Adopt AI

Do not adopt its risks!

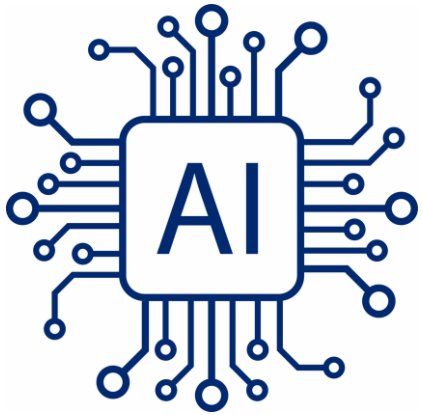
02/07/2024

AIQURIS

A TUV SUD Venture

Context

As AI becomes business critical, it is ever important to navigate AI risks and regulation



AI is transforming the Industry

AI is critical for businesses to stay competitive

Emerging AI risks and Regulation

- AI introduces unique risks with potentially severe and widespread consequences
- AI risks require robust additional risk and quality controls to mitigate
- Intensifying global regulatory activities compel organisations to enhance compliance

Yet many

- Have limited knowledge of the specific risks associated with AI
- Lack knowledge on how to effectively manage AI-related risks and quality
- Do not have a standardised process to manage AI systems from procurement to adoption

State of AI Report 2024

https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_AI-Index-Report-2024.pdf

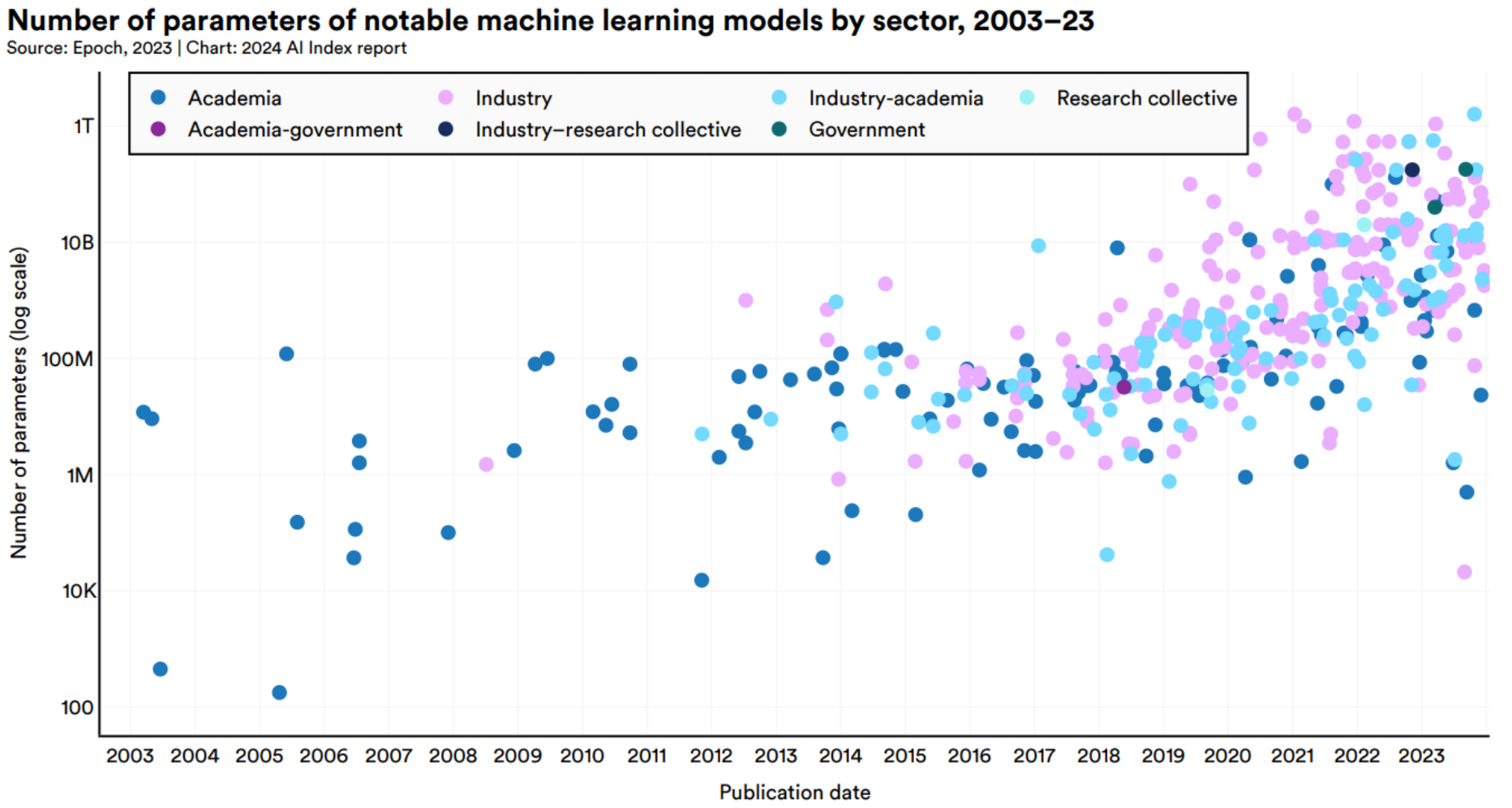
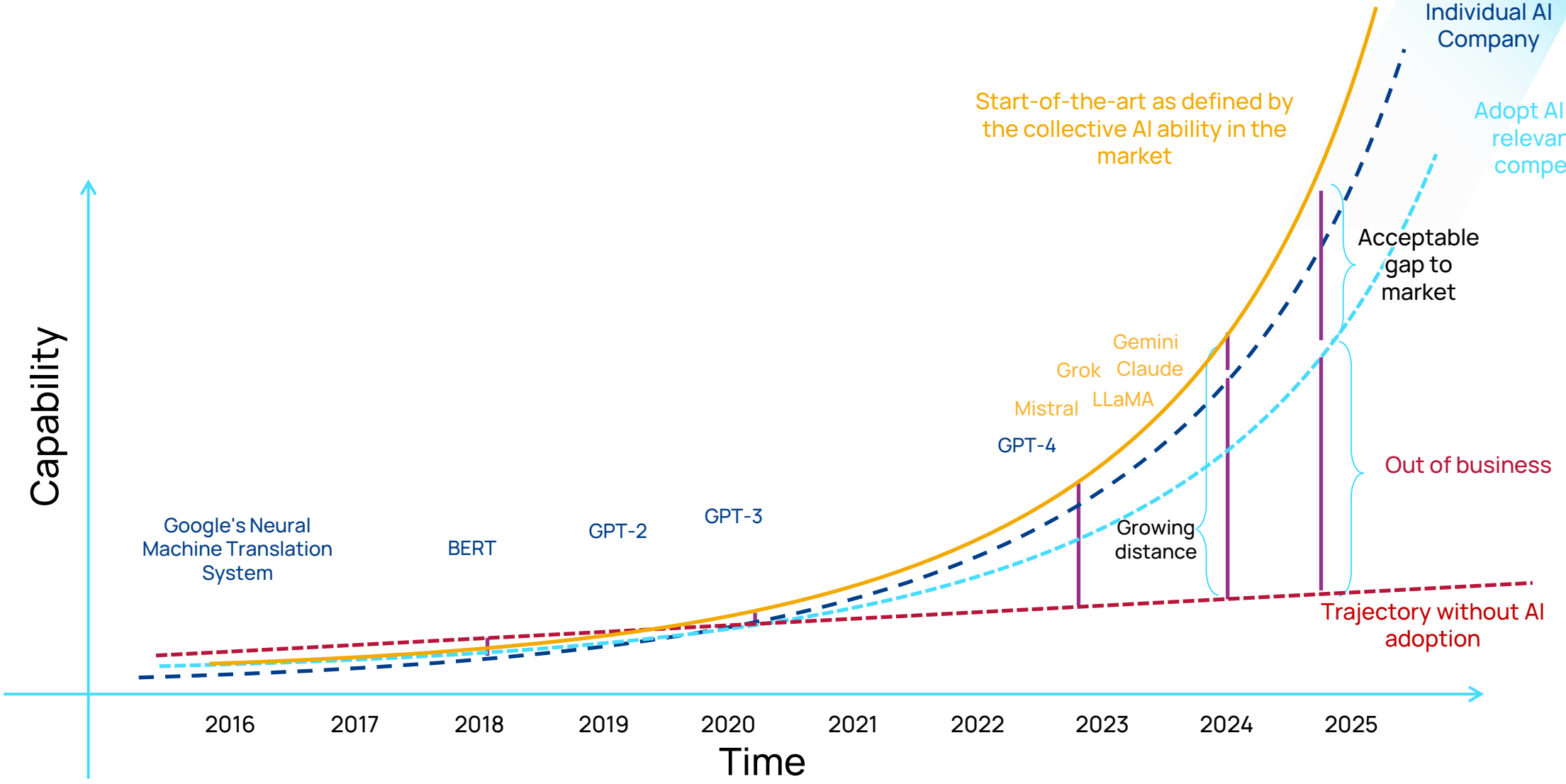


Figure 1.3.5

Business strategy



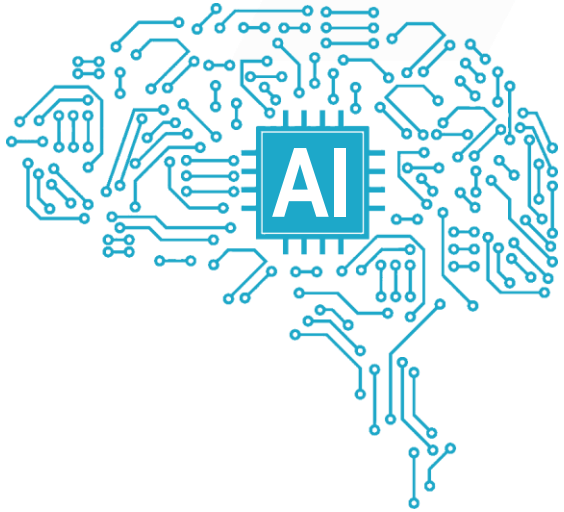
AI risks are different from traditional software and IT risks

AI risks are broader and more severe, but there is a lack of standardised approaches in managing these risks.

AI is different

Classic Software

≠



Understanding a system

Can we understand the building blocks?
Can we understand the composition?

Sources of risk

Technology

- Large input spaces
- Stochastic processes
- Large parameters spaces
- Numeric instability
- Oracle problem

Organizational

- Skills gap
- Challenges to accountability
- Compliance
- Lack of AI policy and efficient scaling strategy
- Stakeholder management

Data

- Inefficient data management and governance strategy
- Data quality issues
- Data usage issues
- Legal challenges

AI Model

- Black box decision-making
- Unwanted bias in prediction
- Concept drift
- Safety and security issues

Processes

- Poor AI lifecycle management
- Lack of controls
- Poor risk management
- Lack of validation and verification

Potential Consequences

Scale of potential consequences

Legal

Reputational

Monetary

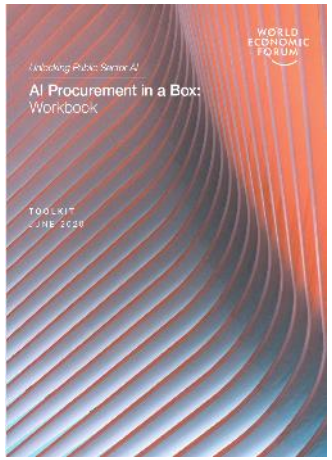
Business

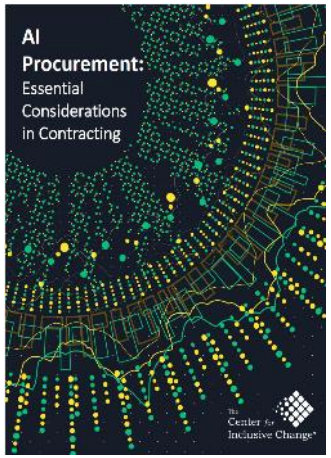
Environment

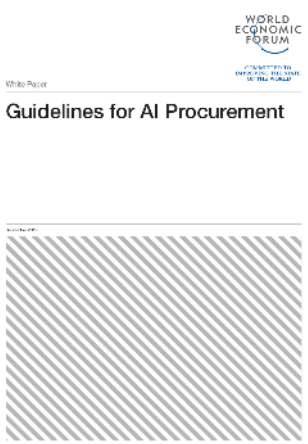
Society

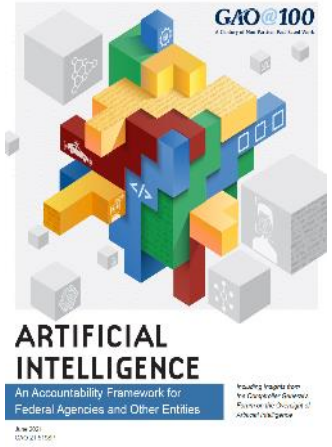
Complex landscape of frameworks, standards, and guidelines

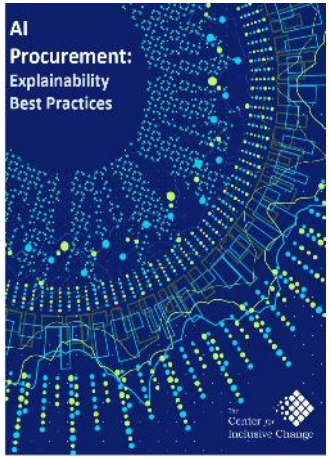
A daunting journey for organisations to navigate these complexities.

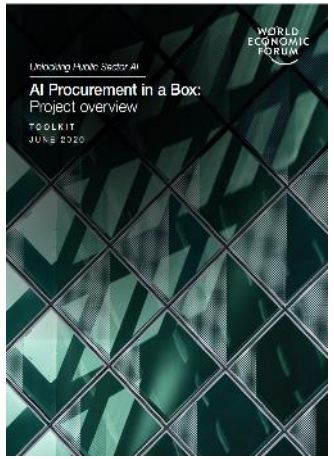


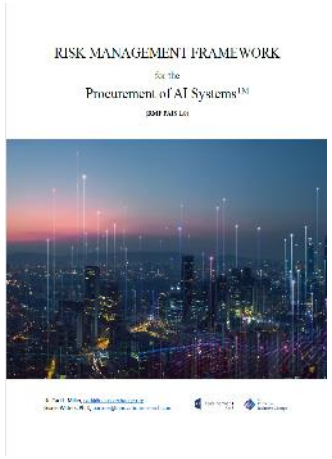


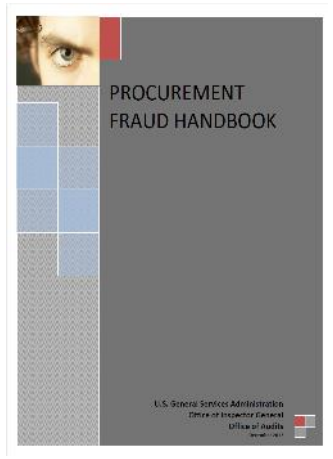


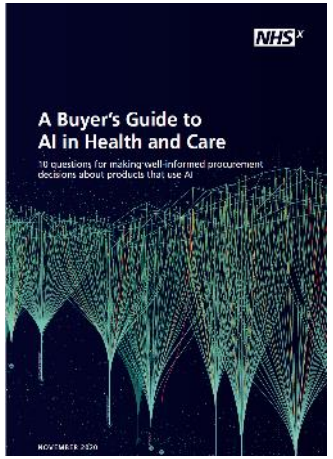












The Solution

Automated process to mitigate risks and qualify AI systems

Turn use cases into practical, scalable solutions that are compliant, meet high quality, and performance standards.

Seamless collaboration between functions
Users, Application Owners, Procurement, IT, Legal, Risk

- Use Case
- Client Situation
- Vendor and AI System

Input

Processing

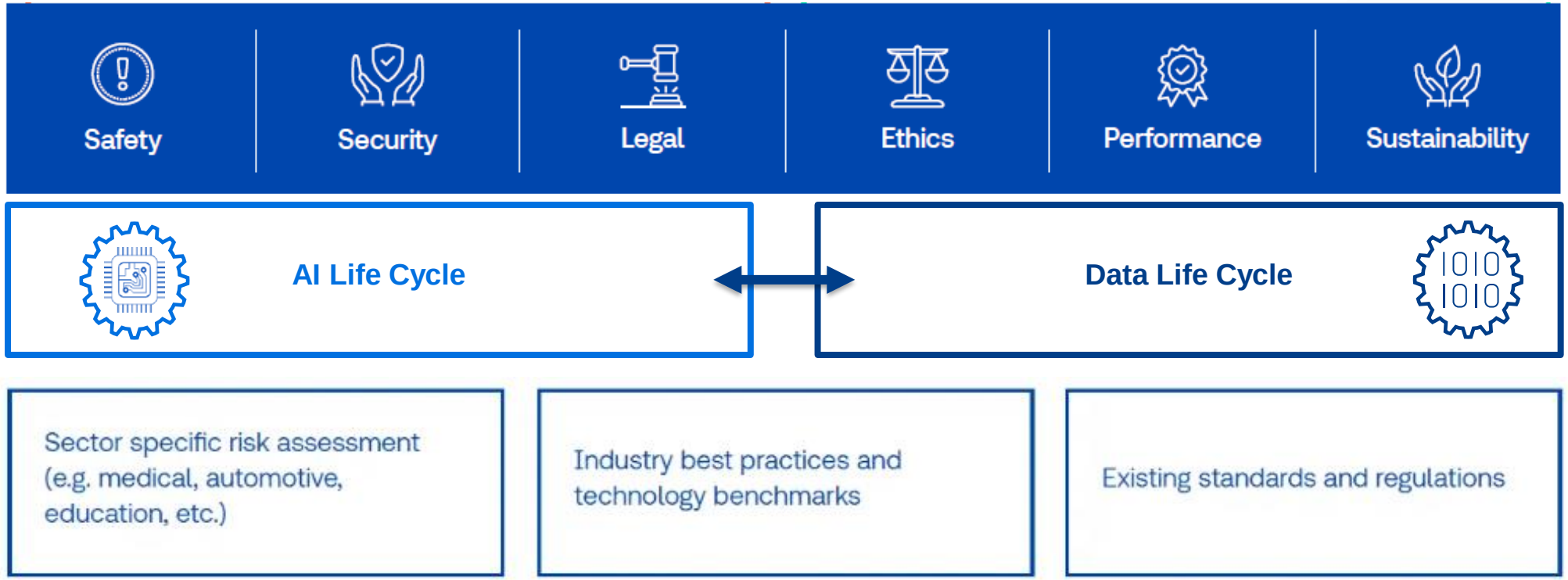
Intelligent engines select and assess relevant quality and risk mitigation controls

Solution

- Comprehensive Risk Profile
- RfI requirements
- Contractual Terms and Conditions

Dynamic Database
Codified Audit Expertise based on Standards, Regulations, Industry best practice

AI Quality Framework



AI Quality Profile

Safety

Has the AI system the potential to directly or indirectly harm anyone/anything?

- Predictability
- Testability
- Traceability
- ...

Legal

Is the AI system and usage compliant with regulations?

- Obligations
- Governance
- Auditability
- ...

Performance

Is the AI system fit for use, accurate, precise and robust?

- Suitability
- Efficiency
- Reliability
- ...

Security

Does the AI system increase cybersecurity risks?

- Confidentiality
- Authenticity
- Recoverability
- ...

Ethics

Does it violate accepted ethical principles for impacted stakeholders?

- Transparency
- Non-discrimination
- Accountability
- ...

IEEE CERTIFAIED AI ETHICS

Sustainability

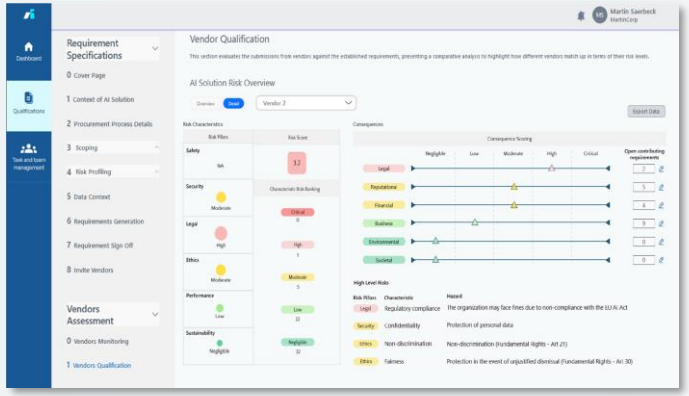
Has the development or operation been conducted with environmental considerations?

- Resource footprint
- Proportionality
- Reusability
- ...

Outcome of the AIQURIS platform

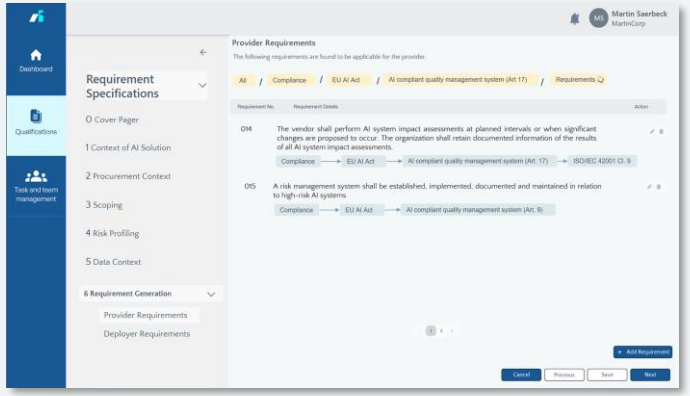
AIQURIS identifies and quantifies all relevant risks associated with AI use cases

Comprehensive risk assessment



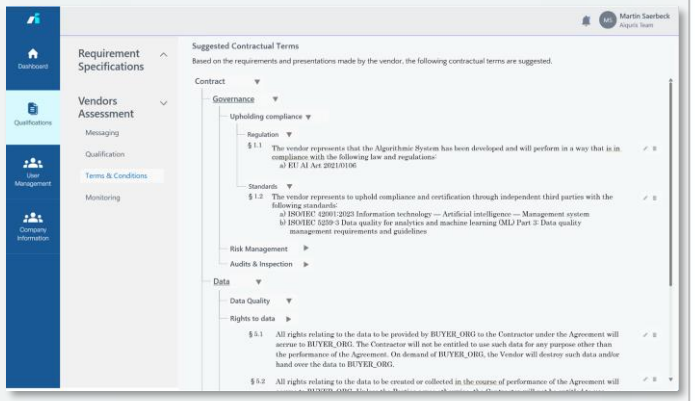
Detailed and quantified risk profile of the use case and its provider enables companies to understand and mitigate potential vulnerabilities and threats.

Specific Requirement Specification



Concrete RfI requirements allow companies to make informed decisions when selecting AI providers.

Intelligent Qualification



Tailored terms and conditions that address specific risks and compliance requirements ensure legal and operational safeguards.

ISO/IEC JTC 1/SC 42

Explanatory notes:

JTC: Joint Technical Committee
SC: Subcommittee
WG: Working Group
JWG: Joint Working Group
TC: Technical Committee
TR: Technical Report

ISO JTC 1 IEC
INFORMATION TECHNOLOGY STANDARDS

WG 1: Foundational Standards

ISO/IEC 42001 Artificial Intelligence – Management System
ISO/IEC 42005 AI system impact assessment
ISO/IEC 42006 Requirements for bodies providing audit and certification of artificial intelligence management systems

ISO/IEC 22989:2022 Artificial intelligence concepts and terminology
ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) systems using Machine Learning (ML)

WG 2: Data

ISO/IEC 5259-x Data quality for analytics and ML
- **5259-1** – Overview, terminology, and examples
- **5259-2** – Data quality measures
- **5259-3** – Data quality management requirements and guidelines
- **5259-4** – Data quality process framework
- **5259-5** – Data quality governance
- **TR 5259-6** Visualization framework for data quality

ISO/IEC 8183 – Data lifecycle framework
ISO/IEC TR 42103 Overview of synthetic data in the context of AI systems

ISO/IEC 24668:2022 Process management framework for big data analytics
ISO/IEC 20546:2019 Information technology — Big data — Overview and vocabulary
ISO/IEC TR 20547-1:2020 Information technology — Big data reference architecture — Part 1: Framework and application process
ISO/IEC TR 20547-2:2018 Information technology — Big data reference architecture — Part 2: Use cases and derived requirements
ISO/IEC 20547-3:2020 Information technology — Big data reference architecture — Part 3: Reference architecture
ISO/IEC TR 20547-5:2018 Information technology — Big data reference architecture — Part 5: Standards roadmap

WG 3: Trustworthiness

ISO/IEC 24029-2 Assessment of the robustness of neural networks - Part 2: Methodology for the use of formal methods
ISO/IEC 23894 Risk Management
ISO/IEC TR 5469 Functional safety and AI systems
ISO/IEC 25059 (SQuaRE) Quality model for AI systems
ISO/IEC TS 25058 (SQuaRE) Guidance for quality evaluation of AI systems
ISO/IEC TS 6254 Explainable AI
ISO/IEC 5471 Quality evaluation guidelines for AI systems
ISO/IEC 6254 Objectives and approaches for explainability of ML models and AI systems
ISO/IEC 8200 Controllability of automated artificial intelligence systems
ISO/IEC 12791 Treatment of unwanted bias in classification and regression machine learning tasks
ISO/IEC TS 12792 Transparency taxonomy of AI systems
ISO/IEC TS 6254 Objectives and approaches for explainability of ML models and AI systems
ISO/IEC TR 42106 Overview of differentiated benchmarking of AI system quality characteristic

ISO/IEC 23894:2023 Guidance on risk management
ISO/IEC TR 24028:2020 Overview of trustworthiness in artificial intelligence
ISO/IEC TR 24027:2021 Bias in AI systems and AI aided decision making
ISO/IEC TR 24029-1:2021 Assessment of the robustness of neural networks – Part 1: Overview
ISO/IEC TR 24368:2022 Overview of ethical and societal concerns

WG 4: Use cases and applications

ISO/IEC 5338 AI system lifecycle processes
ISO/IEC 5339 Guidelines for AI applications
ISO/IEC TR 24030 Artificial intelligence (AI) — Use cases
ISO/IEC TR 21221 Beneficial AI systems
ISO/IEC TR 20226 Environmental sustainability aspects of AI systems

ISO/IEC TR 24030:2021 Artificial Intelligence: Use cases

WG 5: Computational Approaches and Computational Characteristics of AI Systems

ISO/IEC 5392 Reference architecture of knowledge engineering
ISO/IEC TR 17903 Overview of machine learning computing devices

ISO/IEC TS 4213:2022 Assessment of machine learning classification performance
ISO/IEC TR 24372:2021 Overview of computational approaches for AI systems

JWG 3 (TC215): AI enabled health informatics

ISO/IEC TR 18988 Application of AI technologies in health informatics

JWG 1 (SC40): Governance of AI

ISO/IEC 38507:2022 Governance implications of the use of artificial intelligence by organisations

JWG 2 (SC7): Testing of AI-based Systems

ISO/IEC TS 29119-11 Software testing — Part 11: Testing of AI systems
ISO/IEC TS 17847 Verification and validation analysis of AI systems

Selected IEEE Standards

IEEE 2089:2021	Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children	https://ieeexplore.ieee.org/document/9627644
IEEE 2247.3	Recommended Practices for Evaluation of Adaptive Instructional Systems	https://standards.ieee.org/ieee/2247.3/7523/
IEEE 2802-2022	Standard for Performance and Safety Evaluation of Artificial Intelligence Based Medical Devices: Terminology	https://standards.ieee.org/ieee/2802/7460/
IEEE 2807.4	Guide for Scientific Knowledge Graphs	https://standards.ieee.org/ieee/2807.4/10571/
IEEE 2817	Guide for Verification of Autonomous Systems	https://standards.ieee.org/ieee/2817/7644/
IEEE 2841-2022	Recommended Practice for Framework and Process for Deep Learning Evaluation	https://standards.ieee.org/ieee/2841/7674/
IEEE 2894-2024	Guide for an Architectural Framework for Explainable Artificial Intelligence	https://standards.ieee.org/ieee/2894/11296/
IEEE 2959	Standard for Technical Requirements of Standard-Oriented Knowledge Graphs	https://standards.ieee.org/ieee/2959/10372/
IEEE 2986-2023	Recommended Practice for Privacy and Security for Federated Machine Learning	https://standards.ieee.org/ieee/2986/10564/
IEEE 3110	Standard for Computer Vision (CV) - Technical Requirements for Algorithms Application Programming Interfaces (APIs) of Deep Learning Framework	https://standards.ieee.org/ieee/3110/11253/
IEEE 3123	Standard for Artificial Intelligence and Machine Learning (AI/ML) Terminology and Data Formats	https://standards.ieee.org/ieee/3123/10744/
IEEE 3156-2023	Standard for Requirements of Privacy-Preserving Computation Integrated Platforms	https://standards.ieee.org/ieee/3156/10834/
IEEE 3157	Recommended Practice for Vulnerability Test for Machine Learning Models for Computer Vision Applications	https://standards.ieee.org/ieee/3157/10876/
IEEE 7000:2021	Standard Model Process for Adressing Ethical Concerns during System Design	https://ieeexplore.ieee.org/document/9536679
IEEE 7001:2021	Standard for Transparency of Autonomous Systems	https://ieeexplore.ieee.org/document/9726144
IEEE 7002:2022	Standard for Data Privacy Process	https://ieeexplore.ieee.org/document/9760247
IEEE 7003	Algorithmic Bias Considerations	https://standards.ieee.org/ieee/7003/11357/
IEEE 7004	Standard for Child and Student Data Governance	https://standards.ieee.org/ieee/7004/10270/
IEEE 7005:2021	Standard for Transparent Employer Data Governance	https://ieeexplore.ieee.org/document/9618905
IEEE 7007:2021	Ontological Standard for Ethically Driven Robotics and Automation Systems	https://ieeexplore.ieee.org/document/9611206
IEEE 7008	Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems	https://standards.ieee.org/ieee/7008/7095/
IEEE 7009	Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems	https://standards.ieee.org/ieee/7009/7096/
IEEE 7010:2020	Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being	https://ieeexplore.ieee.org/document/9084219
IEEE P2807.1	Standard for Technical Requirements and Evaluation of Knowledge Graphs	https://ieeexplore.ieee.org/document/10416975
IEEE P2840	Standard for Responsible AI Licensing	https://standards.ieee.org/ieee/2840/7673/
IEEE P2863	Recommended Practice for Organizational Governance of Artificial Intelligence	https://standards.ieee.org/ieee/2863/10142/

Medical use case on AIQURIS platform

The Application

Hospital wants to purchase AI-based expert system for mental health diagnosis.

The Product

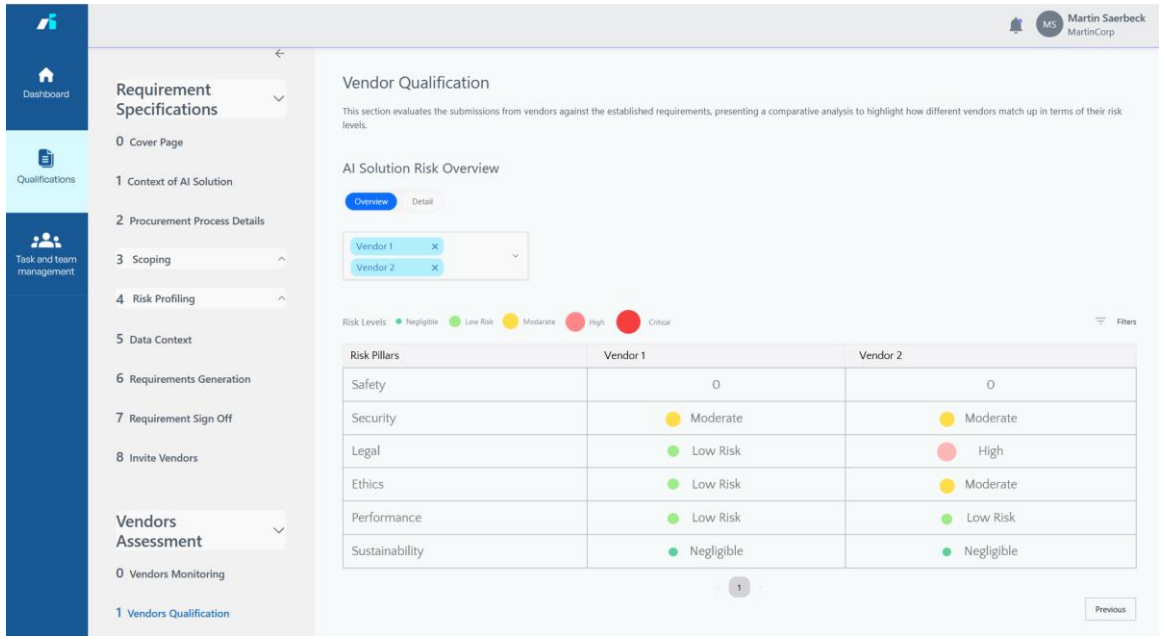
In-situ and ambulatory epilepsy spike and seizure detection interpretation and analysis

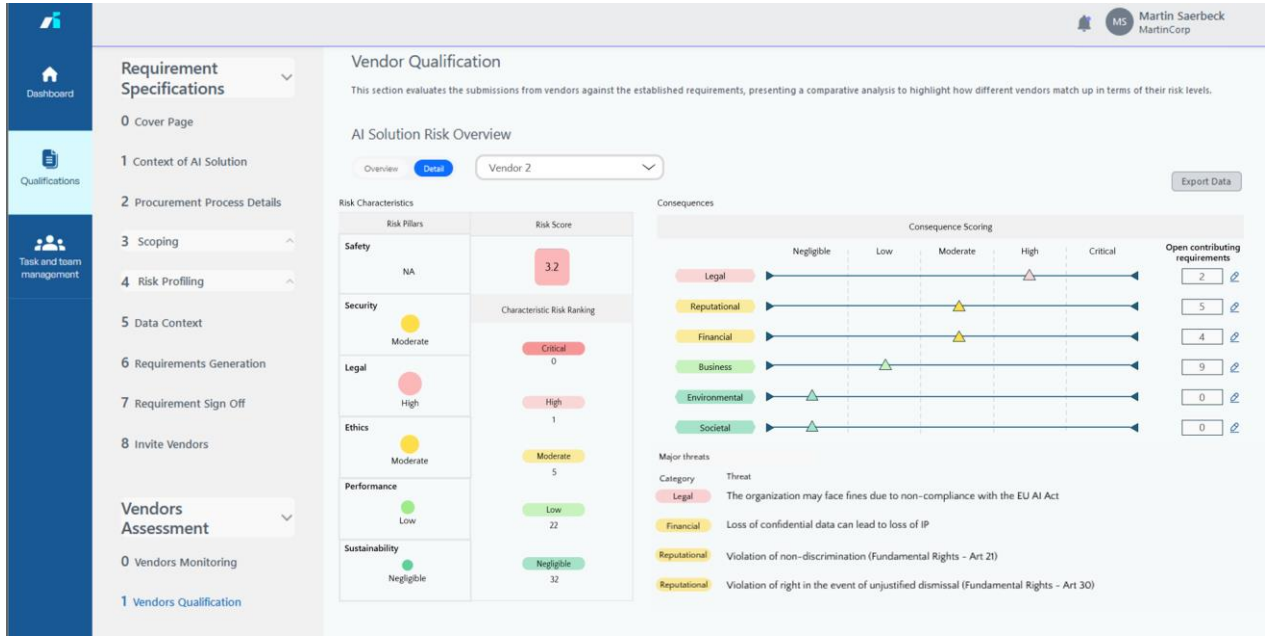
Remote ICU monitoring of non-convulsive seizures and slowing

The Challenge

The procurement department lacks knowledge of qualifying vendors.

Qualification Results





(for illustration only)

Summary

AI is reshaping industry

AI risks are more complex than for classical software

Risk mitigation starts with procurement of AI

Quality management is required across the life cycle

AI legislation is being enforced

Platform based solutions can automate risk and compliance management

THANK YOU!

Book a demo

DR. ANDREAS HAUSER
CEO
andreas.hauser@aiquris.com

DR. MARTIN SAERBECK
CTO
martin.saerbeck@aiquris.com