Third Party Attestation - ISO 42001

FEBRUARY 2025

BDO USA, P.C, a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

Our Agenda Today

- The Need for Trust in AI
- AI Regulations
- What is ISO 42001?
- ISO 42001 – Discussion of Key Points
- FAQ

With You Today

BINITA PRADHAN
Third Party Attestation
Market Managing Principal (West)

bpradhan@bdo.com

VARUN PRASAD
Third Party Attestation
Managing Director

vprasad@bdo.com

Learning Objectives

- Recognize the purpose and benefit of ISO 42001 certification
- Explain how ISO 42001 plays a crucial role in AI Governance
- Describe how to promote public trust in their organizations AI systems

AI Does Fail!

MCDONALDS

- McDonald’s ends its 3-year AI experiment after drive-thru ordering blunders in June 2024
- Was working with IBM

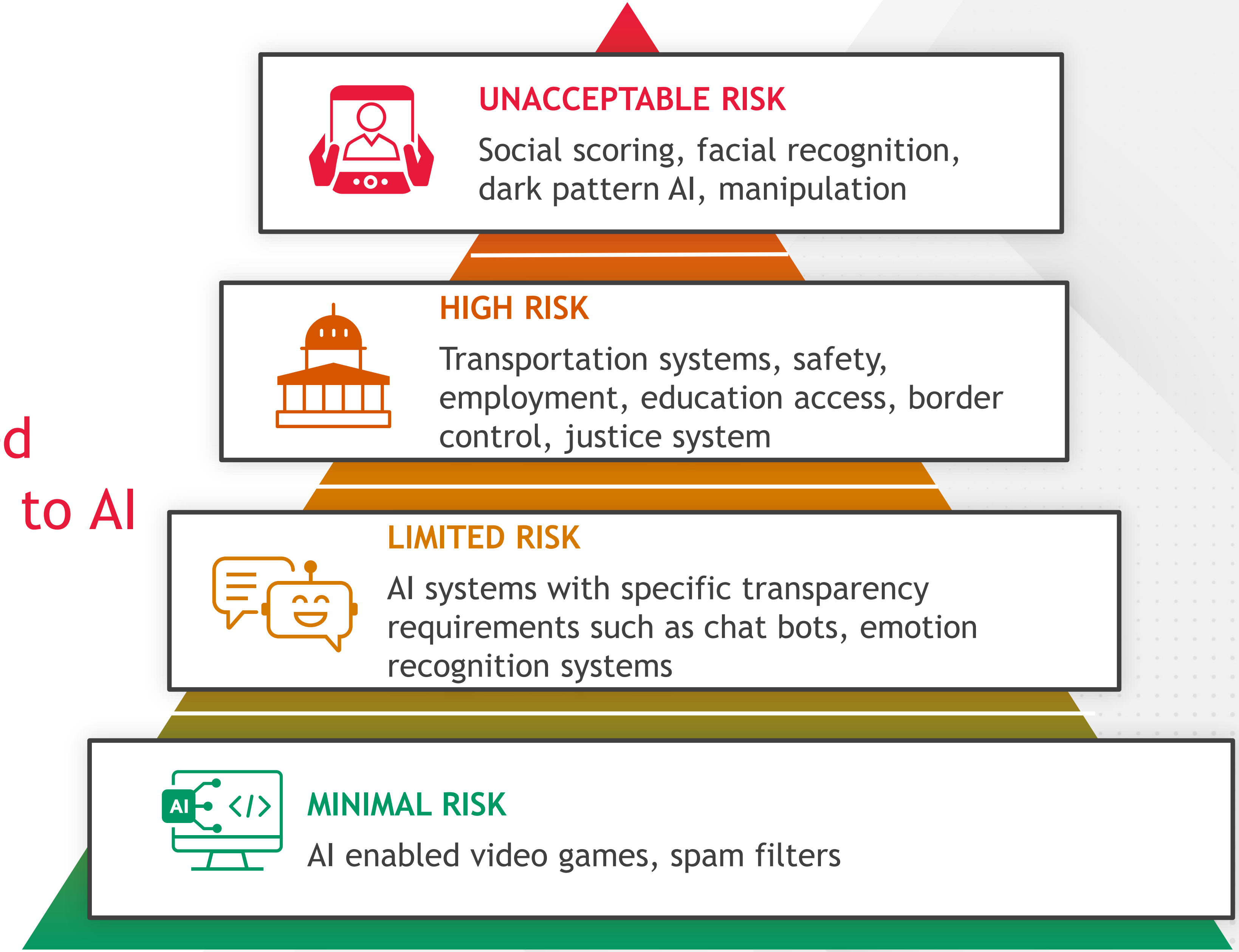
AIR CANADA

- Early 2024, chatbot provided incorrect info to customer
- Airline paid compensation and damages

TRIVAGO

- ACCC vs. Trivago
- Misled customers to book hotels with higher commission
- Paid ~$44M penalties

Risk-Based Approach to AI



UNACCEPTABLE RISK

Social scoring, facial recognition, dark pattern AI, manipulation

HIGH RISK

Transportation systems, safety, employment, education access, border control, justice system

LIMITED RISK

AI systems with specific transparency requirements such as chat bots, emotion recognition systems

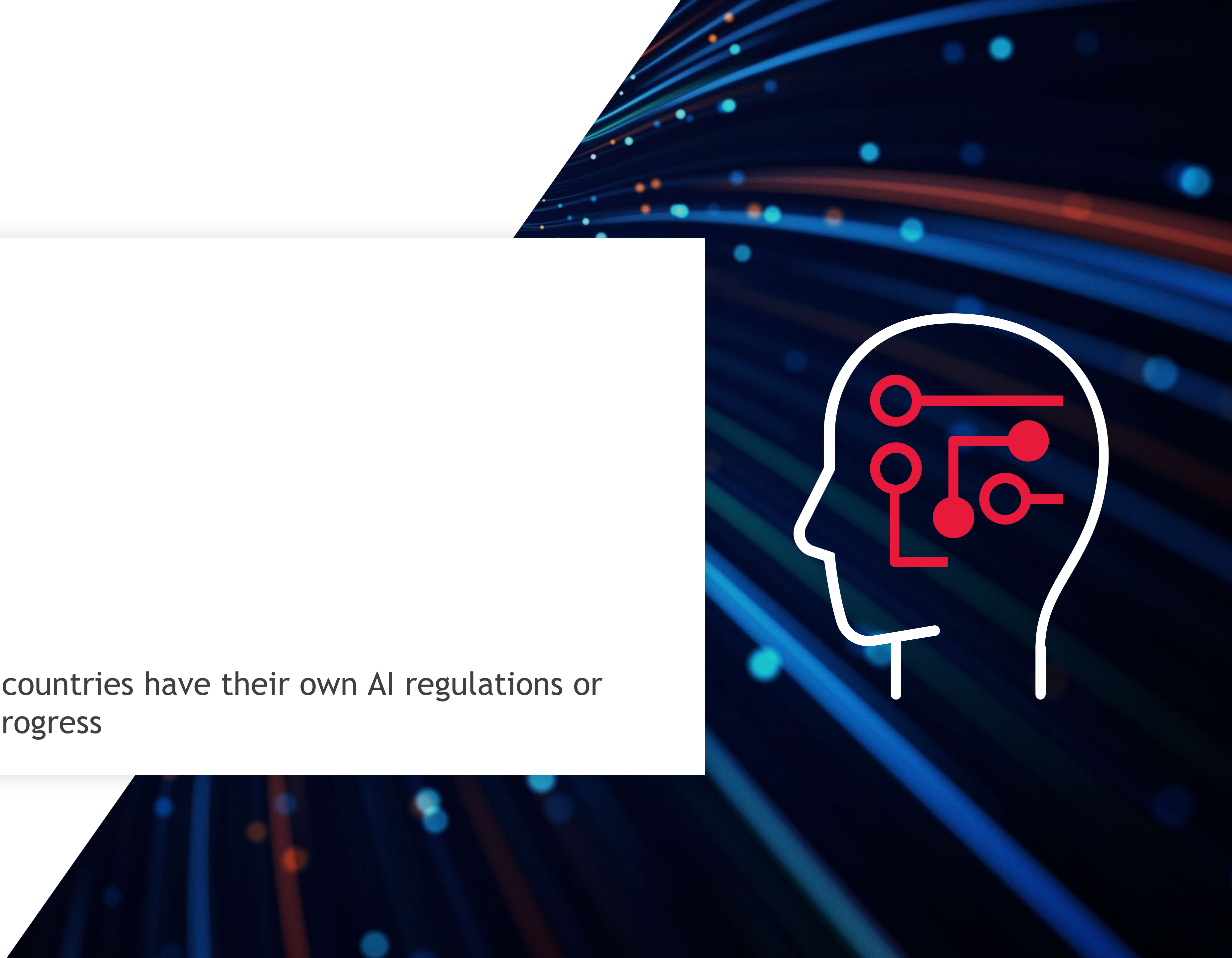
MINIMAL RISK

AI enabled video games, spam filters

https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

AI Regulations

- EU AI Act
- Utah
- California
- Colorado
- Various other states and countries have their own AI regulations or have the regulations in progress



Key Requirements of the EU AI Act for Providers of the High-risk AI Systems:

- Risk Management System
- Quality Management System
- Data and Data Governance
- Accuracy, Robustness and Cybersecurity
- Technical Documentation, Recordkeeping, and Transparency
- Postmarket Monitoring
- Human Oversight
- AI Literacy
- Registration
- Reporting of Serious Incidents

https://www.isaca.org/resources/white-papers/2024/understanding-the-eu-ai-act#f24

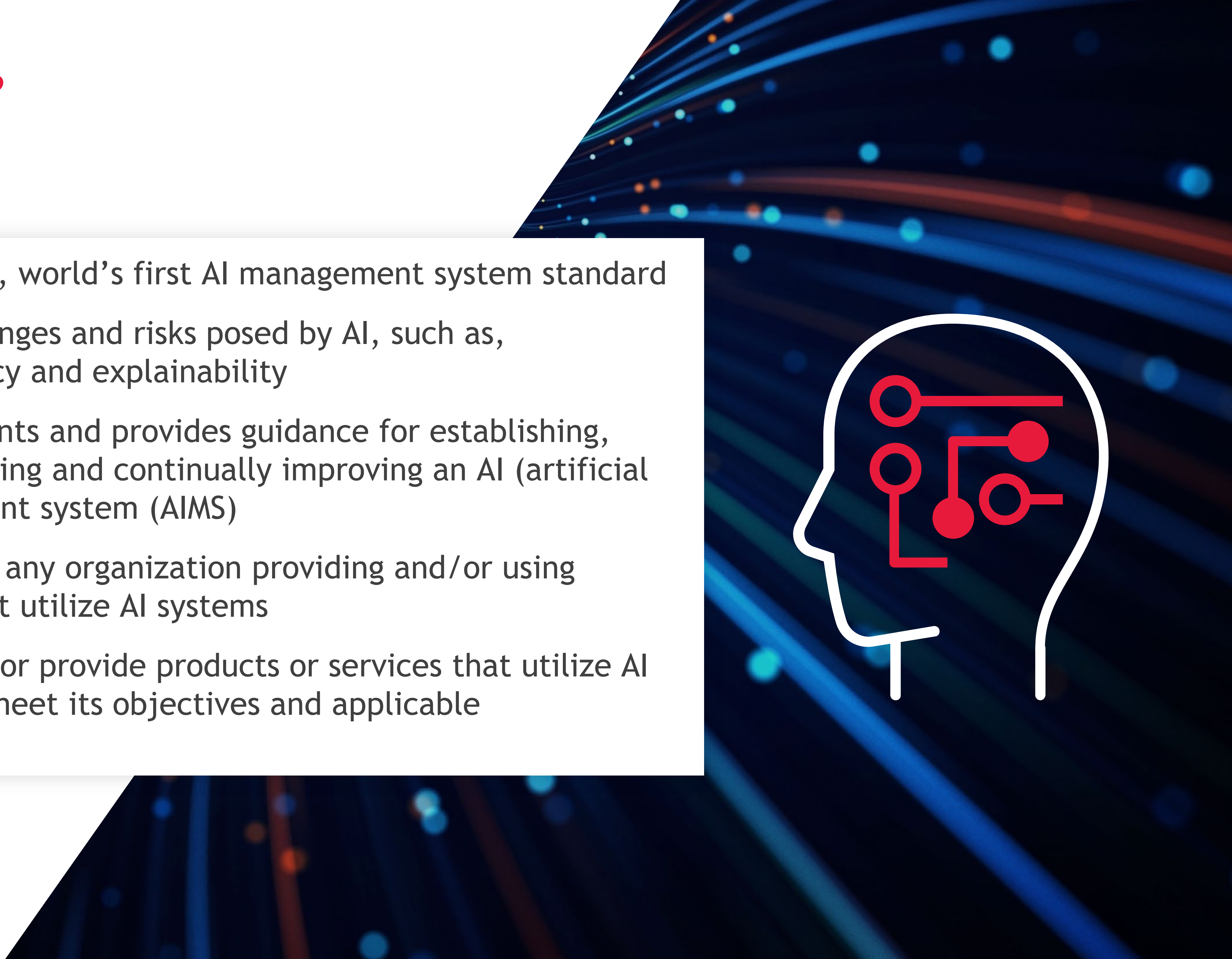
Key Requirements of the EU AI Act for Deployers of the High-risk AI Systems:

- Due Diligence in selecting an AI system provider
- Instruction for Use (Deployers must use the high-risk AI system according to the instruction for use.)
- Human Oversight
- Data Quality
- System Monitoring
- Data Protection Impact Assessment (may also apply)
- Recordkeeping (log retention according to local laws and regulations)
- Transparency and Notice
- Cooperation with Applicable Authorities

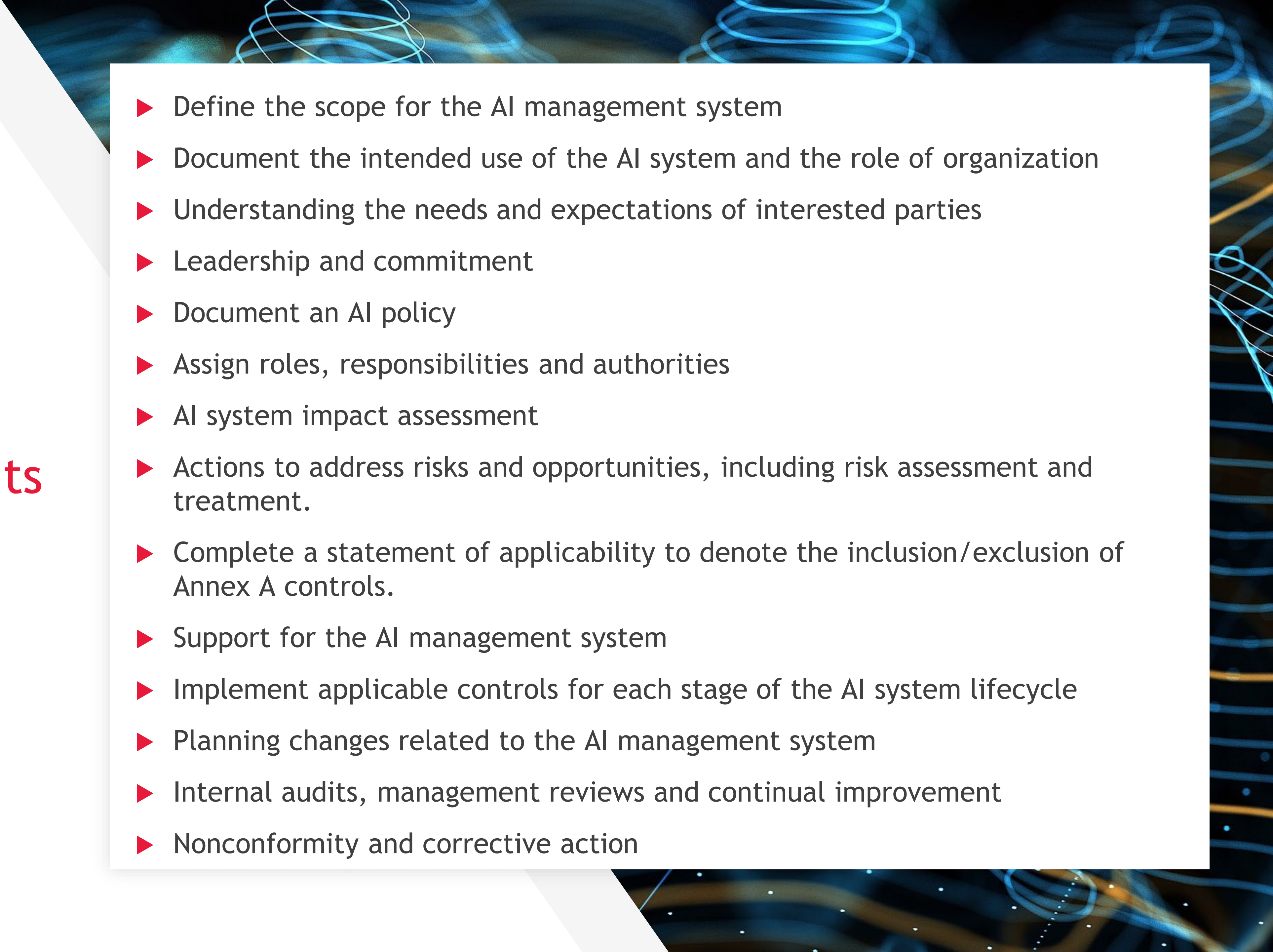
https://www.isaca.org/resources/white-papers/2024/understanding-the-eu-ai-act#f24

What is ISO 42001?

- Introduced in Dec. 2023, world’s first AI management system standard
- Addresses unique challenges and risks posed by AI, such as, ethics/bias, transparency and explainability
- Specifies the requirements and provides guidance for establishing, implementing, maintaining and continually improving an AI (artificial intelligence) management system (AIMS)
- Can be implemented by any organization providing and/or using products or services that utilize AI systems
- Helps organizations use or provide products or services that utilize AI systems responsibly to meet its objectives and applicable requirements



ISO 42001 –
Key Requirements



- Define the scope for the AI management system
- Document the intended use of the AI system and the role of organization
- Understanding the needs and expectations of interested parties
- Leadership and commitment
- Document an AI policy
- Assign roles, responsibilities and authorities
- AI system impact assessment
- Actions to address risks and opportunities, including risk assessment and treatment.
- Complete a statement of applicability to denote the inclusion/exclusion of Annex A controls.
- Support for the AI management system
- Implement applicable controls for each stage of the AI system lifecycle
- Planning changes related to the AI management system
- Internal audits, management reviews and continual improvement
- Nonconformity and corrective action

Organizational vs. Systemic Risks for AI

ORGANIZATIONAL CONSIDERATIONS

- Complexity and relevance
- AI expertise
- Technology readiness
- Data governance
- Accountability and compliance

SYSTEMIC CONSIDERATIONS

- Model or use case level
- Technical aspects for safety and security
- Impact on users of the system - impact to individuals, groups, communities and organization
- Evaluate applicability and risks of AI principles

Data Governance Controls

Define and Implement Data Management Practices

- Data management practices to address topics like:
  - privacy and security implications due to the use of data;
  - accuracy and integrity of the data
  - transparency and explainability aspects including data provenance and the ability to provide an explanation of how data are used for determining an AI system's output; representativeness of training data compared to operational domain of use.

Data Acquisition and Preparation

- Implement processes for acquisition and selection of data used in AI systems
  - Data sources and categories of data
  - Characteristics of data source and attributes
  - Data cleansing
  - Data subject access rights

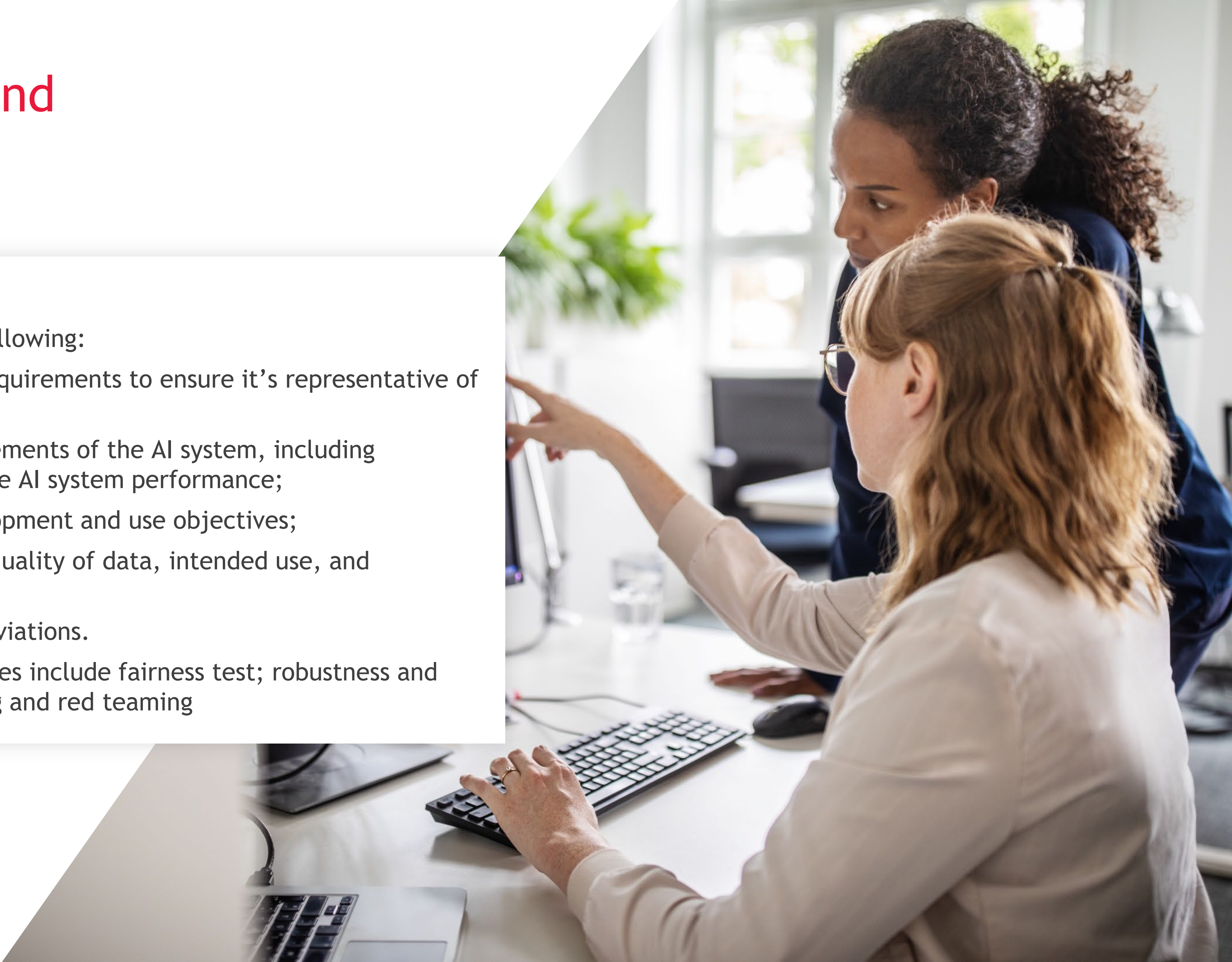
Data Quality

- Ensure data used in AI system lifecycle meets quality requirements
  - Consider impact of bias on system performance and system fairness
  - Training data is always representative of user population

Data Provenance

- Document a process for recording the provenance of data.
- Ensure transparency and accountability

Model Validation and Verification



AI System Testing

- Evaluation plan to cover the following:
  - Selection of test data and requirements to ensure it’s representative of the user base.
  - Reliability and safety requirements of the AI system, including acceptable error rates for the AI system performance;
  - Responsible AI system development and use objectives;
  - Operational factors such as quality of data, intended use, and sandboxing.
- Key metrics and acceptable deviations.
- Types of model testing strategies include fairness test; robustness and accuracy; adversarial AI testing and red teaming

Model Operations and Monitoring

AI System Deployment

- Document a deployment plan or checklist that ensures:
  - Verification and validation objectives including KPI are met
  - Human-in-the-loop

AI System Operations and Monitoring

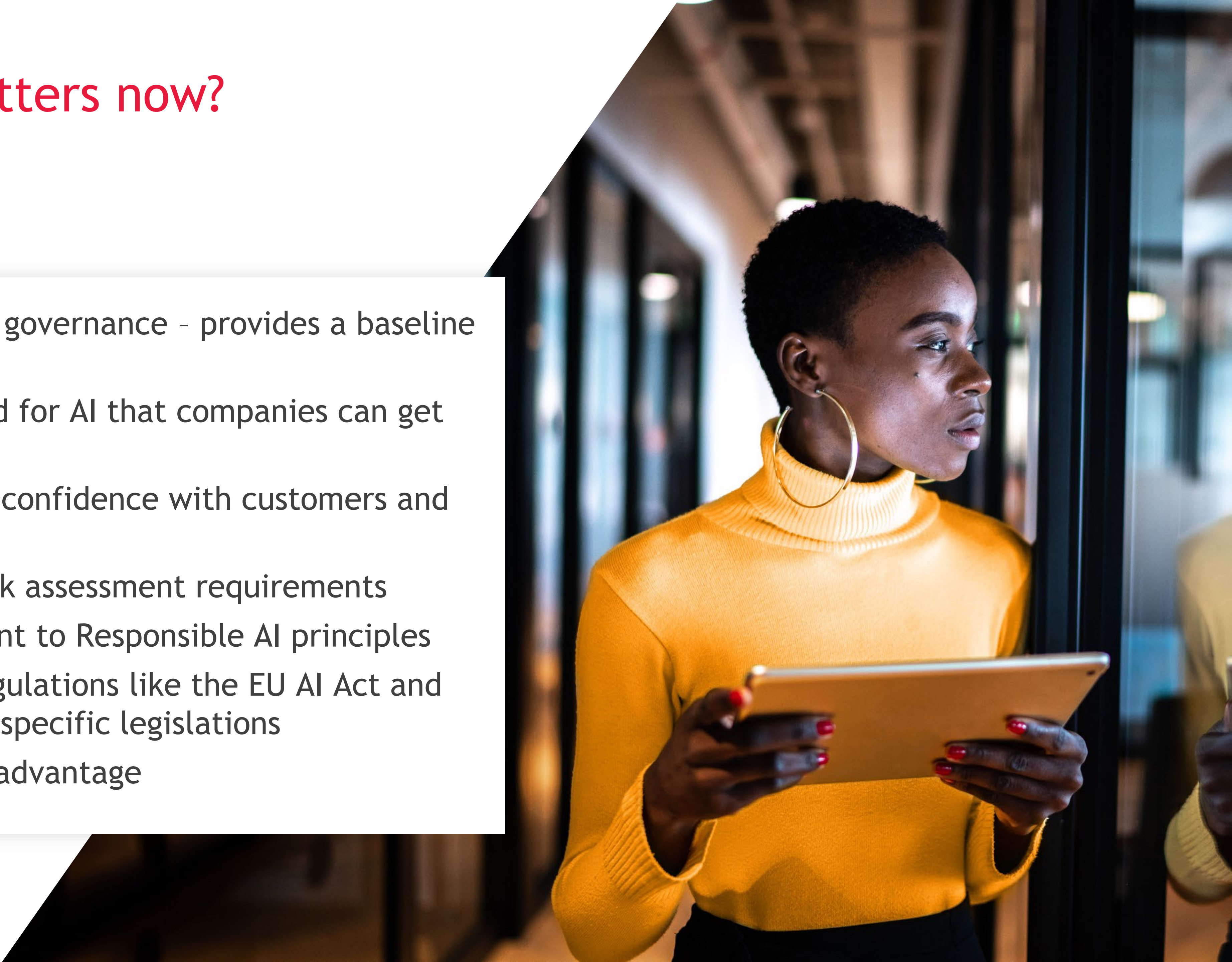
- Covers system and performance monitoring, repairs, updates and support
  - Monitor for general errors or failures
  - Monitor AI observability metrics like accuracy and precision of outputs; bias; data drift; explainability
  - Identify AI-specific information security threats like data poisoning, model inversion attacks, etc.
  - React and responds to alerts

AI System Logging

- Ensure logging of the AI system at various phases to enable traceability and facilitate troubleshooting

Why ISO 42001 matters now?

- The growing need for AI governance – provides a baseline framework
- First-of-its-kind standard for AI that companies can get certified with
- Build trust and increase confidence with customers and stakeholders
- Helps address vendor risk assessment requirements
- Demonstrate commitment to Responsible AI principles
- Helps respond to key regulations like the EU AI Act and other state and country specific legislations
- Leverage early adopter advantage



FAQs

What if the development of AI systems is outsourced to a third-party?

- The ISO 42001 standard is applicable to both, developers and deployers of AI.
- The specific role of the organization is required to be documented as a part of the scope.
- Risk assessment and statement of applicability will help determine the applicable controls that would be applicable.

By implementing ISO 42001 controls, can we meet requirements of other AI regulations?

- Currently, ISO 42001 is the external facing certification available to companies to show how they have implemented their AI governance framework; the specific requirements of regulations must be mapped to the ISO 42001 controls to assess compliance.

How does BDO help with ISO 42001?

- The BDO TPA practice performs ISO 42001 readiness assessments and, certification audits.

Q&A

About BDO USA

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.