

Strategic Resilience: An Integrated AI Risk and Governance Framework for

Admiral Group Plc

Sheikh Ahmad Tijan Jallow

2011987



Global Business Challenges

(BMMB7006)

Rebecca Francis-Davies

University of Wales, Trinity Saint David

24th July, 2026

Executive Summary

Admiral Group has moved beyond isolated AI experimentation. Predictive, generative and emerging agentic applications are being developed or used across underwriting, pricing, claims, fraud management, customer service and internal operations. These capabilities may strengthen risk selection, service efficiency and customer engagement, but they also increase the potential for data-quality failures, opaque outcomes, cybersecurity threats, third-party dependency and inconsistent control across UK and European operations.

The report concludes that Admiral's primary AI governance challenge is not the absence of governance structures. The strategic challenge is closing the assurance gap between the existence of these arrangements and demonstrable evidence that they are consistently embedded, independently validated and effective across jurisdictions, business units and technology suppliers.

Five findings support this conclusion. First, Admiral reports more than 150 GenAI initiatives across different businesses and functions. Second, UK–EU regulatory divergence requires a common governance baseline with local legal classification and approval. Third, AI-supported insurance processes depend on complex data and supplier relationships, creating lineage, residency, cybersecurity, model-change and concentration risks. Fourth, customer trust depends on actual outcomes. Fifth, AI activity is not equivalent to economic value. Benefits must be assessed after implementation, supplier assurance, remediation and expected customer-harm costs.

Admiral should strengthen its existing governance architecture. Implementation should take place over 24 months. Months 1–6 should establish the assurance standard. Months 7–18 should validate high-impact system. Months 19–24 should test operating effectiveness. The Group Risk Committee should oversee delivery.

Table of Contents

Executive Summary	1
2. Methodology and Analytical Framework	4
3. External and Competitive Environment	6
4. Regulatory Divergence and The AI Assurance Gap	8
5. Data Governance	11
6. Ethical AI, Accountability and Customer Trust	14
7. Macroeconomic Uncertainty and Risk-Adjusted AI Value	17
8. Strategic Recommendations	19
8.1 Integrate the Assurance Standard and System Register	19
8.2 Introduce Impact-tiered Approval and Independent Validation	19
8.3 Establish a Customer-Outcome Assurance Standard	20
8.4 Strengthen Third-party and Cross-border Assurance	20
8.5 Link Investment to Independently Verified Value	21
9. 24-Month Action Plan	22
9.1 Phase 1: Foundation (Months 1 -6)	22
9.2 Phase 2: Build and Validate (Months 7 - 18)	22
9.3 Phase 3: Embed and Demonstrate (Months 19 - 24)	23
9.4 Programme Cost	23
9.5 Funding Gates and Success Measures	23
9.7 Reporting and Escalation	24
10. Conclusion	25
Reference List	26

1. Introduction

Artificial intelligence is becoming embedded in insurance underwriting, pricing, claims management, fraud detection and customer communication. These applications can improve risk selection, service speed and operational productivity, but they can also amplify data-quality problems, obscure accountability and produce harmful customer outcomes at scale (Dubey, Astvansh and Kopalle, 2025). The strategic question is therefore not simply whether AI can generate value but whether the Group can demonstrate that AI-enabled growth remains lawful, fair, secure and consistently governed across its multinational operations and third-party technology relationships.

Admiral combines extensive UK retail financial-services operations with insurance businesses in France, Italy and Spain. At the end of 2025, the Group reported more than 15,000 employees and operations serving customers across these four countries (Admiral Group plc, 2026a, p. 6). Its activities include motor, household, travel and pet insurance, alongside personal lending. These products depend on extensive personal data, predictive risk assessment and repeated customer interactions. The geographical structure also requires Admiral to manage overlapping UK and EU requirements rather than rely on a domestic governance model.

Admiral's potential exposure to AI-related risks is increasing as AI becomes integrated across operational and customer-facing processes. The Group reports that it accelerated investment in AI, established a GenAI Centre of Excellence and was managing more than 150 GenAI initiatives during 2025 (Admiral Group plc, 2026a). This demonstrates organisational breadth but does not establish that every initiative is material, customer-facing or involved in automated decisions. Admiral separately identifies AI uses in underwriting and pricing, claims management, fraud prevention and customer communication. Its strategic relationship with Google Cloud covers policy administration, billing, analytics,

machine learning, generative AI and customer-facing digital channels (Admiral Group plc, 2024).

For this report, AI includes machine-learning models, predictive analytics, automated decision-support systems, and generative AI that influence insurance processes, employee actions, or customer outcomes. Conventional actuarial models and traditional statistics are excluded unless they incorporate machine learning or form a material part of an AI-enabled decision process.

The available evidence does not support an argument that Admiral lacks AI governance (Admiral Group plc, 2025). The Group reports a Responsible AI and Data team, integration of AI governance into model-development processes and employee education through its Data and AI Academy (Admiral Group plc, 2026a, pp. 19, 64; Admiral Group plc, 2026c). Its Sustainability Report states that AI tools are introduced with guidance, training and oversight (Admiral Group plc, 2026d, p. 42). These disclosures indicate meaningful foundations. Public reporting, however, provides limited evidence through which an external analyst can evaluate whether controls are applied consistently and produce acceptable outcomes across every business unit, jurisdiction and third-party system. This limitation does create the assurance question examined in this report.

This report covers the UK and EU (using France, Italy, and Spain). It argues that Admiral's main challenge is the assurance gap between established arrangements and evidence of their effectiveness. Admiral should strengthen its architecture through a Group-wide assurance model combining common standards with local approval, independent validation, and continuous monitoring of customer impacts.

2. Methodology and Analytical Framework

This report uses a qualitative documentary case-study method. It evaluates the consistency between Admiral's disclosed activities, its reported governance arrangements, applicable regulation and established academic principles. It does not audit Admiral's systems, test model outputs or claim causal relationships from company-level data.

Five complementary lenses structure the analysis. Institutional Theory evaluates coercive, normative and mimetic pressures across jurisdictions (DiMaggio and Powell, 1983). This is relevant because Admiral must respond to the UK supervisory expectations and the EU's statutory requirements, professional standards and the practices adopted by competitors and technology suppliers (Tomei, Jain and Franklin, 2025).

The Resource-Based View assesses whether Admiral's data, expertise, organisational learning and assurance routines can support sustained advantage (Barney, 1991).

Stakeholder Theory evaluates consequences for customers, employees, regulators, investors and suppliers, including conflicts between efficiency, affordability and fairness (Freeman, 1984).

Managerial economics distinguishes gross technical gains from risk-adjusted net value. Finally, the NIST AI Risk Management Framework's Govern, Map, Measure and Manage functions provide an operational structure for lifecycle assurance (Tabassi, 2023; Autio et al., 2024). PESTLE and Five Forces are used selectively to examine external and industry conditions rather than as substitutes for these deeper lenses.

Governance maturity is assessed through seven criteria: coverage, consistency, accountability, independence, auditability, outcome effectiveness and responsiveness. These distinguish the presence of policies and committees from evidence that controls work and trigger corrective action.

The study is limited by public disclosure. Admiral does not publish complete AI inventories, validation reports, customer-outcome datasets, supplier contracts or internal audit findings. Management benefit estimates cannot be independently attributed to AI, and unequal disclosure across UK and European operations limits direct comparison.

3. External and Competitive Environment

Admiral's AI strategy operates within an environment characterised by regulatory divergence, cost pressure, changing customer expectations and technological acceleration. Morrison (2020) argues that political, economic, social, technological, legal and environmental forces interact in global business decisions. For Admiral, the most material question is whether AI can improve underwriting and service efficiency while assurance remains effective across the UK, EU and technology supply chain.

Political and legal fragmentation creates both cost and governance risk. The UK relies substantially on existing accountability and customer-outcome rules, while the EU AI Act adds prescriptive obligations according to a system's purpose and classification. Institutional Theory suggests that a common Group baseline can reduce duplication and support legitimacy, but uniformity must not obscure legal differences (DiMaggio and Powell, 1983). Admiral should therefore standardise core evidence and controls while retaining local classification and approval.

Economic conditions strengthen the incentive to apply AI to pricing, claims and fraud management. UK CPI increased by 2.8% in the 12 months to May 2026, while the average accidental-damage motor claim reached £3,699 in Q1 2026, 8% higher than in the preceding quarter (Association of British Insurers, 2026; Office for National Statistics, 2026). These measures are not directly comparable and do not establish Admiral's individual cost experience. They nevertheless illustrate continued pressure from repair complexity and claims severity. AI may improve risk assessment, but model error, false positives and inappropriate automation can impose additional cost. Investment should therefore be assessed through risk-adjusted value rather than gross automation.

Customer expectations create a tension between convenience and control. AI can support personalised information and faster claims, but acceptance may fall where systems

influence price or coverage without understandable explanations or accessible human escalation. FCA research indicates potential demand for autonomous financial tools alongside concerns about trust and control (Financial Conduct Authority, 2026b, 2026c). The research covers retail financial services generally, not Admiral customers, but it shows that technical adoption and customer acceptance are different measures.

Porter's Five Forces clarifies the competitive implications (Porter, 2008). Rivalry and buyer power are high in UK motor insurance because comparison services increase transparency and switching. AI may improve pricing speed, but widely available models can intensify competition without creating durable differentiation. Supplier power is moderate but increasing where cloud migration and proprietary services create switching costs. New-entry and substitute threats are moderate: cloud services lower technical barriers, while capital, regulation, claims capability and trusted data remain constraints. Embedded insurance and customer-side AI agents may nevertheless reshape distribution.

Assurance impacts more than compliance costs. As customer-side AI agents automate cover comparisons and switching, weak product data can quickly reduce conversion rates. Conversely, clear machine-readable information supports distribution. Because fragmented governance can slow incumbents, Admiral should treat decision traceability, explanation quality and rapid control approval as core capabilities. Ultimately, governance must reduce the time needed to deploy defensible changes without compromising customer protection.

The Resource-Based View indicates that Admiral's advantage is unlikely to arise from general-purpose technology which competitors can also purchase (Barney, 1991). The more defensible value may come from proprietary data, actuarial expertise, claims knowledge, organisational learning and routines that translate models into reliable outcomes.

Governance maturity can therefore becomes a strategic capability when it enables controlled deployment. A policy document alone is not a competitive resource.

4. Regulatory Divergence and The AI Assurance Gap

Admiral faces regulatory divergence rather than a choice between regulated and unregulated AI. The UK primarily applies existing data-protection, equality, consumer-protection, financial-services requirements and insurance distribution standards (European Union, 2016a) through a principles and outcomes-based model. The EU combines the General Data Protection Regulation with the risk-based EU AI Act. Admiral consequently needs a common Group assurance standard supported by jurisdiction-specific legal overlays.

The FCA has stated that it does not currently intend to introduce separate AI-specific financial services rules. It relies on the Consumer Duty, Senior Managers and Certification Regime and established governance expectations (Smith, 2026). The Consumer Duty requires firms to act in good faith, avoid foreseeable harm and deliver good outcomes (Financial Conduct Authority, 2026a). Each material UK system should therefore be connected to an accountable senior manager, affected Consumer Duty outcomes, monitoring measures and an escalation process.

UK data-protection law changed through the Data (Use and Access) Act 2025 (“Data (Use and Access) Act 2025,” 2025; Information Commissioner’s Office, 2026c). Section 80 replaced Article 22 of the UK GDPR with Articles 22A–22D. The revised regime permits significant solely automated decisions involving non-special-category data in a wider range of circumstances, subject to safeguards including information about the decision, representations, human intervention and contestation (Information Commissioner’s Office, 2026a, 2026b). Stronger restrictions remain for special-category data. This flexibility should not be confused with nominal human oversight. Reviewers must have the competence, evidence, time and authority to change an outcome.

The EU AI Act classifies systems according to risk and imposes obligations concerning governance, data, documentation, logs, human oversight, robustness,

cybersecurity and post-market monitoring (European Union, 2024). Insurance use does not automatically create high-risk status. Annex III specifically identifies AI used for risk assessment and pricing in relation to natural persons in life and health insurance. Admiral's European motor-pricing, claims and customer-service systems must therefore be classified by intended purpose rather than assumed to be high-risk or exempt. Certain employment applications may fall within a separate high-risk category.

Operationally, classification should be recorded in a jurisdictional control matrix rather than left in legal memoranda. For each system, the matrix should state the product, purpose, affected person, degree of automation, data category, Admiral's regulatory role, applicable safeguards and approval owner. The corresponding evidence pack should link the classification to data documentation, validation, human-oversight design, customer information, incident handling and post-deployment monitoring. Where a system is outside an AI Act high-risk category, the record should still identify GDPR, insurance-governance and conduct obligations. This prevents "not high-risk under the AI Act" from becoming an incorrect conclusion that the use is low-risk for Admiral or its customers.

Role classification also matters. Admiral may be a deployer when using a supplier's system according to its intended purpose, but it may assume provider obligations if it develops a system internally, markets it under its name, substantially modifies it or changes its intended purpose. Procurement does not transfer accountability. Supplier contracts must provide the documentation, logs, change notifications and incident information necessary for Admiral's obligations.

Customer-facing generative AI may fall outside high-risk categories while remaining subject to transparency requirements. Informing customers that they are interacting with AI is only the starting point. They should understand the system's function, whether its response affects a policy or claim, its limitations and how to reach a person. The EU GDPR remains

independently applicable: a system may fall outside AI Act high-risk categories while involving profiling, special-category data or a solely automated significant decision under Article 22 (European Union, 2016b).

The AI Act entered into force on 1 August 2024 (European Union, 2024). Prohibited-practice and AI-literacy provisions began applying in February 2025, followed by governance and general-purpose AI obligations in August 2025. At the research cut-off, EU institutions had announced political agreement on revised application dates for high-risk systems, including December 2027 for specified stand-alone uses and August 2028 for systems embedded in regulated products (European Commission, 2026a). Admiral should verify final amending legislation before relying on these dates. Draft classification guidance remained non-binding at the cut-off (European Commission, 2026b, 2026c).

Bradford's (2020) Brussels Effect suggests that EU standards may influence wider Group practice where common controls reduce fragmentation. Admiral should not impose every EU obligation on UK systems automatically. It should adopt a common control where it improves assurance or reduces duplication, while maintaining proportionate local rules. The regimes converge around accountability, transparency, data quality, human oversight and protection from harmful outcomes, but differ in method. That convergence supports common evidence; divergence requires local approval.

5. Data Governance

Admiral's data-governance challenge arises from source diversity, multinational processing and technology dependence. The company reports collecting customer, claims, payment, credit-reference, fraud, device, location and telematics information (Admiral Group plc, 2026a). Its Google Cloud relationship covers core policy and billing platforms, analytics, machine learning, GenAI and digital channels (Admiral Group plc, 2024). Effective assurance requires traceability from collection through model development, decision and deletion.

A representative motor-insurance process illustrates the issue. Customer information may be combined with vehicle details, claims records, fraud indicators, credit-reference information, geographical variables and device data. For telematics, Admiral identifies location, speed, distance, acceleration, braking and cornering data (Admiral Group plc, 2026b). These disclosed categories should not be assumed to appear in every model, but they show how a decision may depend on multiple internal and external sources and derived inferences.

Lineage must capture more than a system diagram. A reproducible decision record requires the source, timestamp, logic, and human interventions behind every outcome. Admiral should regularly test reconstruction times using sampled cases, treating missing data as a control failure.

Purpose limitation must be assessed per use case. Information collected for a quotation may later appear useful for fraud detection, personalisation or model training, but technical usefulness does not establish lawful or expected reuse. Admiral should document purpose, lawful basis, necessity and reasonable expectations. The European Data Protection Board (EDPB) states that reliance on legitimate interests for AI development or deployment requires a defined interest, necessity and balancing of individual rights (European Data

Protection Board, 2024). Consent should not be treated as a universal solution where processing is necessary, withdrawal is impractical or customer choice is not genuine.

Data minimisation should operate at the feature level; variables offering marginal predictive power but significant proxy risks must be evaluated against non-discrimination and data protection standards (van Bekkum, Zuiderveen Borgesius and Heskes, 2025). This is important for postcode, occupation, device information and journey patterns, which may act as proxies for protected or socioeconomic characteristics.

Data quality differs from model accuracy; a model can perform well overall using incorrect individual data. Admiral must be able to trace the origin, transformation, and human involvement for any data influencing a disputed premium or claim. Corrections and erasures must also propagate through all training sets, logs, and supplier systems. The EDPB warns that unlawfully processed training data may affect lawful deployment unless a model is properly anonymised (European Data Protection Board, 2024). This does not mean every erasure request requires retraining; it requires a documented choice between deletion, retraining, output restriction or another remedy.

Cross-border mapping must extend beyond the primary server location to remote access, support teams, sub-processors, backups, logs and model-improvement data. A European cloud region does not prove that all related processing remains in the European Economic Area (EEA). The register should identify origin, destination, controller, processor, transfer mechanism, security, retention and accountable owner.

Outsourcing does not outsource Admiral's accountability. Material suppliers should disclose whether prompts and outputs are retained, whether Admiral data train models, how changes are notified and which logs are available. Contracts should address processing purposes, sub-processors, residency, security, incidents, model changes, rights requests, deletion, audit, portability and exit. For EU operations, these arrangements should also align

with the Digital Operational Resilience Act's ICT third-party requirements (European Union, 2022).

Governance continues after deployment. Repair costs, fraud behaviour, customer populations, field definitions or supplier changes can create drift. EIOPA's insurance-specific Opinion emphasises proportionate data governance, record-keeping, fairness, cybersecurity, explainability and oversight even for systems outside the AI Act's high-risk classification (European Insurance and Occupational Pensions Authority, 2025a, 2025b). Admiral should integrate its AI register, data catalogue, model inventory and procurement records. Deployment should not proceed where material data lack verified provenance, lawful use, quality control or enforceable supplier obligations.

6. Ethical AI, Accountability and Customer Trust

Accuracy and legal permission do not establish ethical legitimacy. Insurance decisions distribute financial protection, prices and access. A model can improve portfolio-level accuracy while creating unjustifiable disadvantages for particular groups and a compliant disclosure may remain unintelligible. Ethical assurance therefore requires evidence about purpose, distribution of benefits and harms, explanations, human control and redress.

Floridi and Cowls' (2019) principles of beneficence, non-maleficence, autonomy, justice and explicability provide a structure. For Admiral, beneficence requires verified customer or business value; non-maleficence requires prevention of foreseeable harm; autonomy requires meaningful control; justice requires defensible treatment of different groups; and explicability requires understandable outcomes and identifiable accountability. These principles matter only when translated into tests, thresholds and actions.

Stakeholder Theory broadens the assessment beyond shareholder returns (Freeman, 1984). AI may improve underwriting and reduce processing time while imposing costs on customers who are incorrectly classified, unable to navigate digital systems or treated as suspicious by fraud models. Management should examine who receives the benefit, who bears errors and whether affected customers have practical challenge routes.

Fairness in insurance does not require identical prices. Risk-based insurance differentiates between customers (van Bekkum, Zuiderveen Borgesius and Heskes, 2025). The relevant question is whether differences rest on accurate, relevant evidence, are proportionate to legitimate insured risk and remain legally and ethically defensible. Admiral should assess procedural fairness, distribution of outcomes, data quality and quality of customer interaction. Removing protected characteristics does not remove proxy risk.

Postcode, occupation, device information or journey patterns may correlate with protected or socioeconomic characteristics.

No single statistical measure proves fairness. Fraud systems require attention to false-positive differences because incorrect suspicion can delay a legitimate claim. Customer-service systems require resolution, escalation and abandonment measures. Metric selection should reflect purpose and be approved by business, risk and customer functions rather than developers alone. The FCA and ICO do not expect firms to collect protected-characteristic data systematically solely for outcome monitoring; Admiral should use legally available, proportionate and privacy-preserving evidence (Financial Conduct Authority and Information Commissioner's Office, 2026).

Customer perception also matters. A Dutch survey of 999 respondents found data-intensive insurance practices were viewed more favourably where customers could influence the outcome and the characteristic appeared logically related to risk (Zuiderveen Borgesius et al., 2025). The results cannot be generalised directly to Admiral's markets, but they indicate that perceived relevance and agency contribute to legitimacy.

Transparency, explanation, auditability and contestability are distinct (Nannini, Balayn and Smith, 2023). Customers need concise information about material factors, consequences, correction and review. Validators need technical evidence. Admiral should test explanations through comprehension, repeat contacts and successful use of review routes. Human oversight is meaningful only if reviewers understand limitations, see relevant evidence, have sufficient time and can change outcomes. Override rates, disagreement reasons, review time and subsequent overturns should be monitored; a very low override rate may reflect strong performance or automation bias.

Contestability requires clear operational design. Review routes must be easily identifiable and accessible for customers. High-impact processes should define service

levels, provide necessary evidence to reviewers, and allow for escalation. Finally, outcomes should inform model monitoring to identify systemic defects.

Every material system requires an executive owner to ensure accountability for customer outcomes. While business and technology teams manage controls, risk and compliance teams challenge them, and Internal Audit verifies their effectiveness (Institute of Internal Auditors, 2020). Trust should be evaluated based on actual behaviour and outcomes rather than relying solely on Net Promoter Scores. Key indicators of this trust include digital abandonment rates, repeat contacts, AI-related complaints, requests for human review, overturned decisions and claims delays. The FCA's insurance review found that firms did not consistently demonstrate comprehensive monitoring of distinct groups, including vulnerable customers (Financial Conduct Authority, 2024, 2025). While not Admiral-specific, this highlights a supervisory concern. Admiral should translate its principles into a clear customer-outcome assurance standard.

7. Macroeconomic Uncertainty and Risk-Adjusted AI Value

Macroeconomic uncertainty strengthens the commercial case for AI and the risk of deploying it too quickly. Claims inflation, repair complexity and affordability increase the value of faster risk detection, while changing economic relationships can reduce the reliability of historical models. Public benefit expectations may also encourage scaling before control costs and customer effects are verified.

General inflation and insurance claims severity follow different paths. UK CPI increased by 2.8% in the 12 months to May 2026, while the average accidental-damage motor claim reached £3,699 in Q1 2026, 8% above the preceding quarter (Association of British Insurers, 2026; Office for National Statistics, 2026). These measures are not directly comparable or Admiral-specific. They show why general inflation is an inadequate proxy for claims costs driven by parts, labour, sensors and vehicle complexity.

AI may improve detection of frequency and severity changes but does not remove pricing lag. Premiums are set before future claims costs are fully known. A model may remain technically operational while becoming economically stale. Monitoring should compare predicted and realised losses, repair duration, severity, fraud patterns and residual errors, with recalibration when thresholds are breached.

Affordability introduces strategic challenges as customers may adjust coverage or face payment issues. While granular segmentation aligns risk, it can seem arbitrary to customers, requiring Admiral to monitor broader customer metrics alongside technical performance.

The Bank of England maintained Bank Rate at 3.75% in June 2026 amid uncertainty over energy prices, inflation and economic activity (Bank of England, 2026). Higher rates may support returns on some invested assets while increasing pressure on borrowers and policyholders. The net effect cannot be inferred from Bank Rate alone. Credit, pricing and

customer-management models should be stress-tested against arrears, disposable income and behavioural change.

Management commentary has referred to more than £100 million in annual efficiency benefits by 2028 from GenAI, automation and cost discipline combined (Lauchlan, 2026). This is not an audited AI-only forecast. It is strategically relevant because benefit expectations affect investment and incentives. Admiral should distinguish activity, technical output, operational outcomes and financial value. Material applications need a baseline, counterfactual comparison, benefit owner, full control-cost allocation and post-implementation review.

Scenario analysis should connect economic conditions to model and customer effects rather than vary revenue alone. A claims-stress scenario should combine higher repair severity, longer settlement times and changes in fraud patterns; an affordability scenario should examine lower conversion, payment difficulty and vulnerable-customer demand; and a supplier-disruption scenario should test loss of a model, cloud service or essential log. A rapid-agentic-adoption scenario should assume that systems can initiate actions across connected processes, materially increasing the speed at which an error propagates. For each scenario, management should define monitoring indicators, operational limits, fallback processes, customer communication and the executive authorised to suspend the application.

Risk-adjusted net AI value should be assessed as realised operating and underwriting benefits plus avoided losses, less implementation, supplier, assurance, remediation and expected customer-harm costs. This is a decision framework, not an accounting formula. The IMF also identifies concentration among cloud and advanced-model providers as a potential common-failure channel (International Monetary Fund, 2026). Testing should therefore cover controlled adoption, economic and claims stress, and rapid agentic adoption.

8. Strategic Recommendations

Admiral should strengthen rather replace its existing governance arrangements through a Group-wide AI assurance model. These are the five connected recommendations for action.

8.1 Integrate the Assurance Standard and System Register

Admiral should connect its AI register, model inventory, data catalogue, procurement records, cloud inventory and customer-outcome monitoring. Each material system should record its purpose, accountable executive, jurisdictions, regulatory classification, data sources, model and prompt versions, supplier dependencies, validation status, customer effect, monitoring thresholds and approval date.

Quarterly reconciliation should identify omitted systems, duplicate tools, shadow AI use, expired approvals and unrecorded supplier changes. This would provide one source of assurance rather than several disconnected records held by different functions.

The recommendation applies the NIST Govern and Map functions and responds to institutional pressure without creating a separate governance bureaucracy (DiMaggio and Powell, 1983). The practical objective is visibility. Admiral cannot govern systems it has not identified or assigned to an accountable owner.

8.2 Introduce Impact-tiered Approval and Independent Validation

Admiral should classify systems according to customer, employee, financial and operational impact rather than relying only on statutory categories.

Low-impact internal drafting tools may require owner review and data controls. Customer-assistance tools require accuracy testing, escalation and output monitoring. Pricing, claims, fraud and employment systems require independent validation. Solely automated significant decisions and agentic systems require continuous monitoring, fallback arrangements and suspension controls.

Validation should be sufficiently independent from development and benefit ownership. It should cover data quality, performance, fairness, explanation, human oversight, cybersecurity, resilience, regulatory classification, supplier dependency and customer outcomes.

Material changes should trigger reassessment. A system should not retain its approval indefinitely where the model, data, supplier, intended purpose or customer impact has changed.

8.3 Establish a Customer-Outcome Assurance Standard

Every material customer-affecting system should define its intended benefit, foreseeable harms, affected groups, fairness measures, explanation requirements, intervention route and remediation thresholds.

Measures should reflect the process involved. Pricing should track quotation, renewal, affordability and decline outcomes. Claims systems should monitor delay, reopening, escalation and overturn. Fraud models should measure confirmed cases, false positives and customer challenge. Chatbots should monitor resolution, incorrect responses, escalation and abandonment.

Customers should be able to recognise when automation materially affects them, understand the principal reason for an outcome, correct inaccurate information, reach a competent person and obtain genuine reconsideration.

Board reporting should focus on outcomes and corrective action rather than the number of completed assessments.

8.4 Strengthen Third-party and Cross-border Assurance

Material suppliers should provide processing location and sub processor transparency, restrictions on secondary training, model-change notification, audit access, logs, incident support, deletion certification, portability and exit arrangements. Admiral

should test contractual rights through continuity, log access and exit exercises. Dependency analysis should consider correlated reliance across policy administration, billing, analytics and customer channels and not merely individual supplier strength.

8.5 Link Investment to Independently Verified Value

Every material initiative should have a baseline, benefit owner, lifecycle cost, customer-outcome measures, post-implementation review and termination criteria.

Continued investment should depend on independently verified operating or underwriting benefit after supplier, assurance, remediation and expected customer-harm costs. Systems should be redesigned, restricted, suspended or retired where benefits remain unverified, customer outcomes deteriorate, errors exceed tolerance or the supplier cannot provide necessary assurance.

The five recommendations are mutually dependent. The integrated register provides visibility. Impact tiers direct assurance resources. Customer-outcome standards demonstrate effect. Supplier controls extend governance beyond Admiral. Value verification determines whether scaling remains economically justified.

The Resource-Based View suggests that this combination of data, expertise, assurance and organisational learning is more defensible than access to general-purpose technology alone (Barney, 1991).

9. 24-Month Action Plan

The programme should integrate existing functions rather than create a parallel AI control organisation. The Group Risk Committee should oversee delivery; the Group Chief Risk Officer should act as executive sponsor; and the Head of Group Responsible AI and Data should coordinate standards. Business executives remain accountable for outcomes, the CIO/CTO for technical controls, the DPO for privacy, Procurement for suppliers, the CFO for benefit verification and Internal Audit for independent assurance. Exact responsibilities should be aligned with Admiral's formal Senior Managers and accountability map.

9.1 Phase 1: Foundation (Months 1 -6)

The first phase should establish the baseline. Admiral should approve the Group assurance standard, reconcile systems and reconcile supplier inventories. Identify material systems across all business units and jurisdictions. Assign executive ownership and complete initial legal and impact classification.

The Group should also identify critical gaps in data, supplier assurance, customer-outcome monitoring and decision reconstruction. Operational, customer and financial baselines should be agreed before improvement targets are set.

By the end of month 6, all identified material systems should have an owner, jurisdiction, risk tier and approval status. Priority gaps should have named owners and deadlines.

9.2 Phase 2: Build and Validate (Months 7 - 18)

The second phase should focus on control implementation and validation. Admiral should independently validate critical and high-impact systems, introduce customer-outcome dashboards, improve decision records, correct data-lineage weaknesses and strengthen supplier contracts, as institutional expertise and tacit knowledge gathered through operational interaction are more valuable than the static documentation used to train models (Grant,

1996). Logging, security , model-change controls and approval gates should be embedded into development and procurement. Staff responsible for ownership, review and assurance should receive role-specific training.

By month 18, all critical systems should be validated or operating under formally approved remediation. At least 95% of high-impact systems should be validated or subject to a time-limited remediation plan. Critical suppliers should have completed assurance reviews and priority customer-outcome monitoring should be operational.

9.3 Phase 3: Embed and Demonstrate (Months 19 - 24)

The final phase should test operational effectiveness. Admiral should compare governance maturity across the UK, France Spain and Italy, conduct supplier continuity and exit exercises. They should also verify realised financial benefits and complete a risk-based Internal Audit testing.

The Group should also assess whether remediations have addressed underlying causes rather than closing individual actions. No material system should remain in operation without current approval or an authorised exception.

By the end of Month 24, cross-jurisdiction assurance comparison, critical supplier exercises and priority benefit verification should be complete. The Board should then approve the next assurance and investment cycle.

9.4 Programme Cost

The cost will depend on existing governance, staff expertise and technology capability. It may reduce incremental expenditure whilst unidentified remediation requirements may increase it.

9.5 Funding Gates and Success Measures

Funding should be gated. At month 3, Admiral should confirm portfolio scale, material gaps and revised cost. At month 6, Phase 2 funding should depend on approved

standards, assigned ownership and baselines. At month 18, final scaling should depend on completed priority validation, operational customer monitoring and credible early benefit evidence. Success must be measured through operating effectiveness. Core indicators include register completeness, validation coverage, decision-reconstruction time, review and overturn rates, false-positive fraud referrals and independently verified net value. Percentage-improvement targets should be fixed after Phase 1 baselines. This staged approach aligns NIST lifecycle risk management with EIOPA's proportionate insurance expectations (Tabassi, 2023; European Insurance and Occupational Pensions Authority, 2025b).

9.7 Reporting and Escalation

Reporting cadence should reflect impact. Critical exceptions, significant customer harm and security incidents require immediate escalation. High-impact systems should receive monthly operational review and quarterly independent challenge, while lower-impact tools on a proportionate cycle. A quarterly Board dashboard should show portfolio coverage, overdue validation, unresolved high-severity findings, customer-outcome trends, supplier dependencies and verified value. It should distinguish systems operating within tolerance, systems under time-limited remediation and systems suspended or withdrawn. Internal Audit should test a risk-based sample after controls have operated long enough to produce evidence, then track whether management closes findings sustainably rather than merely completing actions (Institute of Internal Auditors, 2020).

10. Conclusion

This report has established that Admiral's principal AI governance challenge is not the absence of structures. The Group has disclosed responsible-AI expertise, model governance, employee education and a GenAI Centre of Excellence. The strategic issue is whether these arrangements remain consistently embedded, independently validated and demonstrably effective as AI expands across businesses, jurisdictions and suppliers.

The analysis identifies an assurance gap between governance arrangements and public evidence of their operating effectiveness. AI creates opportunity in underwriting, pricing, claims, fraud and service, but increases lineage, model-change, cybersecurity, supplier and accountability risks. These become more significant where systems rely on opaque relationships or human review without genuine authority. Economic change can also alter model performance and weaken projected benefits.

The UK and EU converge around accountability, data quality, transparency, human oversight and protection from harm, but differ in method. This supports neither complete decentralisation nor rigid uniformity. Admiral needs a common assurance standard with jurisdiction-specific legal approval.

Admiral should therefore strengthen its architecture through integrated registration, impact-tiered validation, auditable records, customer-outcome monitoring, meaningful contestability, supplier assurance and verified benefits. This would protect customer trust and reputation while allowing valuable applications to scale. Long-term advantage will depend not simply on adopting AI faster than competitors, but on demonstrating that Admiral can deploy it reliably, explain its effects and correct harmful outcomes before they become systemic.

Reference List

Admiral Group plc (2024) “Admiral Selects Google Cloud to Accelerate Innovative Customer Experiences.” Available at: <https://www.admiralgroup.co.uk/news-releases/news-release-details/admiral-selects-google-cloud-accelerate-innovative-customer>.

Admiral Group plc (2025) *Recognising Excellence: Governance and Responsible AI at Admiral Group*. Cardiff: Admiral Group plc.

Admiral Group plc (2026a) *Annual Report and Accounts 2025*. Cardiff: Admiral Group plc. Available at: <https://admiralgroup.co.uk/static-files/1cc7d555-af0c-42c8-b2d9-8bae4036c278>.

Admiral Group plc (2026b) “Privacy and Data Protection Information.” Available at: <https://admiralgroup.co.uk/sustainability/esg-policies>.

Admiral Group plc (2026c) *Responsible AI and Governance Policy*. Cardiff: Admiral Group plc.

Admiral Group plc (2026d) *Sustainability Report 2025*. Cardiff: Admiral Group plc. Available at: <https://admiralgroup.co.uk/sustainability/esg-policies>.

Association of British Insurers (2026) *Motor Premiums Remain Stable, but Cost of Repairs Still High*. London: Association of British Insurers. Available at: <https://www.abi.org.uk>.

Autio, C. et al. (2024) *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*. Gaithersburg, MD: National Institute of Standards and Technology. doi:10.6028/NIST.AI.600-1.

Bank of England (2026) *Bank Rate Maintained at 3.75%: June 2026 Monetary Policy Summary and Minutes*. London: Bank of England.

Barney, J.B. (1991) “Firm Resources and Sustained Competitive Advantage,” *Journal of Management*, 17(1), pp. 99–120. doi:10.1177/014920639101700108.

van Bakkum, M., Zuiderveen Borgesius, F. and Heskes, T. (2025) “AI, Insurance, Discrimination and Unfair Differentiation: An Overview and Research Agenda,” *Law, Innovation and Technology*, 17(1), pp. 177–204. doi:10.1080/17579961.2025.2469348.

Bradford, A. (2020) *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press.

“Data (Use and Access) Act 2025” (2025). London: The Stationery Office.

DiMaggio, P.J. and Powell, W.W. (1983) “The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields,” *American Sociological Review*, 48(2), pp. 147–160. doi:10.2307/2095101.

Dubey, S.S., Astvansh, V. and Kopalle, P.K. (2025) “Generative AI Solutions to Empower Financial Firms,” *Journal of Public Policy & Marketing*, 44(1), pp. 45–62.
doi:10.1177/07439156241311300.

European Commission (2026a) *AI Act: Regulatory Framework for Artificial Intelligence*. Brussels: European Commission.

European Commission (2026b) *Guidelines for Providers and Deployers of High-Risk AI Systems: Draft Guidelines*. Brussels: European Commission.

European Commission (2026c) *Targeted Consultation on the Draft Guidelines for the Classification of High-Risk Artificial Intelligence Systems*. Brussels: European Commission.

European Data Protection Board (2024) *Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models*. Brussels: European Data Protection Board.

European Insurance and Occupational Pensions Authority (2025a) *From Traditional AI to Generative AI: Implications for the Insurance Sector*. Frankfurt: European Insurance and Occupational Pensions Authority.

European Insurance and Occupational Pensions Authority (2025b) *Opinion on Artificial Intelligence Governance and Risk Management*. Frankfurt: European Insurance and Occupational Pensions Authority.

European Union (2016a) “Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on Insurance Distribution (Recast),” *Official Journal of the European Union*, L 26, pp. 19–59.

European Union (2016b) “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation),” *Official Journal of the European Union*, L 119, pp. 1–88.

European Union (2022) “Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector (DORA),” *Official Journal of the European Union*, L 333, pp. 1–79.

European Union (2024) “Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act),” *Official Journal of the European Union*, L 2024/1689.

Financial Conduct Authority (2024) *Insurance Multi-Firm Review of Outcomes Monitoring under the Consumer Duty*. London: Financial Conduct Authority.

Financial Conduct Authority (2025) *Firms’ Treatment of Customers in Vulnerable Circumstances: Review*. London: Financial Conduct Authority.

Financial Conduct Authority (2026a) “About the Consumer Duty.” Available at: <https://www.fca.org.uk/firms/consumer-duty>.

Financial Conduct Authority (2026b) *FCA Publishes Landmark Review into Impact of AI on Retail Financial Services*. London: Financial Conduct Authority.

Financial Conduct Authority (2026c) *The Mills Review: Artificial Intelligence and the Future of Retail Financial Services*. London: Financial Conduct Authority.

Financial Conduct Authority and Information Commissioner's Office (2026) *Joint FCA and ICO Statement on Regulatory Expectations Regarding Firms' Approaches to Vulnerability-Related Data*. London: Financial Conduct Authority and Information Commissioner's Office.

Floridi, L. and Cowls, J. (2019) "A Unified Framework of Five Principles for AI in Society," *Harvard Data Science Review*, 1(1). doi:10.1162/99608f92.8cd550d1.

Freeman, R.E. (1984) *Strategic Management: A Stakeholder Approach*. Boston, MA: Pitman.

Grant, R.M. (1996) "Toward a Knowledge-Based Theory of the Firm," *Strategic Management Journal*, 17(S2), pp. 109–122. doi:10.1002/smj.4250171110.

Information Commissioner's Office (2026a) *Data Protection: Automated Decision-Making*. Wilmslow: Information Commissioner's Office.

Information Commissioner's Office (2026b) *ICO Consultation on the Draft Guidance About Automated Decision-Making, Including Profiling*. Wilmslow: Information Commissioner's Office.

Information Commissioner's Office (2026c) *The Data Use and Access Act 2025: Summary of the Changes to Data Protection Law*. Wilmslow: Information Commissioner's Office.

Institute of Internal Auditors (2020) *The IIA's Three Lines Model: An Update of the Three Lines of Defense*. Lake Mary, FL: Institute of Internal Auditors.

International Monetary Fund (2026) *Artificial Intelligence and Cybersecurity in the Financial Sector*. Washington, DC: International Monetary Fund.

Lauchlan, S. (2026) "'A' for AI, 'I' for Insurance (3/3) - How Admiral Is Driving Ahead to Reach Its AI Destination." Available at: <https://diginomica.com/ai-i-insurance-33-how-admiral-driving-ahead-reach-its-ai-destination>.

Morrison, J. (2020) *The Global Business Environment: Towards Sustainability?* 5th edn. London: Red Globe Press.

Nannini, L., Balayn, A. and Smith, A.L. (2023) "Explainability in AI Policies: A Critical Review of Communications, Reports, Regulations, and Standards in the EU, US, and UK," in *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)*. Chicago, IL, USA: Association for Computing Machinery, pp. 1198–1212. doi:10.1145/3593013.3594074.

Office for National Statistics (2026) *Consumer Price Inflation, UK: May 2026*. Newport: Office for National Statistics.

Porter, M.E. (2008) “The Five Competitive Forces That Shape Strategy,” *Harvard Business Review*, 86(1), pp. 78–93.

Smith, A. (2026) *AI in Financial Services: Shaping Our Approach Through Industry Engagement*. London: Financial Conduct Authority.

Tabassi, E. (2023) *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg, MD: National Institute of Standards and Technology.
doi:10.6028/NIST.AI.100-1.

Tomei, P.M., Jain, R. and Franklin, M. (2025) *AI Governance Through Markets*. arXiv.
doi:10.48550/arXiv.2501.17755.

Zuiderveen Borgesius, F. *et al.* (2025) “Discrimination and AI in Insurance: What Do People Find Fair? Results from a Survey,” *European Journal of Risk Regulation*. Cambridge: Cambridge University Press.