GenAirate
TECHNOLOGIES

WHITEPAPER

LEVERAGING AI FOR THIRD-PARTY RISK MANAGEMENT AND OPERATIONAL RESILIENCE IN THE INSURANCE AND REINSURANCE INDUSTRY

Executive Summary

Operational resilience is essential for the insurance and reinsurance sector, ensuring firms can withstand, recover from and adapt to disruptions. A critical component of this resilience is Third-Party Risk Management (TPRM), which addresses risks posed by vendors, partners and service providers. As insurers increasingly rely on third parties for essential services, they face challenges such as operational instability, cybersecurity threats and regulatory compliance issues.

Introduction

Operational Resilience is defined as the ability of firms and the sector to prevent, adapt, respond to, recover from and learn from operational disruptions. An operationally resilient system can absorb shocks rather than compound them and is critical for consumers, firms and financial markets.

Third Party Risk is a fundamental component of Operational Resilience. While engagements with third parties enhance business operations and efficiency, they also introduce risks such as operational instability, data breaches, financial vulnerability and regulatory non-compliance.

Third Party Risk Management (TPRM) focuses on identifying and mitigating risks associated with third-party suppliers, partners, service providers, intra-group companies and vendors who deliver essential products or services.

As businesses become increasingly interconnected, organisations rely more on third parties to provide critical services, support business growth and enable digital transformation.

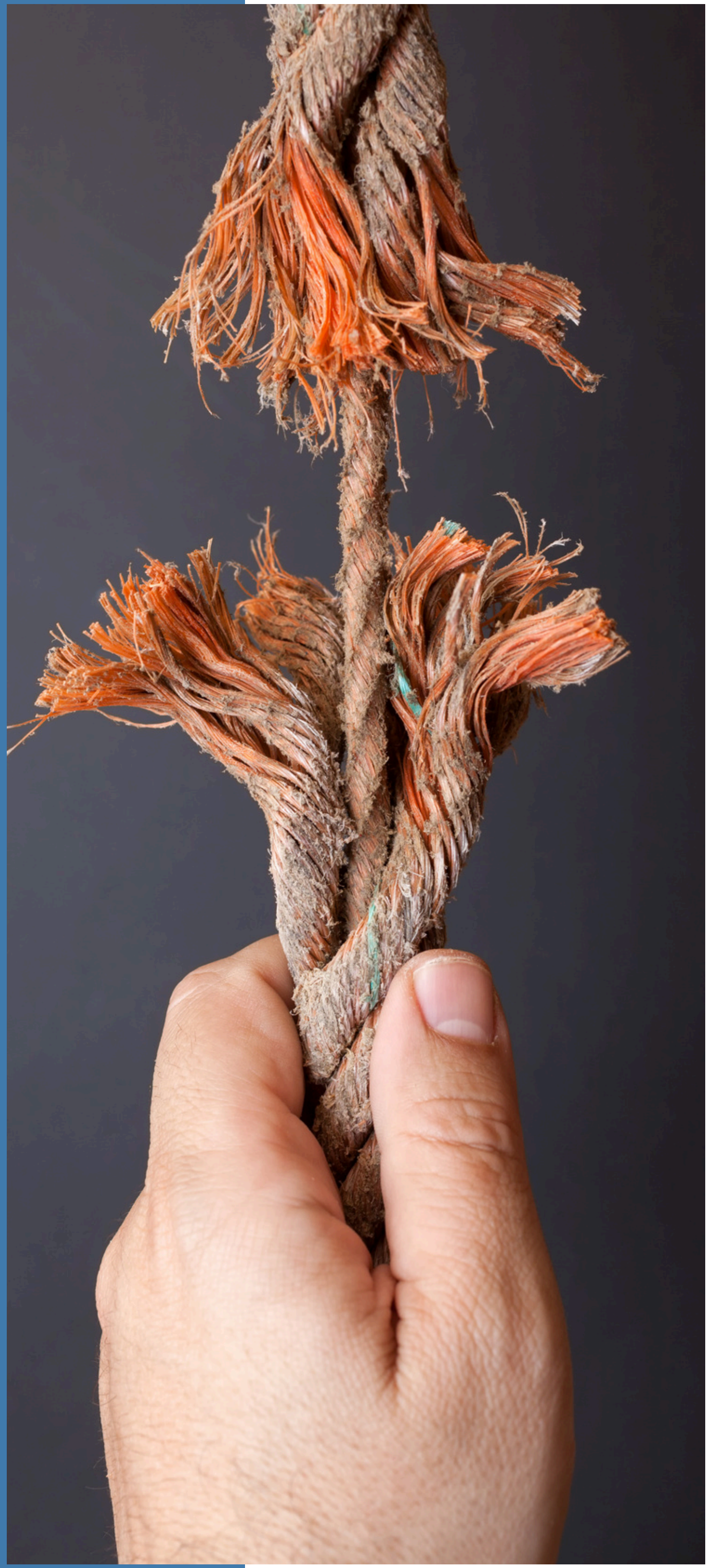
The Role of IAIS in Operational Resilience

The International Association of Insurance Supervisors (IAIS) Operational Resilience Objectives, published in October 2024, have significantly impacted the insurance industry by introducing a standardised framework for managing disruptions. These objectives require insurers to establish robust systems that can withstand and recover from disruptions, protecting policyholders and maintaining market stability.

The IAIS framework includes:

- **Enhanced risk management:** Insurers must proactively identify, assess and mitigate operational risks, such as cyber threats, natural disasters and system failures.
- **Business continuity planning**: Companies must ensure critical services remain operational during disruptions.
- **Incident response capabilities:** Rapid detection and containment of disruptions to minimise customer and business impact.
- **Impact tolerance setting:** Definition of acceptable disruption levels based on criticality and impact.
- **Scenario testing and stress testing**: Regular evaluations to enhance preparedness for disruptions.
- **Regulatory scrutiny:** Supervisory authorities will assess compliance with IAIS objectives, potentially enforcing stricter regulations.

Overall, these requirements encourage insurers to develop a proactive resilience strategy, ensuring sustained operations during challenging circumstances.



Current Challenges with Risk Management in TPRM and Operational Resilience

Despite increased regulatory attention, risk management practices within the insurance sector face significant challenges:

- Manual, inefficient processes – Risk assessments often rely on spreadsheets and questionnaires, leading to outdated and incomplete data.
- Fragmented assessments – Different functions assess risks in silos, limiting a comprehensive understanding of third-party risks.
- Scalability concerns – The growing volume of third-party engagements overwhelms traditional risk management approaches.
- Complex service delivery models – Multi-tiered vendor ecosystems introduce additional risk factors across jurisdictions.
- Lack of continuous monitoring – Static assessments fail to capture real-time risks and emerging vulnerabilities.

These challenges create operational blind spots, making it difficult to ensure resilience in a rapidly evolving risk environment.

How Generative AI Can Enhance Operational Resilience

Generative AI offers significant potential in improving resilience across key areas:

Data Analysis and Prediction

- Synthetic Data Generation: AI can create synthetic datasets to validate models without exposing sensitive data.
- Pattern Recognition: AI models detect anomalies and assess risks across multiple domains.

Risk Assessment and Prediction

- Predictive Analytics: AI analyses historical data to predict vulnerabilities and risk exposures.
- Scenario Modelling: AI simulates potential disruptions, supporting proactive resilience planning.

Compliance and Monitoring

- Automated Monitoring: AI continuously scans for compliance violations and risk indicators.
- Natural Language Processing (NLP): AI-driven document analysis enhances compliance oversight.

Cybersecurity and Threat Detection

- Anomaly Detection: AI identifies unusual activities that may indicate cyber threats.
- Vulnerability Management: AI assesses system weaknesses and recommends security patches.

Supply Chain Resilience

- Predictive Disruption Detection: AI anticipates supply chain disruptions due to external factors.
- Scenario Planning: AI evaluates contingency strategies to mitigate supply chain failures.

Incident Response and Recovery

- Real-Time Monitoring: AI enables rapid incident detection and response.
- Automated Recovery Protocols: AI helps organisations restore operations with minimal downtime.

Decision Support and Business Continuity

- Dynamic Decision-Making: AI supports real-time risk-based decision-making.
- Adaptive Response Strategies: AI assists in adjusting operational strategies during disruptions.

Fraud Detection and Prevention

- Transaction Monitoring: AI detects suspicious patterns that may indicate fraudulent activities.
- Behavioural Analysis: AI analyses anomalies in transaction behaviour to flag potential misconduct.

Training and Education

- Simulation-Based Training: AI-driven simulations improve staff preparedness for various risk scenarios.
- Automated Knowledge Management: AI generates documentation, playbooks, and training resources.

However, the adoption of AI for operational resilience must be balanced with ethical considerations, data security and regulatory compliance. Collaboration between risk, AI, legal and IT professionals is essential for successful implementation.

Potential Risks Introduced by AI

Fig. 1

Fig. 1 Explains that, despite its benefits, AI adoption introduces new risks:

AI RISK	POTENTIAL IMPACT	MITIGATION STRATEGY
Data Privacy & Security	Data breaches, regulatory non-compliance	Encryption, strict access controls
Operational Failures	Service interruptions due to AI malfunctions	Regular testing, human oversight
Bias & Ethical Risks	Discriminatory decision-making, reputational damage	Bias audits, diverse training data
Cybersecurity Threats	AI exploitation through adversarial attacks	Robust security measures, AI risk monitoring
Regulatory Compliance Challenges	Complex legal frameworks for AI governance	Continuous compliance tracking, legal oversight
Vendor Lock-in Risks	Dependence on specific AI providers	Multi-vendor strategy, interoperability focus

To mitigate these risks, insurers should:

- Conduct due diligence on AI vendors.
- Implement robust AI governance and ethical frameworks.
- Ensure continuous monitoring and model validation.
- Maintain human oversight to supplement AI-driven decisions.

Conclusion

AI-driven solutions are transforming operational resilience by enabling insurers to enhance third-party risk management, improve compliance and strengthen cybersecurity. However, successful AI adoption requires a balanced approach that addresses regulatory, ethical and operational risks.

Example Use Case of Gen AI for Risk Mitigation

Fig. 2

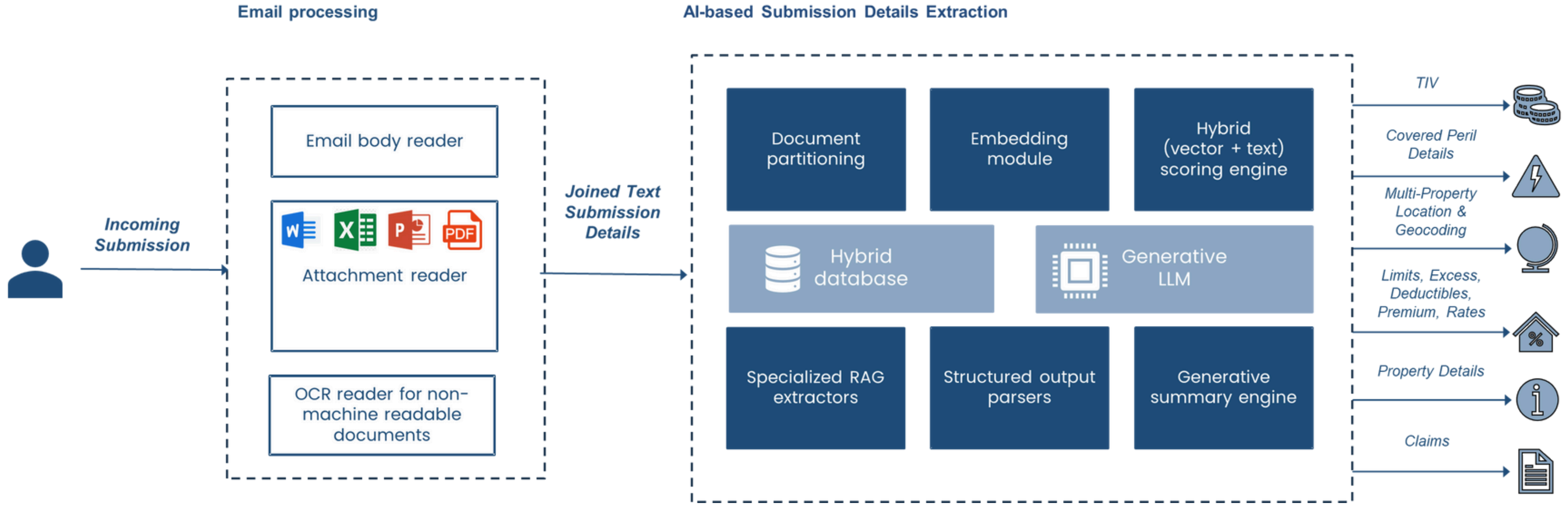

Email processing
AI-based Submission Details Extraction
Incoming Submission
Email body reader
Attachment reader
OCR reader for non-machine readable documents
Joined Text Submission Details
Document partitioning
Embedding module
Hybrid (vector + text) scoring engine
Hybrid database
Generative LLM
Specialized RAG extractors
Structured output parsers
Generative summary engine
TIV
Covered Peril Details
Multi-Property Location & Geocoding
Limits, Excess, Deductibles, Premium, Rates
Property Details
Claims

Fig. 2 Diagrams a use case for how a generative AI insurtech tool like **GenAirate Technologies SnapLine Platform** can be fully customised to take disparate incoming submissions and standardise the output. This doesn't remove human oversight, but it does allow for rapid, error-free handling; reducing several risk factors that damage operational resilience.

CHARLES FORDE

OPERATIONAL RISK ADVISOR

Frmr COO and Head of
Operational Risk at UBS,
Nomura, Allied Irish Banks, EY

" GenAI can enhance Operational Resilience and TPRM by enabling smarter risk management, automation and response strategies in key areas such as underwriting, claims processing and customer engagement. By leveraging AI-driven insights, insurers can proactively anticipate disruptions, strengthen third-party risk oversight and ensure business continuity in an increasingly volatile landscape."

Bibliography

- International Association of Insurance Supervisors - Operational Resilience objectives and toolkit, October, 2024
- UK Government: Official Statistics - Report on Cyber Security Breaches Survey 2024
- Financial Conduct Authority - Operational Resilience Insights and observations for firms
- Prudential Regulation Authority - Operational Resilience Rulebook
- European Union - Digital Operational Resilience Act
- Prudential Regulation Authority - Statement on Insurance Supervision Priorities 2025
- International Association of Insurance Supervisors - Issues Paper on Insurance Sector Operational Resilience
- Supply Wisdom - 'ION Group Ransomware Attack: Was it Predictable?' by Victor Meyer, Chief Strategy Officer
- Massachusetts Institute of Technology, Sloan School of Management - Responsible AI Initiative and Report

GenAirate
TECHNOLOGIES

This whitepaper is sponsored by GenAirate Technologies

To explore how AI can strengthen your organisation's operational resilience, please contact Thomas.Beckett@genairate.io or visit genairate.io for more insights.