**Understanding the Role of 'Critical Third Parties' in the Finance Sector and the Expectations for Technology Providers**

As the finance sector’s relationship with technology continues to evolve, we are witnessing a growing need for higher operational resilience and a heightened awareness of the challenges and advantages brought by Cloud transformation.

Given the increasingly complex digital landscape, geopolitical tensions, and the mounting compliance requirements concerning financial data handling, it is natural for the sector to seek a standard of resilience, security, and flexibility that will equip it for the future and provide customers with peace of mind.

The underlying technology infrastructure of the sector plays a crucial role in this journey, which means it is essential for us, as IT specialists, to take the time to understand the unique requirements and obligations of financial organisations and tailor our solutions accordingly. However, this goes beyond merely exploring customer needs.

In July 2022, the finance sector's supervisory authorities, including the Bank of England, Prudential Regulation Authority (PRA), and FCA, proposed a set of measures to formalise the assessment process for what they term 'critical third parties.' These are defined as third-party entities that the UK government designates as 'critical' under the proposed powers of the FSM Bill. The designation is based on the assessment that a failure or disruption in the services provided by these parties, either individually or collectively, could potentially jeopardise the stability or confidence in the UK's financial system.

While these proposed standards are not exclusive to technology partners, they represent the sector's increasing rigor in assessing potential partners. Therefore, any technology providers seeking engagement with the finance sector must be prepared to provide clear evidence of their ability to meet these criteria. Key considerations include:

Establishing well-defined business continuity and disaster recovery plans that can be swiftly implemented. It is essential to operate under the assumption that breaches or disruptions may occur and plan accordingly.

Regularly evaluating the overall resilience of delivered services and proactively addressing opportunities for improvement.

Familiarising yourself with the long-term objectives of the supervisory authorities and aligning service delivery accordingly. Ensure adherence to recognised standards and undergo regular audits.

Prioritising effective communication. The supervisory authorities are contemplating incorporating communication strategies into their formal assessment process for critical third parties. Establish and utilise reliable communication channels at all levels, not just during crisis situations.

The years ahead will undoubtedly pose challenges for both financial organisations and technology providers. However, close collaboration between teams will not only maintain business continuity and strengthen customer confidence but also drive innovation. By leveraging cutting-edge technology, financial firms can achieve their resilience, security, and service quality goals in both the short and long term. If you would like to learn more about the technology journey in the finance sector, please feel free to contact us.