

Global Insurer Develops Robust Cyber Resiliency and Data Architecture



Data Mesh, Cyber-resilience, and IAM Consolidation and Modernization for a Global Trade Credit Insurance Firm

Our client provides trade credit insurance, surety and collections services to businesses in more than 50 countries

Credit Insurance

The Challenges

Our client is a global credit insurance issuer with a highly diverse customer base, operating large platforms for managing credit insurance and debt collection across the business lifecycle. The company's core product — Credit Insurance — helps protect international trading firms from losses caused by their customers' insolvency, or failure to pay under contract terms.

The insurer recently faced two simultaneous challenges to its business model, ones that it was hoping to solve by leveraging a programmatic approach embedded with innovative technologies such as AI. The insurer had a technical need to modernize its data architecture and security posture, while also putting IT systems in place to comply with a new legal requirement and accounting standard, IFRS 17, which mandated five-year future cashflow forecasts for premium calculation.

IFRS 17 is a Financial Reporting Standard that took effect in Europe in January 2023. The standard applies to insurance and reinsurance contracts issued or held by an insurer. Under the IFRS 17 general model, insurance contract liabilities must be calculated as the expected

present value of future insurance cash flows, with provisions for non-financial risks. While conforming to this new standard, our client also needed to better protect its customers' sensitive data while taking advantage of Generative AI (GenAI) for productivity and efficiency benefits. This would require consolidating and modernizing Identity and Access Management (IAM) and implementing Zero-Trust Security across different regions, as well as for companies acquired in the UK, Spain, and Netherlands. The insurer was also looking for the right partner to optimize its GenAI strategy from a security perspective.

A multifaceted effort of this scale and complexity required an experienced consulting and managed services partner who could bring a programmatic approach. The insurer turned to Persistent to create the data architecture required to meet its security challenges and implement IFRS 17 reporting. The project mandate: "Bring in the best engineering practices, modernize the current state, and assure regulatory compliance."

The Solutions

Persistent commenced the program by building a five-year roadmap for cyber resilience, based on cloud native security support and DevSecOps process enablement. In addition, the roadmap called for significant data model enhancements and implementing a Zero-Trust Framework across all IT

ecosystems (application, infrastructure, and data). We initially engaged with the CISO office in a consulting capacity, then transitioned to implementation work, when our team enhanced the insurer's security posture end-to-end and set up modernized IAM. Persistent also identified

key decision points on tools consolidation, and changes to business processes that would reduce customizations and maintenance costs.

Our architectural consultants recommended that the insurer transition from Data Ops to Data Mesh and helped build a strategic roadmap — this would enable IFRS17 compliance and readiness for any future changes. The mesh paradigm decentralizes data ownership by transferring responsibility from the central data team to the business units that create and consume data. The result is independent, interoperable, business-owned data products that operate as microservices. Data Mesh architecture was key to enabling platform management for IFRS17 regulation and compliance, and it supports the core principles of DevOps.

Our solution team also addressed a series of serious open issues, by determining optimal strategies and then blueprinting and implementing solutions. Our client had been hampered by disparate architecture and operations teams, as well as a huge backlog of security projects due to the operations teams being overloaded with business-as-usual activities. Further, the existing IAM solution was unstable due to a fragmented identity and access data

repository — and mergers had brought in additional vendors, increasing security risks and maintenance costs. Once these issues had been resolved, we were able to deliver a smooth transition with transformation /stabilization and zero disruption to inflight programs.

Finally, Persistent enabled Connected Intelligence by integrating multiple data domains into the Data Mesh, and we delivered an optimized Identity Governance and Administration (IGA) and Single Sign-On (SSO) tool selection based on a nine-point inspection approach. These new tools allowed centralized IAM across the enterprise. We wrapped up the project by developing and presenting to the company board a roadmap for building a corporate Cyber Resilience Office.

For GenAI, Persistent's CTO Office engaged with our client's CISO Office to create the right AI security posture. We set up guardrails for a few selected departments to experiment with GenAI tools, without exposing any organizational data. We're continuing to evaluate market trends and compare the available tools in order to bring the insurer up to date with their Zero-Trust Security posture.

The Outcomes

The business value of Persistent's solution and approach can be simply expressed: Our client achieved **full compliance with IFRS 17, Zero-Trust Security**, and a **20% cost savings through Azure cloud services optimization**. Further, the flexible Agile operating model — introduced with the solution — enabled the insurer to **transition into an SLA-driven outcome-based model in just three months**.

Our solution also featured a fully transparent cost breakdown, with a clear team structure — allowing our client the flexibility to ramp up the transformation team as needed per the solution roadmap. The company board subsequently approved the budget for the Cyber Resilience Office, along with our recommended consolidation of tools and process definitions.

Technologies Used

Azure

Axio

Databricks

See Beyond, Rise Above

About Persistent

With over 23,000 employees located in 21 countries, Persistent Systems (BSE & NSE: PERSISTENT) is a global services and solutions company delivering Digital Engineering and Enterprise Modernization. As a participant of the United Nations Global Compact, Persistent is committed to aligning strategies and operations with universal principles on human rights, labor, environment, and anti-corruption, as well as take actions that advance societal goals. With 268% growth since 2020, Persistent is the fastest-growing Indian IT Services brand according to Brand Finance.

UK

Level 1,
Broadgate Tower,
20 Primrose Street,
London EC2A
2EW, United Kingdom

USA

Persistent Systems, Inc.
2055 Laurelwood Road,
Suite 210, Santa Clara,
CA 95054
Tel: +1 (408) 216 7010

India

Persistent Systems Limited
Bhageerath, 402
Senapati Bapat Road
Pune 411016
Tel: +91 (20) 6703 0000



Persistent

www.persistent.com