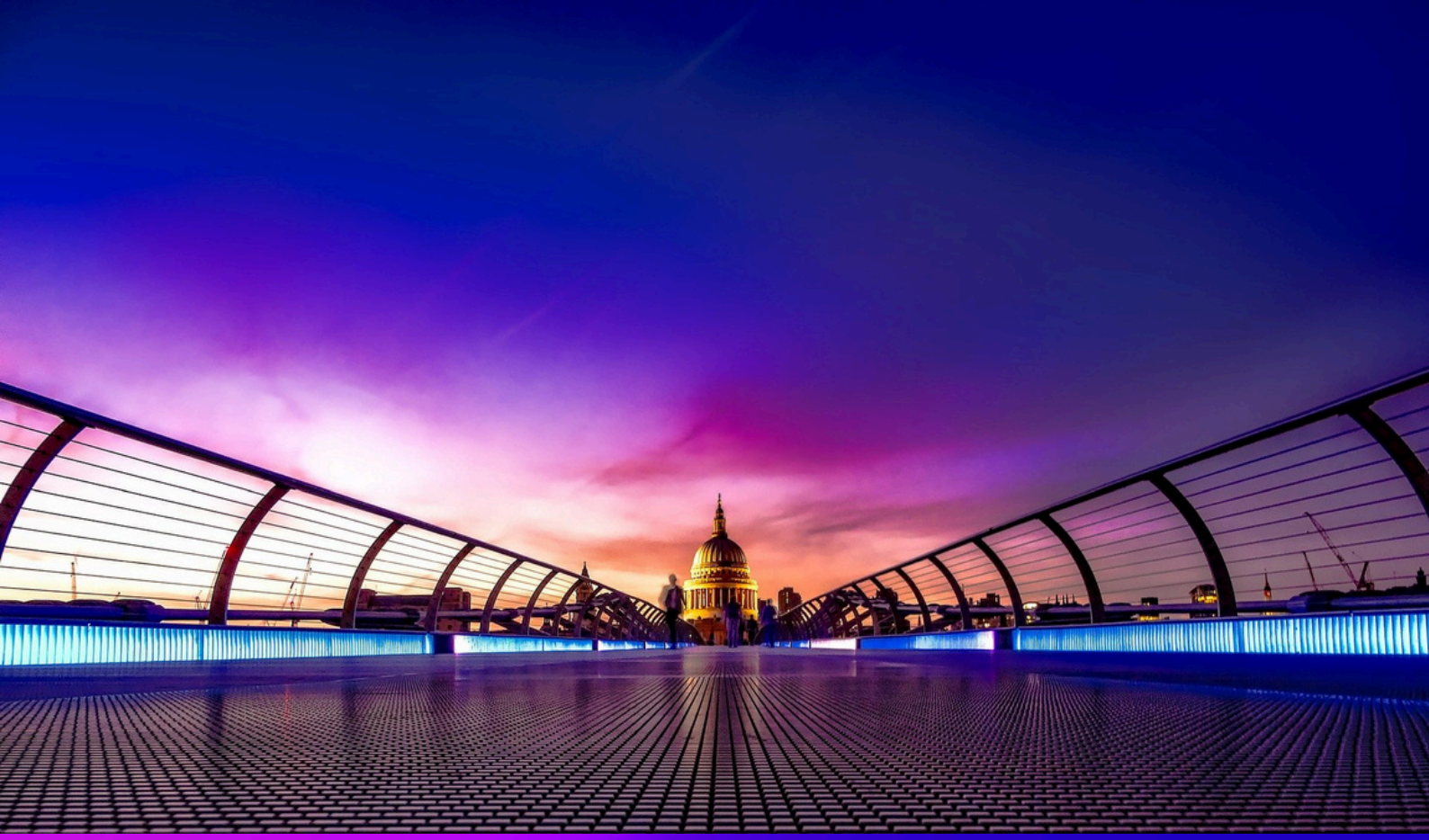

Strengthening third-party resilience: Addressing current challenges with an eye to the future

Steph Stylianou, George Peters and
Lawrence Hicks

Be SHAPING THE FUTURE

Third-party resilience is an evolving area of non-financial risk within the financial services industry, with increasing regulatory scrutiny. This paper explores the key pillars of third-party risk management, challenges within the financial services industry, emerging regulation and Be UK's recommendations as presented on our recent third-party resilience roundtable. This paper also outlines the areas of third-party risk that are of concern to the industry and insights from an industry leader that were discussed during the roundtable.

Key pillars of third-party risk management (as proposed by Be UK)

Third-Party Risk Management (TPRM) is the process of identifying, assessing, managing, and monitoring risks arising from relationships with external vendors or service providers to ensure regulatory compliance and business continuity. The key pillars (as proposed by Be UK are):

Risk assessment - Conduct structured assessments to evaluate the risk posed by a third party before engagement, including tiering or segmentation models.

Due diligence - Assess the third-party's resilience, continuity, subcontracting, and exit strategy (planned and unplanned) - capabilities, ensuring they support critical services and align with operational resilience requirements.

Contracting - Embed mandatory requirements into contracts, such as subcontracting restrictions, performance standards and service level agreements (SLA), business continuity and exit and transition clauses.

Ongoing performance management - Establish processes for continuous review of third-party performance and identification of emerging risks that may arise after the contract has been executed and service provision is underway.

Incident management and reporting - Ensure detection, escalation and resolution of third-party incidents including assessing incident impact and implementing corrective actions.

Key challenges

Firms face a number of obstacles, both regulatory and non-regulatory, which pose significant challenges to their third-party resilience. Below are some of the key challenges Be UK have seen across the industry:

- Complexity of existing regulatory requirements.

- Interconnectedness of existing regulatory requirements.
- Ineffective tooling (manual, disparate, legacy systems).
- Absence of cross-functional business alignment.
- Unavailability of a 'supply chain' view.
- Poor data availability, quality, and granularity.

New and emerging regulations

Emerging regulations bring new challenges, as well as new opportunities to get ahead and drive value within the firm:

Critical Third-Parties (CTP) under PRA / FCA / BoE

- Provides designation of CTPs to the UK financial sector that are subject to resilience testing and reporting obligations.
- Effective Date: 1st January 2025.

DORA (Digital Operational Resilience Act) under EBA / EIOPA / ESMA

- Provides direct oversight of critical ICT third-party service providers and comprehensive ICT risk management.
- Effective Date: 17th January 2025.

Operational Incident and Outsourcing, and Third-Party Reporting under PRA / FCA / BoE

- Covers mandatory requirements for incident notifications for third parties specifying reportable categories, timelines and content.
- Consultation published December 2024.
- Effective Date: Expected H2 2026.

Be UK's recommendations

Despite these challenges, firms can turn pain points into value adding sustainable ways of working with targeted actions for embedded third-party risk management. Our recommendations are:

- Conduct a regulatory interpretation and traceability review to understand regulatory expectations.

- Review and (re-)design an integrated TPRM framework incorporating the various relevant regulatory requirements across the TPRM lifecycle ensuring no duplication of effort.

- Conduct an extended supply chain mapping and resilience assessment (including 3rd, 4th, and 5th parties) to improve understanding of downstream dependencies.

- Conduct an operating model and roles / responsibilities review to establish clear accountability across the organisation's various functions.
- Evaluate current tooling and define future-state requirements to support a more integrated TPRM capability to improve operational efficiency.
- Establish minimum data standards for third-party risk and implement data quality controls at third-party onboarding to enable higher quality insight to support decision making.

Benefits of the above include:

- Improved understanding of regulatory expectations.
- Removal of duplication of effort for implementing requirements for multiple regulations.
- Improved understanding of downstream dependencies.
- Clear ownership of responsibilities.
- Improved operational efficiency.
- Higher quality insights supporting decision making.

Concerns within the industry and insights from industry leader

On Be UK's recent roundtable a poll was run to find out what the most concerning/critical areas of third-party risk are within the industry. The most common concerning/critical area by far was "changing and growing regulatory expectations". "Balancing compliance requirements with commercial efficiencies" and "impact of artificial intelligence" also ranked high. Lower comparative levels of concern were raised for "changing geopolitical landscape", "securing senior leadership buy-in" and "cross-industry collaboration including use of utilities".

Insights were provided by the guest speaker (a banking global head of third-party risk management), touching on the various areas of concern highlighted in the poll:

Regulatory expectations: Regulatory expectations are rapidly evolving, creating challenges for organisations and requiring most heads of department to devote up to 90% of their resources to compliance. International collaboration is limited, with regulations often competing across jurisdictions. Over time, regulatory focus has shifted from basic process adequacy to deeper scrutiny and robust testing.

Non-negotiable areas in supplier management include information security, business continuity (including evidence of testing), data privacy, and financial stability.

Supply chain risks: Fourth-party risks are difficult to manage, with prime vendors often tasked with identifying them. Tools like GRX and Bitsight aid in risk rating and due diligence, providing visibility across supply chains.

Concentration risk: Concentration risk, previously a 'tick box' exercise, is drawing greater attention as regulators and firms address vulnerabilities tied to dominant vendors. This is a big part of the context for the critical third-party regulation.

Senior management buy-in: Senior management engagement is essential but often lacking; high-profile incidents can prompt action and raise TPM's profile.

Artificial Intelligence: AI-powered platforms such as GRX automate workflows, risk scoring, and compliance reporting, with pilots underway to test these systems against traditional management.

Cross-industry collaboration: Incident response and industry collaboration remain key: lessons from major vulnerabilities highlight the need for both individual and coordinated approaches. Consortiums like KY3P facilitate comprehensive due diligence, though senior buy-in and cost impede implementation.

Conclusion

It is evident from the roundtable that there are challenges to ensure third-party resilience in financial services firms, with changing and growing regulatory expectations a key concern across the industry. Firms should focus on regulatory interpretation, enhancing data and tooling, whilst securing senior leadership buy-in, to ensure third-party resilience. The scrutiny around third-party risk management will not go away so proactivity is key for firms across the industry, so they don't fall behind.

Upcoming roundtable

Join us for our next roundtable on **'Cloud region concentration risk - challenges, regulatory risks and preventing disaster'** on 22nd October.

About us

Be | Shaping the Future is a leading pan-European financial services management consultancy, operating in 13 countries across Europe.

We are a disrupter to the top-tier consultancy brands, trusted by five out of ten of Europe's leading banks (alongside other leading financial institutions and FinTechs).

We are one of the fastest growing consultancies with dedicated specialist teams in:

- Retail and commercial banking
- Capital markets
- Cards and payments
- Risk, regulatory and compliance
- Finance & CFO advisory
- ESG

At Be UK, we've worked with a range of financial services firms to help design, implement, and enhance scenario testing frameworks.

Our team brings a wealth of experience in operational resilience, data strategy, and regulatory compliance equipping us to support firms wherever they are on their journey, whether it's improving cross-team collaboration, modernising testing methods or unlocking the value of data, we're here to help firms turn insight into action.

Utilising our broad experience from across the banking sector, we ensure our clients take advantage of market disruption to achieve lasting value.

Bringing deep industry expertise and expert consulting capabilities, we support our clients to tackle their biggest opportunities and challenges to deliver fundamental and enduring change to their businesses.

Contact

For more information on how we can help you on your risk journey, please get in touch.

Lawrence Hicks
Associate Partner - Non-Financial Risk
E: l.hicks@beshapingthefuture.co.uk
T: +44(0) 7891473391

George Peters
Senior Manager- Non-Financial Risk
E: g.peters@beshapingthefuture.co.uk
T: +44(0) 7939032650

Steph Stylianou
Manager - Non-Financial Risk
E: s.stylianou@beshapingthefuture.co.uk
T: +44(0) 7557678506