AI Governance Framework

EQUAL EXPERTS

AI GOVERNANCE FRAMEWORK

AI adoption challenges facing enterprises

We see several common challenges facing organisations in adopting AI.

1 Lack of strategy

Lack of strategic vision and roadmap detailing the solutions and resources needed to deliver business value

2 Time to value

Lack of use case prioritisation approach and standard ROI model results in unclear investment priorities

3 Complexity in scaling

Complexity around model fine-tuning and lack of curated use cases slow down deployment and increase timelines and costs

4 Security and responsibility

Data security and privacy, IP infringement concerns coupled with quality of output concerning erroneous facts and hallucinations

5 Too much choice

Thousands of public AI and open-source private AI models makes it difficult to choose the right platform and model that is future-proofed for their requirements

AI GOVERNANCE FRAMEWORK

AI is more than just adopting technology

AI requires a holistic approach across four essential areas.

Strategy and transformation

Align AI strategy with business strategy

Get executive buy-in and leadership

Focus on tangible results

Innovation and technology

Parallel investments in core IT

Embrace complementary technologies

Prioritise scalability

People and culture

Address the skills gap

Promote a culture of learning and data-driven decision-making

Democratise AI through employee enablement

Ethics, safety and sustainability

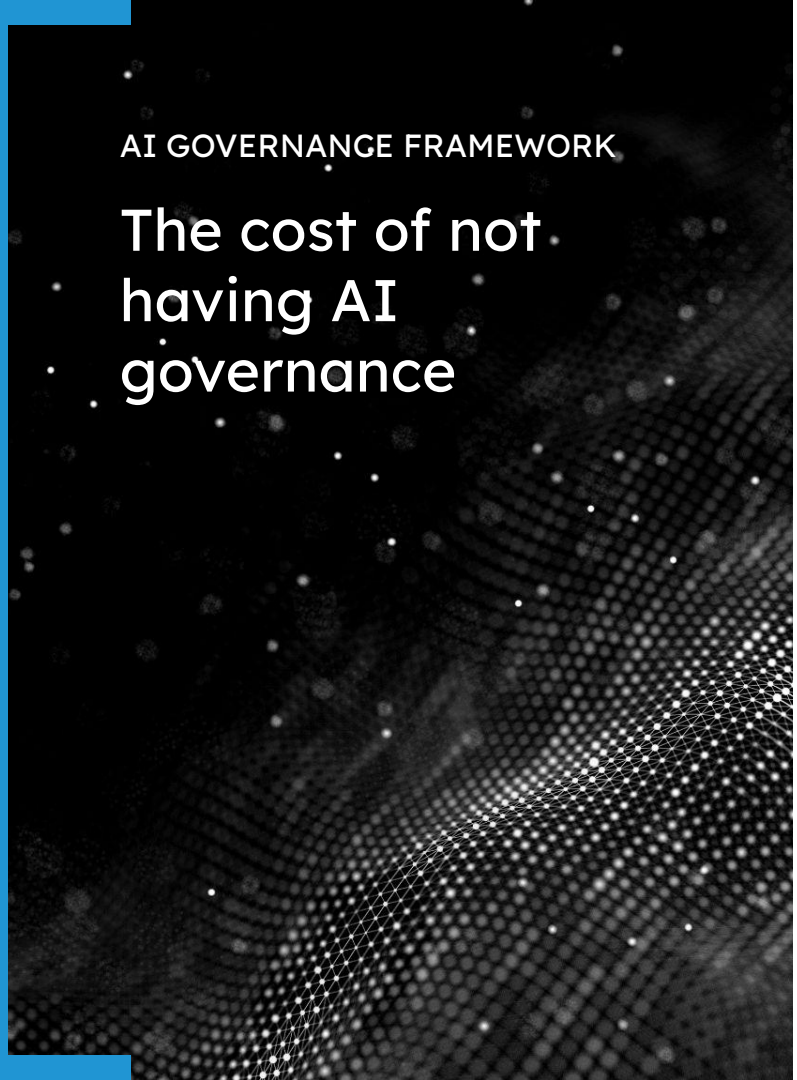
Establish clear ethical and AI safety frameworks

Prioritise data governance

Address sustainability concerns

AI GOVERNANCE FRAMEWORK

The cost of not having AI governance



Ethical concerns

Without proper governance, AI systems can perpetuate biases and discrimination, leading to ethical issues and potential harm to individuals.

Regulatory Compliance

Organisations may struggle to comply with varying AI regulations across different jurisdictions, risking legal penalties and reputational damage.

Data privacy and security

Lack of governance can result in inadequate data protection measures, increasing the risk of data breaches and misuse of sensitive information.

Transparency and accountability

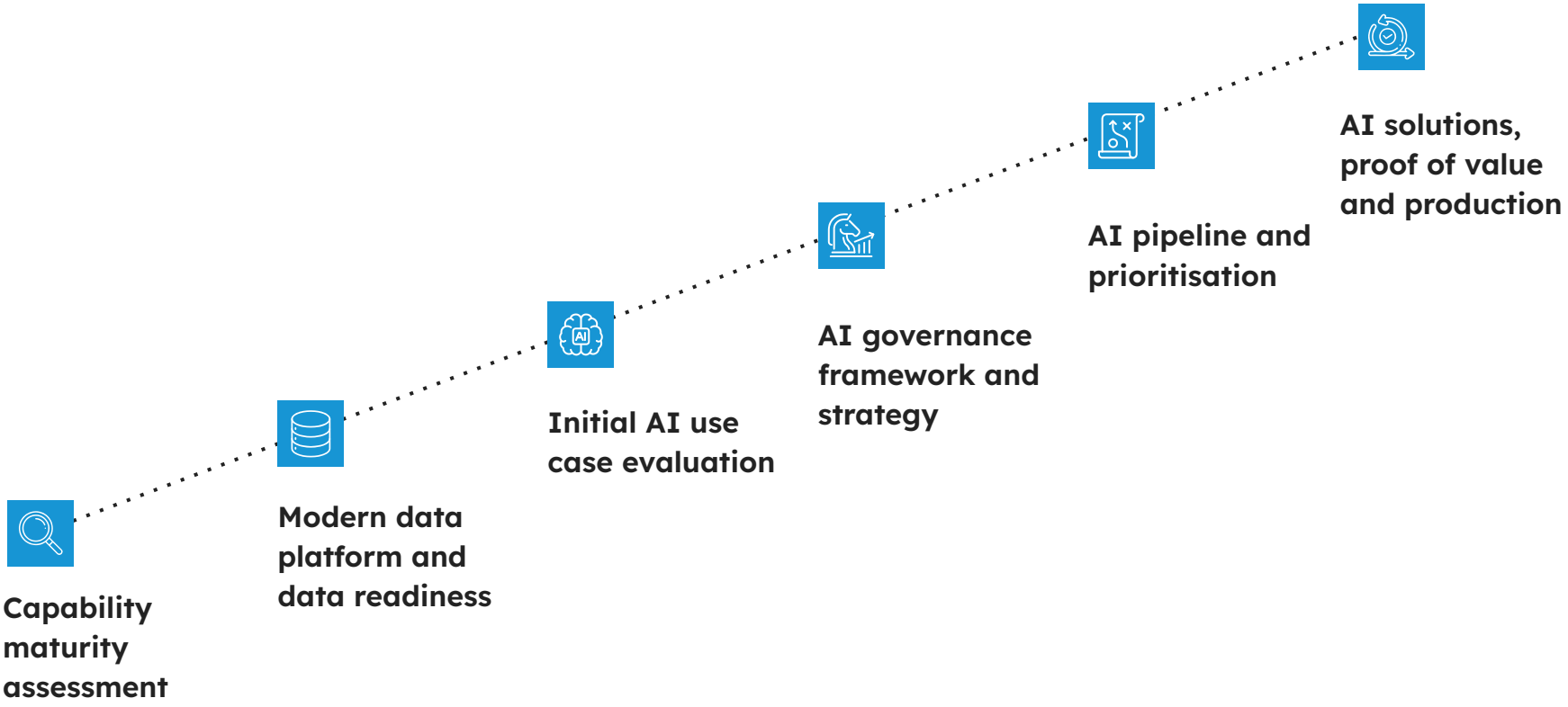
Without clear governance, it becomes difficult to ensure the transparency and explainability of AI algorithms, which can erode trust among stakeholders.

Operational risks

Inconsistent or absent governance can lead to operational inefficiencies, such as unreliable AI outputs and difficulties in managing third-party AI technologies.

AI GOVERNANCE FRAMEWORK

The enterprise AI journey



AI Governance Framework

A comprehensive framework integrating secure AI, ethics, governance, accountability, transparency, and excellence in Data Quality, providing organisations with a robust structure for responsibly and securely navigating the realms of artificial intelligence.

Component	Subcomponents	Objective	Guidelines
Organisation roles and structures	• AI Governance Board • AI Ethics Committee • AI Development Teams • AI Risk Management Team	Ensure clear roles and responsibilities for AI governance and ethical oversight.	• Establish and maintain governance bodies • Define roles and responsibilities • Conduct regular meetings and reviews
Operating model	• AI Policy Framework • AI Implementation Guidelines	Establish a structured approach for AI deployment and management.	• Create and enforce policy frameworks • Provide implementation guidelines
Risk, compliance and security	• Risk Assessment • Compliance Monitoring • Security Protocols • Incident Response	Mitigate risks, ensure compliance with regulations, and maintain security.	• Conduct regular risk assessments • Monitor compliance continuously • Implement and update security protocols • Develop incident response plans
Data management	• Data Governance • Data Quality Management • Data Privacy • Data Access Controls	Ensure the integrity, quality, and privacy of data used in AI systems.	• Establish data governance policies • Monitor and improve data quality • Ensure data privacy compliance • Implement access controls
Tools and technologies	• AI Development Platforms • AI Monitoring Tools • AI Security Tools	Provide the necessary tools and technologies for effective AI development and monitoring.	• Select and maintain development platforms • Implement monitoring tools • Ensure security tools are up-to-date
AI lifecycle	• AI Design & Development • AI Adoption • AI Deployment • AI Maintenance	Manage the entire lifecycle of AI systems from design to deployment and maintenance.	• Follow best practices for AI design • Develop and test AI models • Deploy AI systems • Maintain and update AI systems
Monitoring	• Performance Monitoring • Ethical Monitoring • Compliance Monitoring	Continuously monitor AI systems to ensure they meet performance, ethical, and compliance standards.	• Implement performance monitoring • Conduct ethical reviews • Ensure ongoing compliance monitoring

AI GOVERNANCE

Roles and structure

Implementation of a robust AI governance structure in line with strategic oversight on AI program of work, day-to-day governance and the technical oversight required to implement AI at scale, while ensuring alignment with risk management posture.

Strategic leadership

Enterprise Risk Function

Responsible for approving high risk use cases.

AI Council

Assesses and approves AI initiatives for implementation based on the accrued value and benefits to the enterprise. Reviews performance of completed projects.

AI working group

A forum to discuss AI-related issues between various divisions of the company.

Operational governance

AI Lead

Resource allocated to coordinate the operational activities of the broader AI program of work.

Technical oversight

Architecture Review Board

Provides guidance on use of various AI architecture patterns to be used for solution development purposes.

Enterprise Architect (AI)

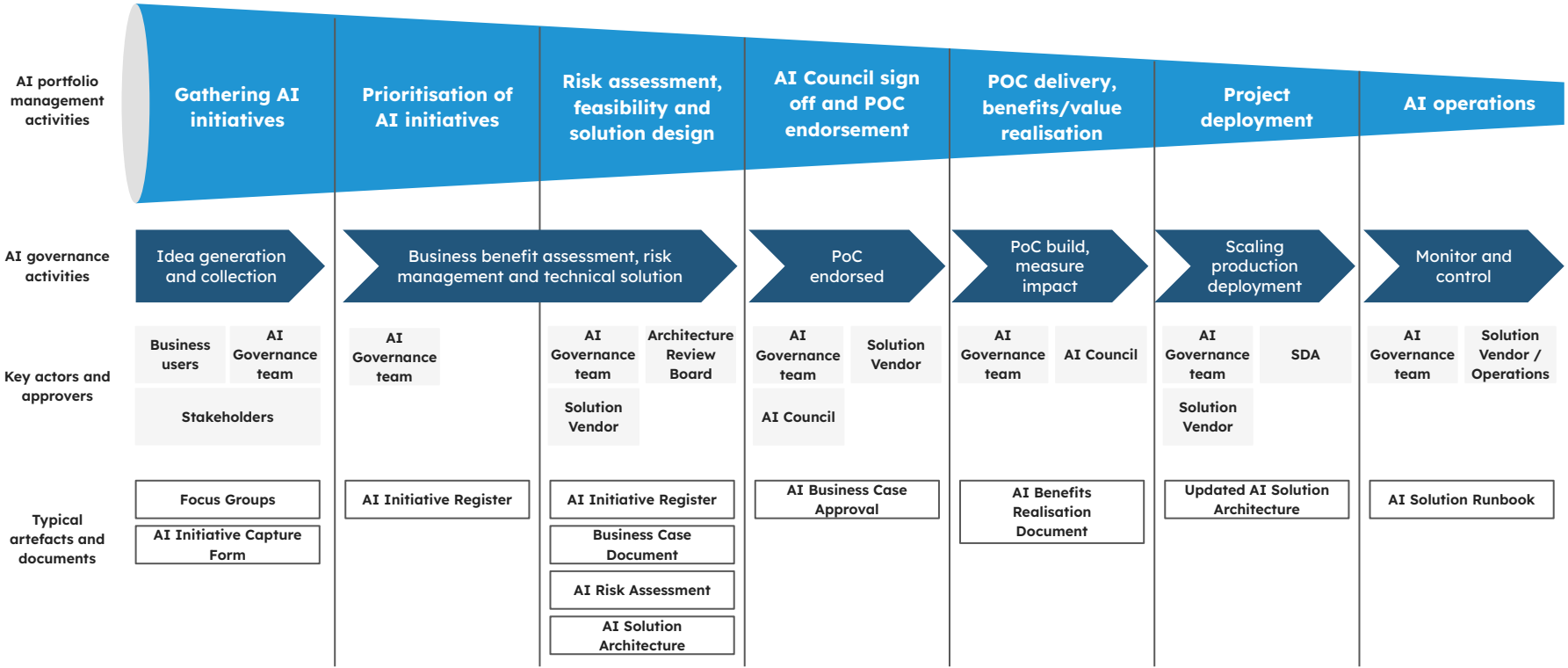
Provides technical due diligence on solution design and technical risk profile of AI projects being undertaken.

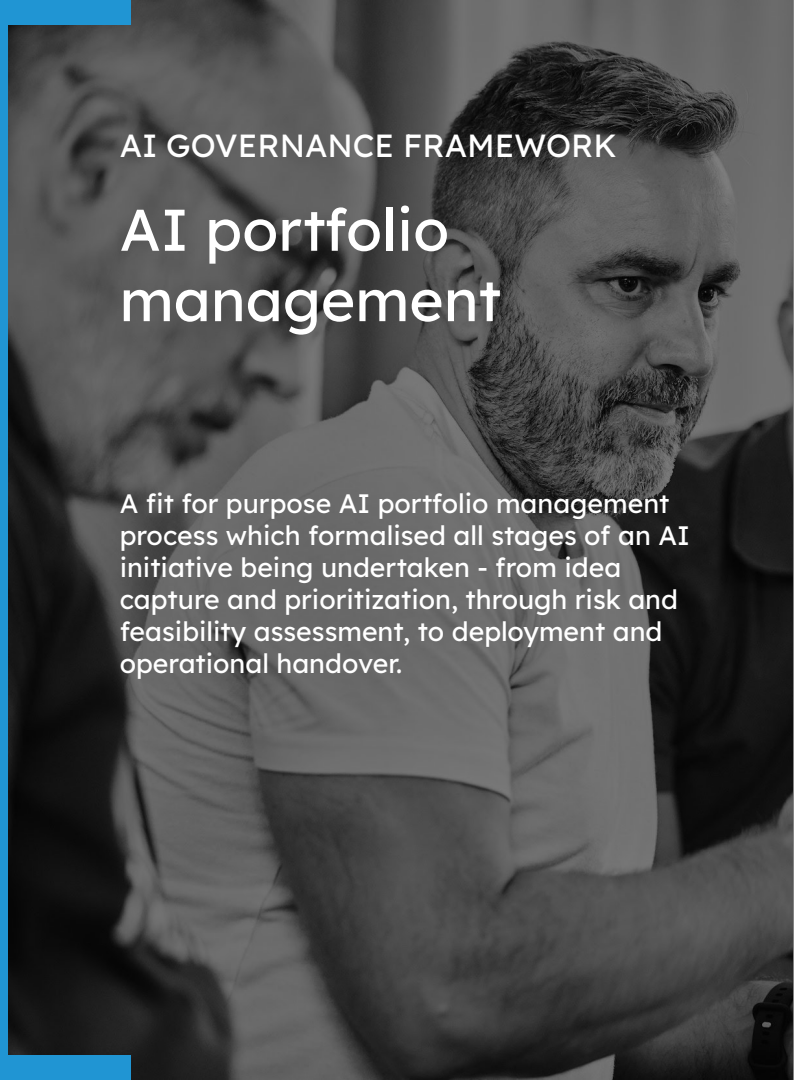
What does it mean in context?

- Establish governance layers with clear responsibility
- Formalise risk and compliance oversight in context of AI
- Establish a standard mechanism for prioritising AI initiatives based on value
- Technical due diligence for each proof of concept and solution
- Measure and report value delivered through the use of AI

AI GOVERNANCE FRAMEWORK

High level AI stage gates





AI GOVERNANCE FRAMEWORK

AI portfolio management

A fit for purpose AI portfolio management process which formalised all stages of an AI initiative being undertaken - from idea capture and prioritization, through risk and feasibility assessment, to deployment and operational handover.

Initiative capture and initial prioritisation

Systematically gather AI initiative ideas from across the business and prioritize them based on strategic alignment, potential value, and feasibility.

Risk assessment, technical feasibility and business case

Evaluate each initiative for business benefits, risks (including ethical and compliance risks), and technical feasibility. Develop a robust business case to justify investment.

Initiative funding approval

Secure funding for prioritized initiatives through a formal approval process, ensuring resource allocation aligns with business priorities

Proof of Concept (PoC) delivery and benefits measurement

Deliver a PoC to validate the solution's value and technical approach. Measure and document the benefits achieved against initial objectives.

Decision gate to productionise or discard solution

Assess PoC outcomes and decide whether to scale the solution into production or discontinue the initiative based on value realization.

Handover to AI Operations

Transition successful AI solutions to operational teams for ongoing management, monitoring, and continuous improvement.

AI GOVERNANCE FRAMEWORK

AI risk management methodology

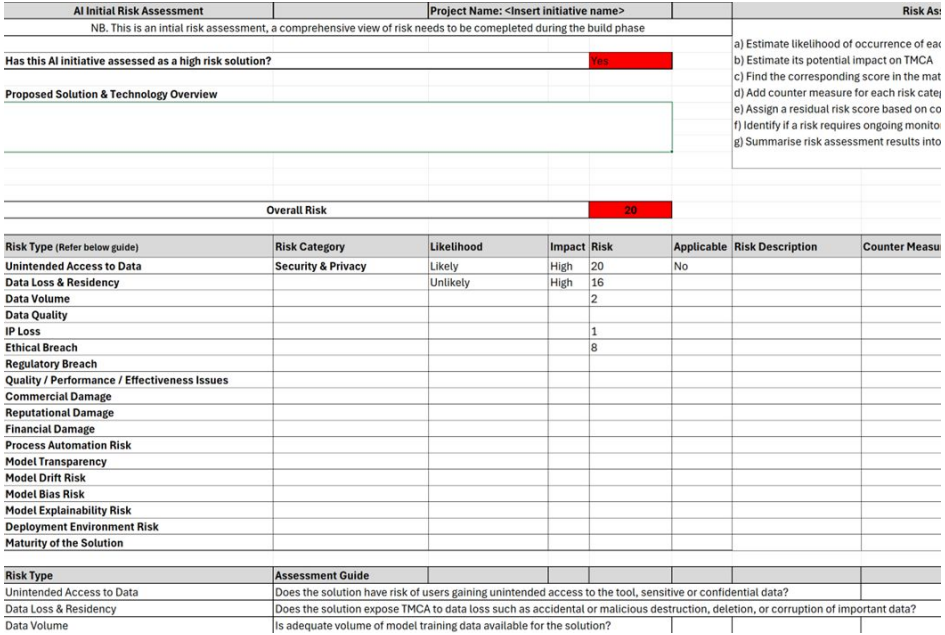
ISO 23897-aligned risk management methodology providing a robust, structured framework for identifying, assessing, and managing the unique risks associated with AI solutions.

Key features

- Structured, step-by-step risk assessment process (Identify → Analyse → Treat → Monitor)
- Covers all major AI risk categories: Security & Privacy, Data Management, Compliance, Business Impact, Model Risks, Technical Implementation
- Uses standardised likelihood and impact scales for consistent risk scoring
- Provides clear risk treatment options: Accept, Mitigate, Transfer, Avoid
- Calculates and documents residual risk after controls are applied
- Flags risks requiring ongoing monitoring throughout the AI lifecycle
- Integrates with business case documentation for governance and decision-making
- Comprehensive documentation and audit trail for each assessment step

Benefits

- Ensures thorough and repeatable assessment of AI-specific risks
- Supports regulatory compliance and responsible AI deployment
- Enhances transparency, stakeholder trust, and decision-making
- Proactively identifies and manages potential harms (ethical, legal, reputational, financial)
- Facilitates continuous improvement and lifecycle monitoring



AI Initial Risk Assessment		Project Name: <Insert initiative name>				Risk As
NB. This is an intial risk assessment, a comprehensive view of risk needs to be comepleted during the build phase						a) Estimate likelihood of occurrence of eac
Has this AI initiative assessed as a high risk solution?				Yes		b) Estimate its potential impact on TMCA
						c) Find the corresponding score in the mat
Proposed Solution & Technology Overview						d) Add counter measure for each risk cate
						e) Assign a residual risk score based on co
						f) Identify if a risk requires ongoing monito
						g) Summarise risk assessment results into
		Overall Risk		20		

Risk Type (Refer below guide)	Risk Category	Likelihood	Impact	Risk	Applicable	Risk Description	Counter Measu
Unintended Access to Data	Security & Privacy	Likely	High	20	No		
Data Loss & Residency		Unlikely	High	16			
Data Volume				2			
Data Quality							
IP Loss				1			
Ethical Breach				8			
Regulatory Breach							
Quality / Performance / Effectiveness Issues							
Commercial Damage							
Reputational Damage							
Financial Damage							
Process Automation Risk							
Model Transparency							
Model Drift Risk							
Model Bias Risk							
Model Explainability Risk							
Deployment Environment Risk							
Maturity of the Solution							

Risk Type	Assessment Guide
Unintended Access to Data	Does the solution have risk of users gaining unintended access to the tool, sensitive or confidential data?
Data Loss & Residency	Does the solution expose TMCA to data loss such as accidental or malicious destruction, deletion, or corruption of important data?
Data Volume	Is adequate volume of model training data available for the solution?

AI GOVERNANCE FRAMEWORK

AI Ops/Technical architecture

DataOps Data pipeline

Ingest, process, and curate data for AI.

Model development and experimentation

Explore, experiment, collaborate – build iteratively.

Continuous Integration and Deployment (CI/CD)

Enable DevOps through CI/CD for packaging and deployment.

Monitoring and observability

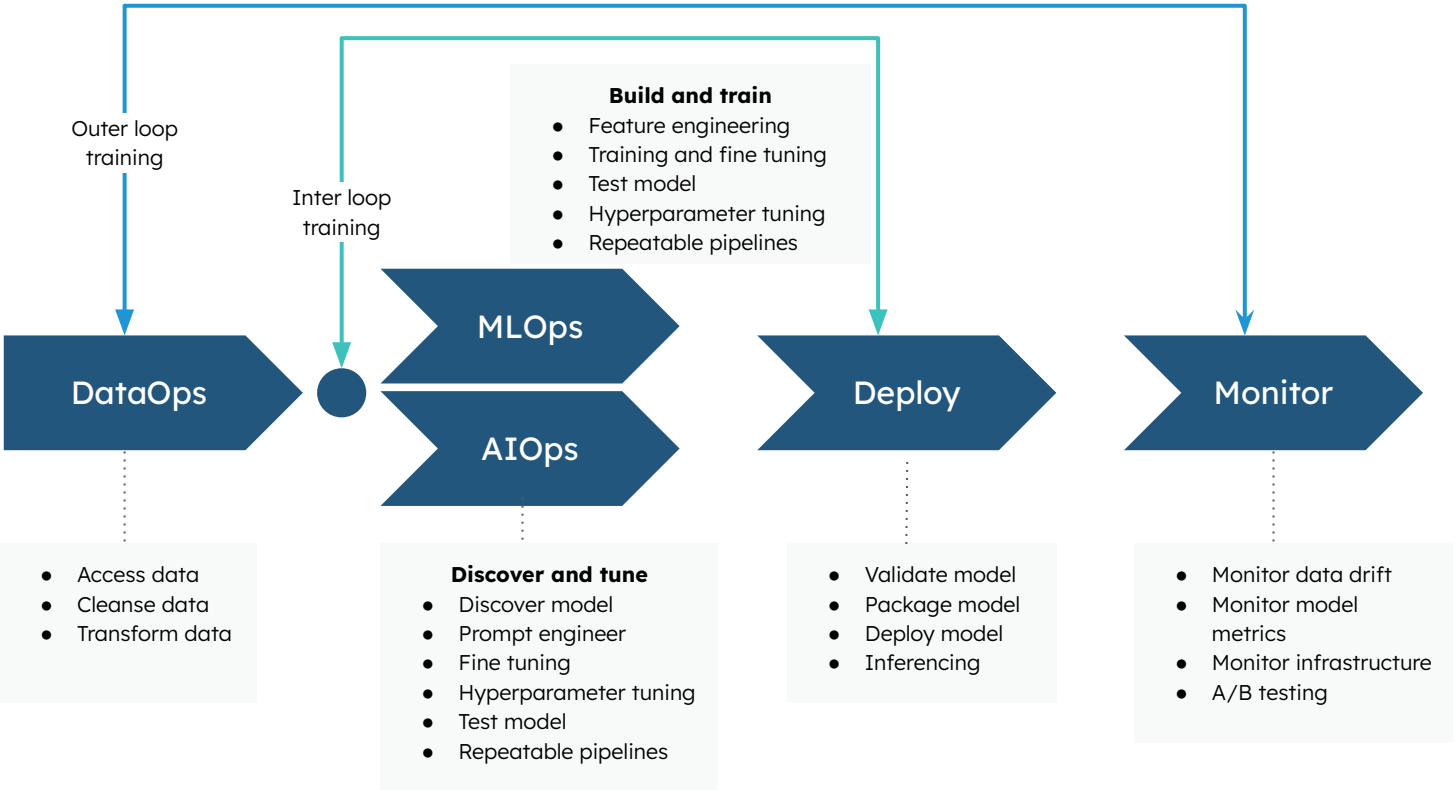
Continuously monitor model performance and system health in production.

Feedback loops and continuous improvement

Learn from production data – iteratively improve for better outcomes.

AI GOVERNANCE FRAMEWORK

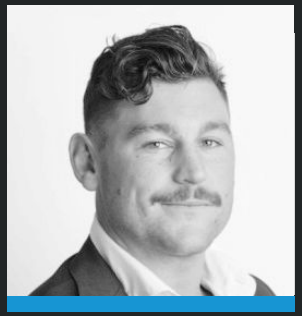
AI Ops - Logical design



GET IN TOUCH

Contact the team

Andy Canning
APAC MD
Andy.Canning@equalexperts.com



Matthew Waugh
APAC Sales Director
Matthew.Waugh@equalexperts.com