resillion

Assure. Secure. Innovate.

Empowering banks and financial institutions with end-to-end digital assurance and cyber strength

The financial sector operates in a highly regulated, digital-first environment where resilience and security are baseline requirements for trust and compliance. Customers demand confidentiality, system availability and data integrity. Any outage or breach can jeopardise reputation and investor confidence.

The acceleration of digital services such as contactless payments, open banking, APIs and mobile banking places pressure on institutions to remain secure and resilient. This also amplifies ecosystem risk and third-party dependency, making secure connectivity and interoperability critical for operational resilience.

Key challenges for financial institutions:

- Intensifying regulatory scrutiny (DORA, TIBER-EU, ISO standards)
- Escalating cyber threats targeting sensitive data
- Operational resilience mandates requiring systems to withstand peak usage and stress scenarios
- Customer expectations for speed, personalisation and seamless experiences

These expectations are no longer differentiators. They are baseline requirements for competitiveness and compliance.

Our unique value proposition

In a fragmented financial landscape, connectivity is both an enabler and a source of ecosystem risk. By combining interoperability with rigorous cyber defense and lifecycle assurance, we make sure that platforms are partner-ready.

Every third-party integration is secure, every transaction compliant with international standards, and every user experience flawless, driving faster innovation and reducing risk across the BFSI ecosystem.

resillion

Assure. Secure. Innovate.

Resillion's strategic offering

Resillion provides solutions designed to strengthen your digital ecosystem and ensure compliance across the entire lifecycle - design, testing and live operations.

- **Digital assurance and cyber resilience**

End-to-end testing and validation of digital platforms, tailored cyber security services, managed SOC, penetration testing, incident response and continuous monitoring.

- **Regulatory readiness**

Evidence-based compliance and risk management aligned with supervisory expectations - helping institutions demonstrate resilience under evolving frameworks (e.g., DORA, TIBER-EU).

- **Quality Engineering for seamless experience**

Stress and performance testing, automated testing frameworks, UX validation and data integrity testing to ensure reliability during peak demand.

- **Legacy modernisation and IT transformation**

Migration strategies and robust test processes for integration and business alignment.

Why Resillion?

Partnering with Resillion delivers measurable advantages:

- ✓ Operational resilience to minimise disruption and maximise uptime
- ✓ Enhanced customer confidence through secure and reliable experiences
- ✓ Regulatory compliance aligned with global supervisory expectations
- ✓ Accelerated innovation enabled by agile, secure release cycles

Our approach combines expertise, innovation and trust. By integrating cyber services, conformance and Quality Engineering, we transform compliance from a cost centre into a competitive advantage. This unified approach ensures digital products are secure by design, globally compatible and resilient enough to maintain 'always-on' availability in a volatile threat landscape.

Europrivacy™ Official Partner

CREST

CERTIFIED CCV CYBER SECURITY PEN TEST

epi European Payments Initiative