QUALITEST™

Strategic Digital Engineering Quality Assures Cyber Security & Data Compliance for New IaaS Product for Top UK Insurance Firm

Challenge

Assure data compliance and cyber security for new cloud-based product.

Move from legacy to IaaS platform for progression of AI-driven digital transformation.

Solution

Map requirements and test plan to evolving data privacy/ cyber security cloud standards.

Shift left and automate all functional and non-functional testing.

Results

Established framework for long-term cyber security, data compliance and business change capability.

Testing time reduced from 118 days to 2 hours.
12x faster time to release.

Client overview

The Client is a leading service provider for personal, commercial, motor, property and protection insurance. Serving over 2 million customers in the UK alone, the organization generated premiums worth over £800 million in 2021. The business is served via a variety of broker, intermediary and direct distribution channels.

The Client has over 60 years industry experience and over 2000 employees spread over several locations in the UK. Their talented workforce includes a large internal software development capability whose sole focus is digital transformation and cloud adoption.

High hopes for a ground-breaking cloud product

In 2018 our Client began a partnership with a globally leading health insurance provider to deliver a disruptive digital product that would reward customers for driving safely. The partners aimed to deliver an offering that would prosper in today's competitive insurance market while progressing their ongoing digital transformations. Our Client's specific goals were:

- To increase new business growth through affinity partnerships
- To move from legacy on-premise systems to a secure cloud-hosted IaaS solution, enabling full digital transformation to an AI-powered, big data-driven infrastructure
- To implement a Continuous Integration/Continuous Delivery (CI/CD) pipeline capable of rapid deployment and efficient business change.
- To adhere to data compliance and cyber security regulations from the outset.

This product would be built almost entirely on cloud-hosted technology to enable scaling with future business growth, and include:

- The Client's new microservices platform.
- An InsurTech SaaS provider, to allow simple integration with other insurance industry systems and prospective business partners.
- A customer-facing web application.
- TAPIs for enabling integration with the Internet of Things, to increase the number of data outputs for analysis.
- Various event-driven technologies.

Cloud adoption would facilitate the storage and rapid analysis of the big data being collected, using AI technology to increase competitive advantage and optimize customer experience. However, cloud hosting also meant strict adherence to cloud-specific compliance regulations related to data privacy/protection and cyber security, some of which were just emerging.

Automate first and shift left

A key challenge at the start was the lack of data compliance and non-functional (specifically cyber security) requirements. At our Client's request, Qualitest led a series of workshops that resulted in a clearly defined set of testable requirements that were cascaded to the relevant Agile teams as part of standard delivery.

For the test plan, we took an "Automate First" approach, with squads automating features within each sprint. We set an automation coverage target of 85%, carefully monitoring progress to prevent technical automation debt and enable rapid delivery.

Our test automation strategy realigned our client's Automation Pyramid, shifting left and ensuring that higher volumes of tests were executed faster in the lower environments–unit and API levels–with the number of "slower" automated tests greatly reduced near the top of the pyramid, the system integration and UI levels. All automation was implemented into the CI/CD pipeline so that code would not be promoted through the pipeline until it had passed the necessary tests in the earlier environments.

We also strategized and implemented a shift-left approach for cyber security testing. This was a significant evolutionary step for the Client, who had relied on penetration testing at the end of the development lifecycle—a legacy approach with significant risk of vulnerabilities being identified late in the testing program, endangering release times, disrupting business and adding costs.

Moving target: Assuring compliance amid evolving rules

Adding to the complexity were regulations from the governing bodies related to data privacy/protection and cyber security:

- ICO (Information Commissioner's Office)
- FCA (Financial Conduct Authority)

The solution was required to be compliant with the following regulations:

- GDPR (General Data Protection Regulation)IFRS17 (Financial Reporting Standards)
- PCI DSS (Payment Card Industry Data Security Standard)

Some of these rules were changing and new ones emerging over the course of the project. We took a rigorous, proactive approach to stay ahead of changes and address them appropriately in our plan.

> **"I am pleased that I have a partner in Qualitest that I can trust to quality assure our delivery, but who can also support us with our evolving IT and Digital Transformation goals. I look forward to this fantastic relationship continuing for many years to come."**
>
> –Client's Chief Technology and Information Officer

Data compliance

The EU's data privacy and protection standards, the GDPR, was just taking effect when the project began. Qualitest analyzed and translated all GDPR regulations into system requirements and then mapped them to relevant technology and insurance journeys. We designed tests with clear traceability from requirement to test tracked in the test management tool, for security and also to assure our Client would pass any audits or reviews. Failure could mean fines and delays in product release.

A key consideration was customer correspondence, such as policy documentation delivered by email or SMS. For GDPR compliance. It was essential that we ensure the accuracy of static and dynamic content so that customers were linked to the correct data. To provide repeatable quality and high speed of test execution, we then automated the tests and plugged them into CI/CD pipelines.

Cyber security

For cyber security, we collaborated with the Client to build a robust plan split into three phases, with the following objectives:

- Identify best practices for cloud security.
- Secure cloud infrastructure.
- Satisfy security compliance regulations.
- Build cyber security tests into the CI pipeline.

Phase 1: Discovery

In this phase we held a serious of technical workshops to understand the client's technology, tools and SDLC.

Phase 2: Design and preparation

We identified checklists for key focus areas:

- Cloud Security, including best practices for AWS and Kubernetes
- Secure Development Lifecycle, including secure coding best practices, static and dynamic security testing and secure build pipeline.
- Compliance, including PCI DSS

We identified test tools to facilitate the testing identified in the checklists and then created automated tests and plugged them into CI/CD pipelines.

Phase 3: Execution, Analysis and Reporting

We executed the checklists associated with each defined area.

Data compliance & cyber security

For both data and cyber security, our teams monitored all tests closely to ensure they were fully and properly executed, results analyzed and defects raised for failures. The defect management processes ensured defects were carefully triaged and prioritized. Our team produced thorough test completion reports, with traceability to requirements to provide a clear view of quality.

Key benefits

The three-year project was delivered on time and under budget. Our Client now has a state-of-the-art product that delivers an exceptional customer experience and differentiates them in the highly competitive insurance market. It is compliant with current and upcoming compliance regulations, demonstrably secure and guaranteed of success not only for today, but also in the future. The Client is becoming known as a ‘go to’ partner for brands seeking a strategic insurance technology ally.

Our Client also has a secure and compliant IaaS platform, with cloud- hosting supporting rapid change, adaptation and scaling with the business over time. It is enabled to support big data storage and real-time AI analytics, and the new microservices and APIs support seamless integration with other complementary businesses and systems.

- Automation coverage was maintained at 96% (target 85%), using Qualitest’s proprietary automation framework, Qualiframe.
- 2,548 automated tests were created for the program.
- Total automated execution time was 2 hours (parallel execution), as opposed to an estimated 118 days to execute the test pack manually.

- The shift left (Automation Pyramid) strategy successfully reduced the number of defects as code transitioned through the environments, with close to two-thirds found at the lowest (API) level. come.

- The client now has repeatable automated data compliance (GDPR) and cyber security test assets, which will ensure compliance for years to come.

> **“The release of business change to production is now 12 times faster (quarterly release cycles reduced to 2 weeks) and we have benefited from a 10% year-on-year reduction in testing costs.”**

–Client’s Head of Engineering

QUALITEST™

Connect with Us

www.qualitestgroup.com

https://www.linkedin.com/company/qualitest
https://www.instagram.com/lifeatqualitest
https://twitter.com/Qualitest
https://www.facebook.com/Qualitestgroup