From Component Monitoring to Systemic Resilience

AI Failure Path Mapping

The Risk Gap: Internal Fragility vs. External Threat

As companies integrate AI, the risk profile shifts. It is no longer just about external attacks; it is about the fragility of internal complexity. It is the difference between an AI model remaining mathematically '*accurate*' while processing corrupted data that leads to poor operational and executive decisions.

Undetected AI Failures

A Finance Example

Scenario: Credit Decision

Trigger: Third-party data feed starts returning stale income data (T+30 days old)

Propagation:

- Feature engineering normalises values (masks staleness)
- Model training on recent data includes stale features
- Model drift goes undetected (accuracy metrics stable)
- Credit decisions use outdated applicant data

Critical Impact: Improper credit approvals go undetected over 6 weeks.

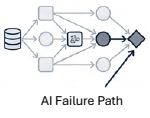
Business Consequences: Lost revenues and loss of customer trust.

Regulatory Consequences: Bias treatment of customers is a breach of Consumer Duty. Under SM&CR both the organisation and an individual board executive are held accountable.

The Issue: Your Risk Blind Spot

MLOps tools monitor isolated components (e.g. "*Is the model accurate?*"), missing the chain reaction failures where data degradation cascades into catastrophic business or regulatory breaches.

The Solution: AI Failure Path Mapping



AI-FPM adapts the proven cybersecurity discipline of Attack Path Mapping (APM) to AI. The process maps reveal how seemingly minor failures in an AI pipeline can impact critical operational and executive decisions.

The Strategic Value

Deploy safe-guards and circuit breakers where they have the greatest opportunity to contain failure cascades and reduce risk business risk.

The Regulatory Fit

Directly supports compliance with the PRA's SS1/23, the EU AI Act, and ISO 42001 by demonstrating rigorous control over complex model pipelines and interdependencies.

"Finally, a framework that speaks the language of the Risk Committee, not just the IT department." CHIEF RISK OFFICER & BOARD DIRECTOR

ADVANTAGE AI

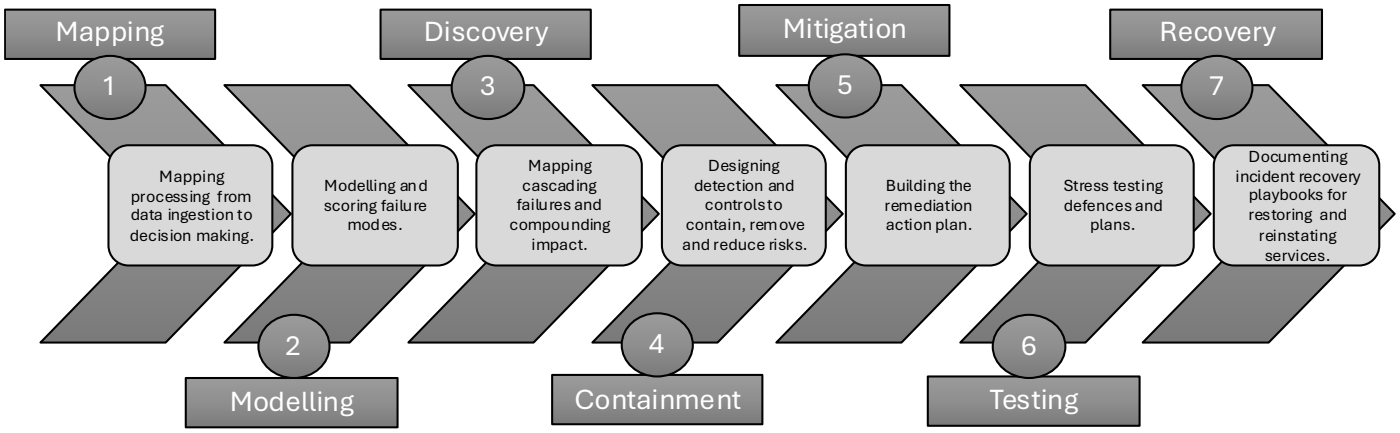
Your customers and regulators expect assurance. ADVANTAGE AI delivers it.

From Component Monitoring to Systemic Resilience

AI Failure Path Mapping

A Comprehensive Process

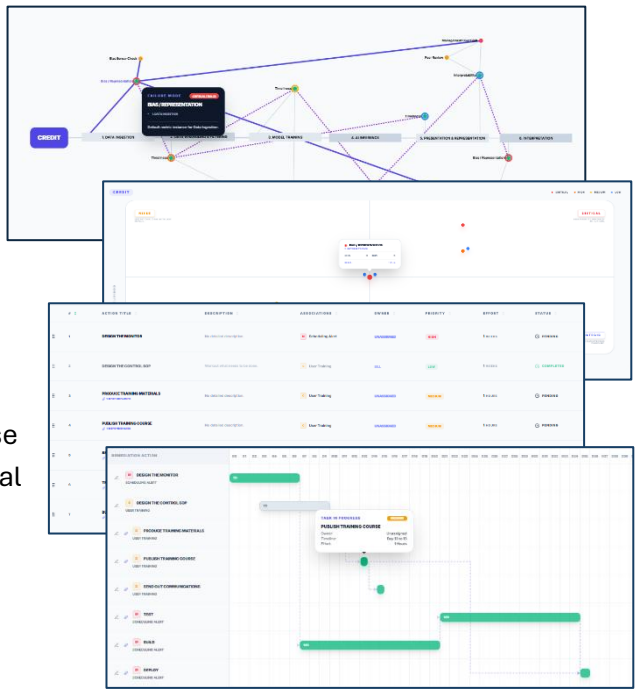
AI-FPM combines a comprehensive 7-step process with a bespoke toolset to deliver quantified risk clarity and an actionable risk mitigation plan.



Phase	Activity	Outcome
Mapping	Process Mapping	Process Map from Data Ingestion to Decision Making
Modelling	Failure Modelling Analysis	Identification of AI Pipeline Risks
Discovery	Failure Path Discovery	Compounding Failure Impact
Containment	Control and Detection Engineering	Guardrails, Fail-Safes and Monitoring
Mitigation	Risk Reduction & Removal Planning	Actionable Remediation Plan
Testing	Tabletop “Failure Detection & Control” Exercise	Stressed Tested Defenses
Recovery	Restore & Reinstate Design	Incident Playbooks

An Advanced Toolset

Our unique AI-FPM toolset provides a clear and consistent foundation for managing identified AI risks. Features span all 7 stages of the process with clear graphical functions for process mapping, risk identification, risk scoring, risk intelligence and risk mitigation.



The system automatically generates key customer outputs such as Failure Path Maps, Risk Heatmaps and Remediation Plans that can be exported in various formats for clients to use within their internal documentation or imported into their local systems to track risks, manage remediation actions and enhance operational recovery procedures.

ADVANTAGE AI

Your customers and regulators expect assurance. ADVANTAGE AI delivers it.

From Component Monitoring to Systemic Resilience

AI Failure Path Mapping

AI Resilience Delivered at Pace

Whilst our full AI Assurance assessments can take 6-8 weeks, the highly efficient AI-FPM process can deliver a detailed risk assessment and actionable remediation plan within days. These intensive workshops rapidly, yet comprehensively, review current state, identify gaps, determine the desired target state, test planning assumptions and document operational playbooks in the matter of just a few days.

Alignment to Regulators and Best Practice Methodologies

The AI-FPM methodology is aligned with leading global standards and UK-specific mandates - meeting the increasing expectations for algorithmic accountability

While frameworks like NIST AI RMF and ISO 42001 provide the "*what*" of AI governance, AI-FPM provides the "*how*" for specific, high-stakes use cases. Our process operationalises the MAP and MEASURE functions of NIST by turning complex technical interdependencies into a visual blueprint of risk.

For regulated finance companies operating, the methodology serves as a critical tool for satisfying the PRA's SS1/23 Principle 3, requiring firms to identify and remediate model limitations and systemic weaknesses. It also provides the "end-to-end transparency" necessary for Consumer Duty compliance proving that AI-driven decisions are not resulting in foreseeable harm or biased outcomes for customers.

AI-FPM Phase	NIST AI RMF	UK PRA (SS1/23) & FCA	EU AI Act	ISO 42001
Mapping	**MAP**: Establishes context and system boundaries by mapping data ingestion to decisioning.	**Principle 1 & 3**: Documents model logic, data lineage, and intended purpose.	**Art. 13**: Provides transparency on the characteristics and functioning of the AI system.	**A.8**: Conducts a systematic AI system life cycle assessment.
Modelling	**MAP**: Identifies and categorizes internal fragilities and potential failure modes.	**Consumer Duty**: Identifies potential for foreseeable customer harm or biased outcomes.	**Art. 9**: Establishes a targeted risk management system for the specific use-case.	**Clause 6.1**: Directly identifies AI-specific risks and opportunities for the business.
Discovery	**MEASURE**: Quantifies cascading impact of failures across the model pipeline.	**Principle 3**: Analyses systemic risk, interdependencies, and model limitations.	**Art. 9.2**: Identifies and analyses known and reasonably foreseeable risks.	**B.5**: Assesses the specific impact of the AI system on individuals and society.
Containment	**MEASURE / MANAGE**: Deploys data-driven safeguards and circuit breakers to halt failure chains.	**Op. Resilience**: Prevents critical service disruption and ensures robust performance.	**Art. 15**: Implements technical robustness, accuracy, and fail-safe plans.	**A.10.3**: Defines and implements specific AI risk treatment controls.
Mitigation	**MANAGE**: Prioritises risk reduction and resource allocation for identified weaknesses.	**SM&CR**: Provides documented evidence of executive control over AI risk profiles.	**Art. 9.4**: Adopts targeted measures to manage and minimize residual risks.	**Clause 8.3**: Executes the risk treatment plan within the operational context.
Testing	**MEASURE**: Validates the efficacy of controls through rigorous stress-testing.	**Principle 3.2**: Provides independent challenge and rigorous performance testing.	**Art. 14**: Validates human oversight mechanisms and intervention effectiveness.	**A.10.5**: Regularly tests the performance and security of AI system controls.
Recovery	**GOVERN**: Establishes operational continuity via incident playbooks and recovery plans.	**FCA SYSC 15.1**: Creates actionable playbooks for restoring and reinstating services.	**Art. 15.3**: Ensures resilience against technical errors, faults, or inconsistencies.	**A.9**: Designs incident response, monitoring, and service reinstatement design.

From Component Monitoring to Systemic Resilience

AI Failure Path Mapping

Let AI-FPM Outcomes Become Your Strategic Advantage

Technical-Executive Gap: Complex technical AI processing is turned into tangible business risk. AI-FPM directly maps the impact of AI failures on revenue, customer trust and regulatory compliance.

Isolated and Compounding Risk: Move beyond simple error logs. AI-FPM provides the visual blueprint of failure movement, showing how a data corruption can pollute operational and executive decisions.

Clear Risk Mitigation: Pin-point pipeline weaknesses and design robust safe-guards and circuit breakers where they have the biggest impact in detecting, limiting and halting failing AI process chains.[1]

Investment and Resource Prioritisation: Actionable remediation plans based directly on risk ensures the greatest ROI from risk reduction, removal and containment activities.

Operational Continuity: Stress tested incident playbooks provide clear steps for recovery, restore and service reinstatement to enhance operational resilience.

Regulatory & Compliance Excellence: AI-FPM provides the end-to-end transparency demanded by regulators with clear evidence of your proactive AI risk management approach and operational resilience strategy.

[1] We have a network of trusted partners ready to support those clients that don't have the capability or capacity to implement the identified remediation actions.

ADVANTAGE AI was formed in 2024 to provide AI consultancy, delivery and training services. We have led the introduction and built the internal training for the use of AI for 10,500 users located in over 50 countries. Leveraging this experience and recognising the support organisations now need with AI governance, the company has pivoted to providing niche AI Assurance, Adoption and Training services.

We have a specialist bench capability with deep experience in risk management, business process optimisation and technology transformation within highly regulated environments. We have delivered complex, global projects for the Bank of England, the Financial Conduct Authority, the London Stock Exchange Group, Royal Bank of Scotland, Deutsche Bank, AXA XL, MS Amlin and many other clients across the Aviation, Telecoms, Health, and Government sectors.

OPERATIONALISING YOUR RESILIENCE

ADVANTAGE AI provide independent AI-FPM workshops for high stakes organisations. The workshops rapidly and effectively deliver clarity on quantified AI risks with a practical remediation solution.

Take control of your AI risk exposure before the regulator does. Contact us today...

Web: https://advantage-ai.co.uk **Phone**: +44 (0)7471 359987 **Email**: info@advantage-ai.co.uk

ADVANTAGE AI don't sell AI systems.
We assure them.
Independently.

ADVANTAGE AI

Your customers and regulators expect assurance. ADVANTAGE AI delivers it.