaluate the tool's applicability.
- How will this tool enhance or improve my current work processes?
- Are there any potential negative implications of using this tool in my role?

Tool Legitimacy

- Is this tool officially recognized or approved by my organization or department?
- If not, are there any policies against using third-party tools in my position? Detail the process for tool approval within the organization to better navigate bureaucratic hurdles.
- What are the potential consequences of using an unauthorized tool? Consider the risks to self and the company.

Data Sensitivity & Security

- Will I be using the tool with sensitive or classified data? Clarify the types of sensitive data (personal, financial, strategic) to assess risk levels more precisely before beginning.
- How does the AI tool handle data privacy and encryption?
- Are there risks of data leaks or breaches when using this tool?
- Where is the data being pulled from?

Ethical Considerations

- Does the AI tool align with the ethical standards of my organization and position? Write out the defined ethical standards to ensure alignment with organizational values and societal norms and avoid losing track of them in the process.
- Are there potential biases or fairness issues associated with the tool's outputs?
- How might the use of this tool impact stakeholders or the public?

Usability & Training

- How user-friendly is the AI tool?

- Are there training resources or guides available for this tool?
- Do I possess the necessary skills and knowledge to use the tool effectively?

Transparency & Accountability

- How transparent are the tool's processes and output production mechanisms?
- If questioned, can I explain the tool's processes and outputs?
- Am I prepared to take responsibility for the tool's outputs in my work?

Performance & Reliability

- How accurate and reliable is the AI tool in delivering the desired outcomes?
- Are there mechanisms to verify or cross-check the tool's outputs?
- How does the tool handle errors or inaccuracies?

Integration with Current Systems

- Is the AI tool compatible with the software and platforms I currently use
- Are there potential integration challenges or conflicts with my existing systems?
- Will using this tool disrupt my regular workflow?

Feedback & Support

- Is there a support system or helpline available for this AI tool?
- How can I provide feedback or report issues with the tool?
- Are there user communities or forums where I can seek help or share experiences?

Budget & Costs

- Is there a cost associated with using this AI tool?
- If so, will I need to get budget approval or will it be an out-of-pocket expense?
- Are there additional costs for updates, premium features, or extended usage?

Contingency & Backup

- What are my backup plans if the AI tool fails or provides incorrect outputs?
- How will I handle any challenges or discrepancies arising from the tool's use?
- Are there alternative tools or methods I can rely on if needed?

Legal Liability

- Are you protected by Insurance?

- Legally, are you protected from lawsuits?
- How do you regulate AI?
- Where does consent and accountability come in?
- Who “owns” AI created product?

Infrastructure & Compatibility

- Does our current IT infrastructure support the technical requirements of the third-party AI tool we're considering?
- Have we identified potential integration challenges with our existing systems?
- Is our team equipped to handle the integration process?
- Are there backup systems in place in case of integration failures?

Interoperability & Ecosystem Compatibility

- Can the AI tool seamlessly interact with other tools and systems in our technology ecosystem?
- Does the tool support standard data formats and APIs for easy integration with existing databases and applications?
- What are the implications of tool integration on data flow and system architecture within our existing IT infrastructure?

Vendor Credibility & Risk

- Has the AI tool provider successfully worked with public sector entities before?
- What feedback or reviews are available about this vendor's performance and support?
- How does the vendor handle updates and improvements to the tool?
- Are there case studies or references we can review? Specify criteria for evaluating vendor credibility, such as industry reputation, client testimonials, or specific types of case studies.
- Has the vendor been through a third-party risk assessment?
- Is the vendor regularly monitored through tools like Dun & Bradstreet, LexisNexis Bridger Insight, Silobreaker, or other intelligence/risk screening tools?

Data Management & Security

- How does the AI tool handle data privacy, storage, and transfer?
- Are there clear protocols to ensure our data remains protected and compliant with regulations?
- How frequently is our data backed up?
- In case of a security breach, what are the vendor's response protocols?

Ethical and Responsible Use

- Does the vendor provide guidelines on the ethical application of their AI tool?
- How are issues like potential bias or fairness addressed within the tool?
- Are there mechanisms to audit the tool's decisions for ethical considerations?
- How does the vendor handle controversial or ethically ambiguous scenarios?

Training & Vendor Support

- What training resources does the vendor provide to ensure successful implementation?
- Is there a dedicated support team available for troubleshooting and queries?
- How frequently are training updates provided?
- Are there user communities or forums for peer support and knowledge sharing?

Scalability & Future-Proofing

- How scalable is the AI tool in response to growing data volumes and evolving business needs?
- Does the tool offer flexibility to adapt to future tech advancements or changes in business strategy?
- What are the vendor's commitments (and capability) to updating and improving the tool in alignment with future trends and technologies? (Very important!)

Stakeholder Engagement

- How can we effectively communicate the role and impact of this AI tool to our stakeholders?
- Are there features within the tool to facilitate transparency and public engagement?
- How can stakeholders provide feedback or express concerns?
- Is there a plan to keep stakeholders updated on AI tool outcomes and changes?

Regulatory Adherence

- Is the AI tool compliant with all relevant local, state, and national regulations?
- How frequently is the tool updated to remain compliant?
- Are there dedicated teams or individuals monitoring regulatory changes?
- How are users informed of regulatory changes affecting the tool?

Performance Monitoring

- What metrics or benchmarks can we use to evaluate the tool's effectiveness and accuracy?
- Are there mechanisms in place to provide feedback and get updates?
- How does the tool handle errors or inaccuracies?

- Are there regular performance reports available for review?

Impact Assessment & Value Realization

- How will the tool's implementation impact current operational efficiencies and employee productivity?
- What metrics will be used to measure the tool's impact on achieving strategic objectives and delivering value?
- Is there a framework in place to regularly assess the tool's contribution to targeted business outcomes and ROI?

Transparency & Accountability

- How transparent are the AI's processes, decision making, and/or output production mechanisms?
- Is there a clear channel to hold the tool or vendor accountable for any discrepancies or issues?
- Are there logs or records of the AI's outputs? Are these accessible to the agency? Are these accessible to the public?
- How are disputes or disagreements with the tool's outputs resolved?

Budgetary Considerations

- Have we accounted for all costs, including initial setup, licensing, and ongoing maintenance?
- Does the ROI of the AI tool justify its costs for our agency?
- Are there hidden costs or potential financial pitfalls we should be aware of?
- How does the tool's pricing compare to similar tools in the market?

Contingency Protocols

- What are our protocols in case of tool malfunctions, misleading outputs, or other challenges?
- How swiftly can the vendor respond to critical issues or challenges?
- Are there backup tools or systems in place?
- How frequently are contingency protocols reviewed and updated?