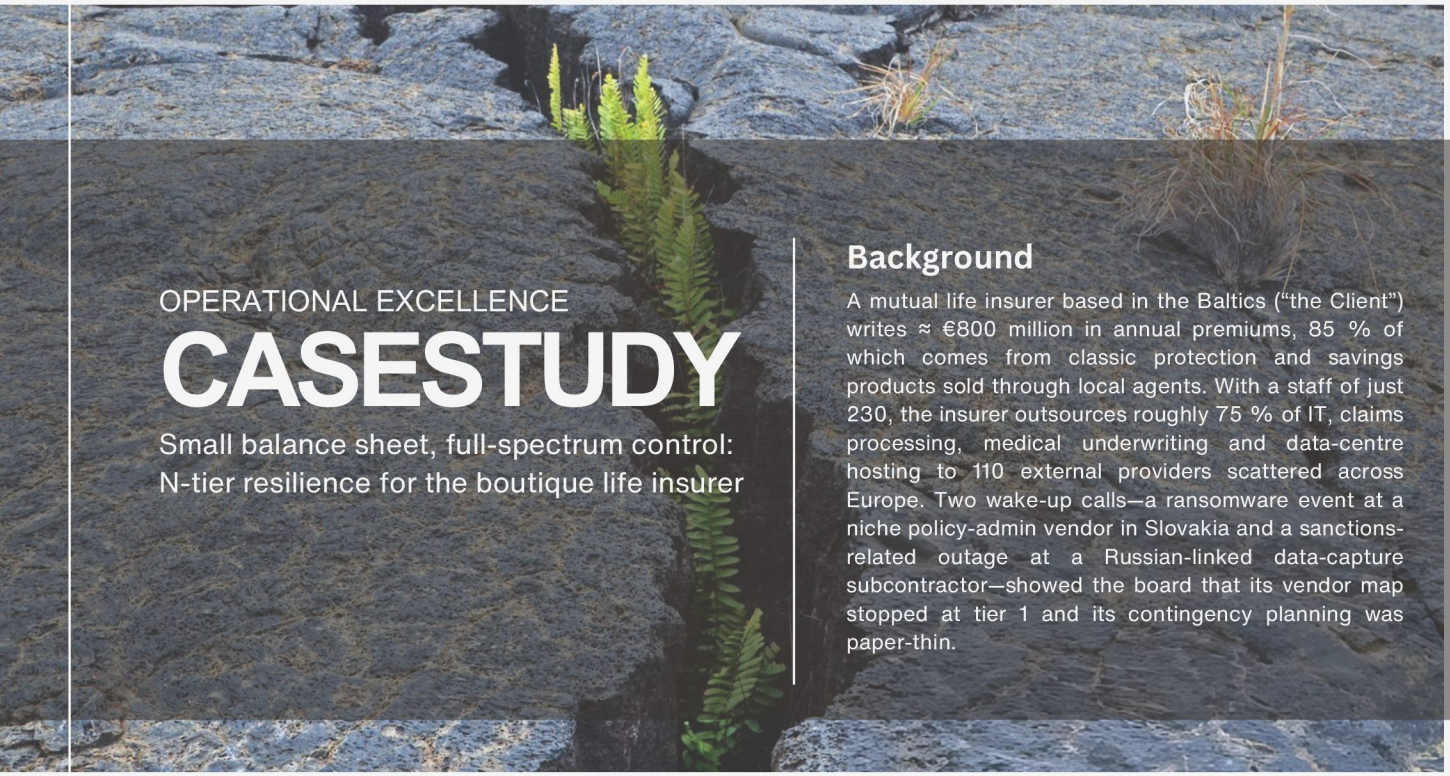

OPERATIONAL EXCELLENCE

CASESTUDY

Small balance sheet, full-spectrum control:
N-tier resilience for the boutique life insurer

Background

A mutual life insurer based in the Baltics ("the Client") writes ≈ €800 million in annual premiums, 85 % of which comes from classic protection and savings products sold through local agents. With a staff of just 230, the insurer outsources roughly 75 % of IT, claims processing, medical underwriting and data-centre hosting to 110 external providers scattered across Europe. Two wake-up calls—a ransomware event at a niche policy-admin vendor in Slovakia and a sanctions-related outage at a Russian-linked data-capture subcontractor—showed the board that its vendor map stopped at tier 1 and its contingency planning was paper-thin.

Introduction

Enigma Risk Advisory, was engaged as a strategic advisor to "right-sized" Third-Party & Supply-Chain Risk-Management (TPRM) programme that would:

- Deploy Gen-AI-powered, always-on N-tier risk sensing across every supplier and sub-supplier.
- Convert formerly optional controls into hard-law compliance with Digital Operational Resilience Act (DORA) , Network and Information Security Directive 2022/2555 (NIS 2), European Insurance and Occupational Pensions Authority (EIOPA) outsourcing rules, and the incoming Corporate Sustainability Due-Diligence Directive (CSDDD).
- Bake ESG and ethical-sourcing metrics directly into quarterly vendor scorecards.
- Provide a digital-twin map plus what-if stress-testing for cyber, climate and geopolitical shocks.
- Create a friend-shoring playbook so critical workloads can be shifted rapidly to lower-risk locations.

Challenges Faced

Theme	Pain Point	Consequence for a Small Insurer
Visibility Gaps	Only 38% of tier-2/3 subcontractors identified; no dependency graph	Hidden single-points-of-failure
Regulation Gets Teeth	DORA & NIS 2 elevate ICT-outage controls; CSDDD adds supply-chain liability	Potential fines up to 2% of GWP; officer liability
ESG Integration Lag	Asset-side ESG tracked, vendor-side ignored	Reputational and sustainability-rating risk
Static Risk Assessments	Annual questionnaires only	Late response to sanctions, ransomware, extreme weather
Geopolitical Shifts	40% of IT spend in higher-risk or high-energy-cost regions	Service disruption & cost volatility

OPERATIONAL EXCELLENCE

CASESTUDY

Small balance sheet, full-spectrum control:
N-tier resilience for the boutique life insurer

Results and Impact

- N-tier mapping coverage jumped from 38% to 93% in eight weeks; unknown dependencies cut by 78 %.
- Early-warning lead-time improved by 21 days thanks to Gen-AI risk-signal engine.
- €3.2 million economic-capital release after digital-twin stress tests justified targeted rather than blanket contingencies.
- All critical vendors now scored on ESG & ethical-sourcing, leading to two strategic exits and one rapid remediation.
- Zero material findings in the insurer's first DORA self-assessment; supervisor letter called the approach "proportional best practice."

Solutions Implemented

a. Gen-AI, Always-On Risk-Sensing Hub

- Multilingual LLM ensemble ingests news, sanctions lists, CVE feeds, realtime climate alerts and vendor financials; semantic search links signals to supplier IDs.
- A Teams bot pushes high-severity alerts within 15 minutes, tagging contract owner and risk category.

b. Digital-Twin Dependency Graph & What-If Simulator

- Neo4j graph with 3 100 nodes (applications → vendors → sub-vendors → geo assets).
- Monte-Carlo engine runs 500 cyber, flood and geopolitical scenarios; outputs downtime, solvency impact and recovery options.

c. Hard-Law Control Translation

- Parsed DORA, NIS 2, EIOPA and CSDDD into 73 atomic controls embedded as policy-as-code checks in onboarding.
- Purchase-order workflow blocked until exit-plan test and data-protection clauses are confirmed.

d. ESG & Ethical-Sourcing Scorecards

- Aggregates EcoVadis ratings, NGO human-rights indices and self-reported emissions.
- Vendors below 70 th percentile enter a 90-day remediation track or are off-ramped.

e. Friend-Shoring & Diversification Blueprint

- Total-cost-of-risk model recommended dual-sourcing cloud DR in Finland & Spain; moved claims-processing from Belarus to Latvia.
- Escrowed source code and lift-and-shift clauses cut maximum tolerable outage by 57 %.

f. Culture & Operating Model

- TPRM Guild (Procurement, Cyber, Sustainability, Legal) meets bi-weekly; dashboards live in Confluence.

Quarterly "Black-Swan Game-Day" drills ransomware, sanctions shock and severe-heat data-centre loss,

Conclusion

In under nine months the Client shifted from after-the-fact supplier oversight to proactive, proportional N-tier risk orchestration that meets tough EU regulations, satisfies ESG-savvy stakeholders and safeguards policyholders against geopolitical shock. The digital-twin cockpit and Gen-AI alerts now anchor every board discussion on outsourcing, growth and capital—proof that even a sub-€1 billion life insurer can achieve enterprise-class resilience.