opentext™

POINT OF VIEW

Strengthening digital trust across the insurance enterprise

Integrated information management and AI-driven governance help insurers secure data, prove compliance, and manage cyber risk across complex ecosystems

Business backdrop

Insurance is modernizing fast, digitizing customer journeys, connecting to brokers and partners in real time, and adopting AI to speed underwriting and claims. That speed comes with rising exposure. Fragmented legacy estates and siloed repositories complicate cyber hygiene and recordkeeping, while expanding third-party networks multiply attack surfaces and operational dependencies. Regulators are simultaneously tightening expectations for resilience, data privacy, and model risk management in AI. Maintaining trust in data and in the outcomes of automated decisions has become a competitive necessity, not merely a compliance task. McKinsey highlights that derisking emerging technologies is now central to financial services strategy and oversight.[2]

Across the sector, security programs are being re-tooled to address ransomware, supply chain compromise, and systemic cyber events, while operational-resilience mandates require verifiable controls, audit trails, and rapid recovery. Boards want assurance that customer data is protected, third-party concentration risks are understood, and AI systems are explainable and governed. The mandate for insurers is clear: embed cyber resilience and information governance into everyday operations so that security, compliance, and automation reinforce each other, enabling growth with confidence.

> **"Cyber resilience is now a fundamental business capability for insurers, requiring real-time detection, rapid response mechanisms, and proactive scenario planning for systemic disruptions from ransomware, supply chain failures, and geopolitical cyber events."[1]**

[1] Accenture, *5 predictions for the insurance industry in 2025*, January 2025

[2] McKinsey & Company/Institute of International Finance, *The Cyber Clock Is Ticking: Derisking Emerging Technologies in Financial Services*, March 2024

"Third-party cyber risk management, in particular, faces increased attention… Carriers are called to examine who the core third parties are, and what their cyber risk levels are… Investors and regulators want to know if the carrier has additional concentration risk, and what a third party's software 'bill of materials' is.."[3]

Complex ecosystems, expanding exposure

Insurers work through vast networks of brokers, administrators, and technology vendors. In an analysis of 150 insurance-related firms, 59 percent of breaches involved third-party attack vectors, roughly double the global average.[4]

Legacy infrastructure, modern demands

Seventy-four percent of insurers still run core processes on aging platforms. Estimates indicate about 70 percent of IT spend goes to maintaining "old tech," hampering efficiency and compliance readiness.[5]

Responsible AI and compliance convergence

Generative AI and cloud adoption are accelerating, yet without guardrails they introduce auditability and fairness risks. Munich Re flags rapid advances in AI and cloud as key cyber-risk drivers.[6]

"Strong data and cybersecurity data protocols earn policyholder trust and loyalty. They safeguard sensitive customer data, including personal information and claims history, to maintain or improve retention rates and market reputation."[7]

[3] McKinsey, *Navigating shifting risks in the insurance industry*, July 2024

[4] SecurityScorecard, *59% of Breaches Impacting Insurance Sector Caused by Third-Party Attack Vectors*, 2024–2025 update

[5] Insurance Business America, *Are legacy systems weighing down the insurance industry?*, 2023–2024

[6] Munich Re, *Cyber Insurance: Risks and Trends 2024*, 2024

[7] Capgemini, *Capgemini Financial Services Top Trends 2025: Health Insurance*, January, 2025

OpenText vision

Build a trusted information foundation

Our vision is an insurance enterprise where security, governance, and automation converge to create transparency and resilience, so teams can innovate without compromising control. With decades in enterprise information management, we help unify structured and unstructured content under consistent policies, permissions, and lifecycle rules. This supports privacy, evidentiary recordkeeping, and faster regulatory response.

Automate compliance and assurance

By equipping content workflows with policy-driven retention, legal holds, and automated evidence capture, compliance shifts from periodic effort to continuous assurance. Audit trails become complete and queryable, reducing manual effort and speeding attestations.

Enable responsible, explainable AI

AI adds real value when it is governed. We help insurers establish transparent data lineage, document model intent and performance, and enforce guardrails on usage, so automated decisions remain traceable and defensible.[8]

Proof through experience

Insurers that unify information management, governance, and AI oversight gain not only compliance assurance but also the agility to innovate with confidence. Customers cite stronger access control, centralized oversight, and demonstrable improvements in security posture when adopting our best-practice frameworks, alongside secure developer tooling and continuous testing in software pipelines to raise quality and reduce vulnerability risk.

> “Cyber resilience is now a fundamental business capability for insurers, requiring real-time detection, rapid response mechanisms, and proactive scenario planning.”[9]

> “Leveraging OpenText, our end users and administrators have secure, centralized, and audited access to our applications as well as to protected servers and endpoints. Multi-factor authentication has improved our security, enabling our users access to our systems securely from any location.”

Hamza Mahafzah
Head of Enterprise
Architecture, Najm

[8] OpenText, *Responsible AI and Information Governance in Financial Services*, 2024

[9] Accenture Insurance Blog, *Cyber resilience for insurers in 2025*, 2025

Comprehensive table of potential solutions

Capability area	Relevance to insurers	Value proposition/Outcome
Monitoring and analytics	Enterprise-wide event correlation and security insight	Reduce mean time to detect, improve visibility, support audits
Application security	Shift-left and runtime safeguards for policy, billing, claims	Prevent exploitable defects, demonstrate secure SDLC
Forensics and investigation	Defensible evidence capture across endpoints and repositories	Speed investigations; satisfy regulatory examinations
Data protection	Format-preserving encryption/ tokenization for PII/PHI/PCI	Protect data in use, motion, and at rest; enable privacy compliance
Threat intel and MDR	24×7 awareness of emerging threats relevant to insurance	Prioritize and mitigate sector-specific risks
AI and analytics governance	Insight extraction with explainability and controls	Use AI confidently with documented lineage and outcomes
Content and records governance	Policy-driven retention, legal holds, discovery readiness	Reduce compliance exposure, streamline responses
Business network/API control	Secure, monitored data exchange with brokers and TPAs	Reduce third-party risk, increase transaction reliability
Backup and cyber resilience	Orchestrated recovery for critical workloads	Minimize downtime, test recovery against ransomware
Communications and experience controls	Governed customer communications at scale	Ensure accuracy, consistency, and traceability

Business outcome

Insurers that combine robust information governance with automated controls and cyber-resilience practices realize measurable gains:

- **Operational resilience.** Centralized monitoring, immutable backups, and tested recovery reduce downtime and improve service continuity during cyber incidents or supplier outages.
- **Regulatory confidence.** Unified policy enforcement and comprehensive audit trails accelerate inquiries, exams, and attestations, lowering the burden on risk, compliance, and IT.
- **Efficiency at scale.** Automated retention, evidence capture, and reporting free expert capacity, speeding claims and underwriting decisions while reducing manual rework.
- **Risk reduction.** Encryption, least-privilege access, and secure SDLC practices drive down data-exposure likelihood and material impact, especially across third-party integrations.[10]

[10] SecurityScorecard, *59% of Breaches Impacting Insurance Sector Caused by Third-Party Attack Vectors*, 2024–2025 update

- **Sustainable innovation.** Governed AI enables new experiences and productivity gains with documented lineage and explainability, building trust with customers, regulators, and partners.[11]

The net effect is a shift from reactive controls to proactive assurance. Organizations move from siloed tooling to an integrated operating model where information is protected by default, processes are instrumented for compliance, and analytics are deployed with guardrails. This reduces total cost of control, limits reputational downside (Aon estimates reputational events after cyber incidents can reduce shareholder value by ~27% on average), and creates space to pursue growth in new products, channels, and partner ecosystems with confidence.[12]

Next steps

1. **Introductory alignment.** Set up a meeting between OpenText and your Global Account Director and security, risk, and data leaders to align objectives, constraints, and regulatory expectations.
2. **Joint roadmap exchange.** Host a half-day working session to review current capabilities, third-party landscape, and priority use cases (e.g., claims modernization, AI governance, third-party risk).
3. **Value and architecture assessment.** Partner with the OpenText Business Value Consulting team to quantify benefits (effort reduction, audit-cycle time, MTTR, recovery metrics) and outline a target reference architecture and adoption plan.

Why OpenText?

OpenText unites information governance, data protection, and intelligent automation in a single, integrated approach tailored to insurance. We bring deep financial services expertise, proven frameworks for regulatory alignment, and tooling that scales across content, data, applications, and third-party ecosystems. The result is trusted information, resilient operations, and responsible AI, so your teams can move faster with confidence.

Contact us

Monica Hovsepian
Global Senior Industry Strategist,
Financial Services

mhovsepi@opentext.com
linkedin.com/in/monicahovsepian

> “We have introduced a best practice deep defense framework, including dynamic code scanning and intrusion testing, supported by documentation and training. [OpenText Core Application Security] has been fully integrated in the effort to improve the quality and, more specifically, the security of the applications we deliver to the business.”

Xavier Pernot
IS Security Specialist,
Generali France

Read the customer story ›

[11] Munich Re, *Cyber Insurance: Risks and Trends 2024*, 2024

[12] Aon, *2025 Global Cyber Risk Report: Reputation Risk Events Can Reduce Shareholder Value by 27%*, June 17, 2025