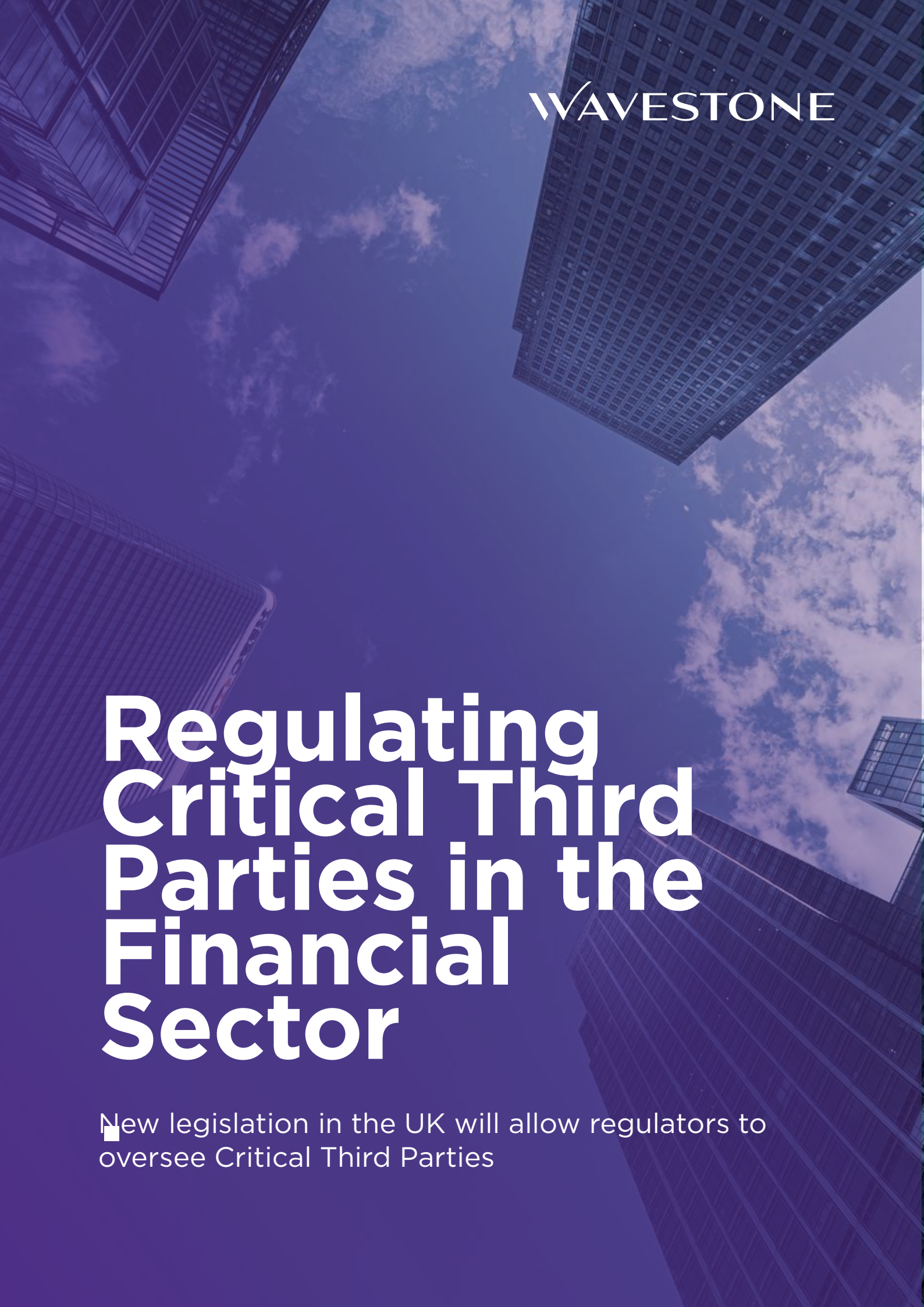
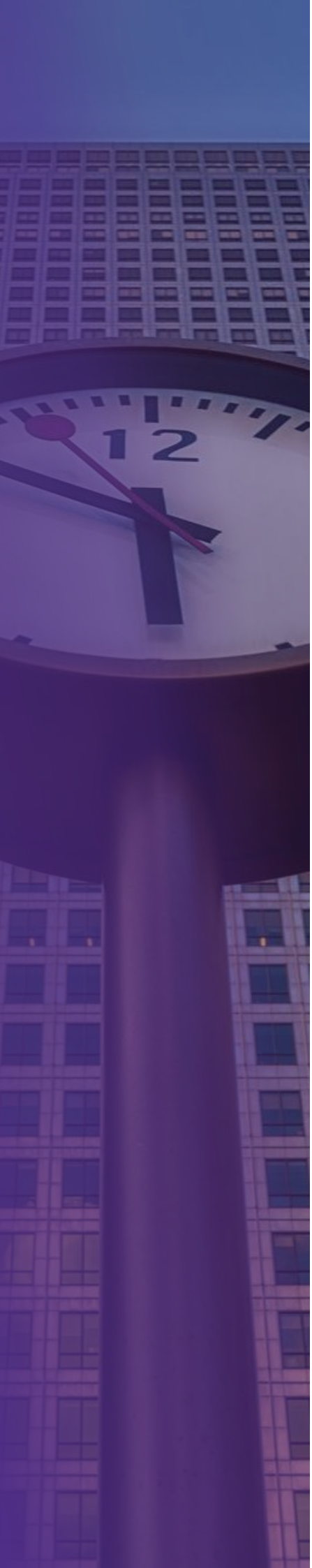


WAVESTONE

Regulating Critical Third Parties in the Financial Sector

New legislation in the UK will allow regulators to oversee Critical Third Parties



Introduction

HM Treasury published its much-anticipated Policy Statement 'Critical Third Parties to the Finance Sector' setting out the principles for new legislation to be enacted that will permit regulators in the UK to oversee and directly enforce against third parties that provide 'Critical Services'.

Calls for greater levels of scrutiny of 'critical' third parties have been made for some time and accelerated recently during the Covid-19 pandemic, where financial firms have fast-tracked moving critical services to the cloud environment. The rate at which cloud providers are now carrying out critical services for financial institutions has been increasing rapidly over the last 5 years. However, the concentration risk has now reached a tipping point for the UK Government prompting greater levels of action from regulators to monitor and address the concentration risk.

The Policy Statement emphasises that since 2020 'over 65% of UK firms used the same four cloud providers for cloud infrastructure services'.

What will the new framework and regime cover? How will the new rules affect third parties and financial firms?

AUTHORS

Mathew WELLS

Senior Manager

Euan BRIGGS

Consultant

Policy Statement

CRITICAL THIRD PARTIES TO THE FINANCE SECTOR'

A New Regulatory Framework

The Policy Statement proposes a new regulatory framework that would allow the Bank of England (BoE), including the Prudential Regulation Authority (PRA), and the Financial Conduct Authority (FCA) new powers to oversee and enforce against providers of 'critical services' to the financial industry.

This is a first major step in addressing a very recent but increasing problem of systemic concentration risk within the financial sector.

Increasing Reliance on Third Parties Outside the Financial Regulatory Orbit

Third party outsourcing arrangements to cloud providers and other technology providers have been steadily increasing and accelerated in recent years. The key issue now is that a large proportion of financial firms are outsourcing their critical services and functions to a small number of third parties, in particular cloud infrastructure providers. This has created a very real systemic risk to the viability of the financial sector and in turn UK plc. The Policy Statement highlights that as of 2020, 65% of financial firms are currently relying on four major cloud providers.

Under the new legislation HM Treasury has stated that certain third parties can be designated as 'critical', which will allow financial regulators to be able to make rules, gather information, and take enforcement action, in respect of certain services that critical third parties provide to firms of particular relevance to the regulators' objectives (which the regulators refer to as 'material' services)'.

This is an important first step as up until now the policy direction has been principally focussed on the outsourcing arrangement itself and the services as 'critical' rather than the direct third-party provider, which has been a key limitation in addressing concentration risk.

HM Treasury states that 'no single firm can manage risks originating from a concentration in the provision of critical services by one third party to multiple firms'. Therefore, new legislation is required.

Operational Resilience Framework

The Policy Statement acknowledges that the current regulatory landscape and powers do not address systemic concentration risk.

The new legislation will complement the current Operational Resilience regulatory framework where 'firms are required to ensure their contractual arrangements with third parties allow them to comply with this operational resilience framework, which includes requirements on areas such as data security, business continuity and exit planning'. Firms will continue to ultimately remain responsible for their operational resilience obligations, but HM Treasury emphasises that the new legislation will address the systemic concentration risk attached to critical third parties and therefore the new legislative framework will 'complement but not replace the individual responsibilities of firms'.

Designating a Third Party as Critical

HM Treasury will need to consult the financial regulators and other relevant bodies to finalise the approach to designating a third party as 'critical' subject to passing primary and secondary legislation.

Under the proposed approach, HM Treasury has stated that:

'Financial regulators might proactively recommend the designation of certain third parties as 'critical' to HM Treasury, based on their analysis of data and information from firms'. In addition, 'finance sector firms could also make representations to HM Treasury in relation to their own third parties'.

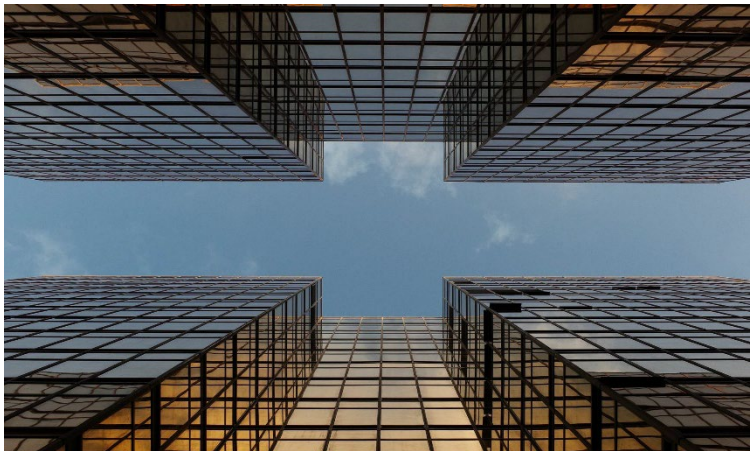
Will There Be Enforcement Powers?

The Policy Statement directs that regulators will be able to request information directly from critical third parties on the resilience of their material services to firms, or their compliance with applicable requirements;

- Commission an independent 'skilled person' to report on certain aspects of a critical third party's services;
- Appoint an investigator to look into potential breaches of requirements under the legislation;
- Interview a representative of a critical third party and require the production of documents; and
- Enter a critical third party's premises under warrant as part of an investigation

The regulators will have a 'suite of statutory powers', including:

- The power to direct critical third parties from taking or refraining from taking specific actions;
- Enforcement powers including a power to publicise failings; and
- Prohibit a critical third party from providing future services or continuing to provide services to firms.



Next Steps

HM Treasury will legislate 'when parliamentary time allows'.

The regulators will be publishing a Discussion Paper setting out the powers granted to them under the legislation and how they will be used as well as seeking industry views. This is expected some time during the Summer 2022.

Following the regulators' finalising its rules HM Treasury will commence designating certain third parties as critical under the new regime.

What will the new Regime mean for Providers of 'Critical Services'

Speculation of direct oversight and potential enforcement by the regulators of critical third parties have been circulating for some time and the UK Government and regulators have communicated in the last 12-months their intention of addressing systemic concentration risk in the finance sector. Therefore, the Policy Statement is not a surprise. The issue of how to address systemic concentration risk has been long-time coming

If a third party has been designated as 'critical' under the new framework, HM Treasury has stated that the regulators will be empowered 'to set minimum resilience standards that critical third parties will be directly required to meet'.

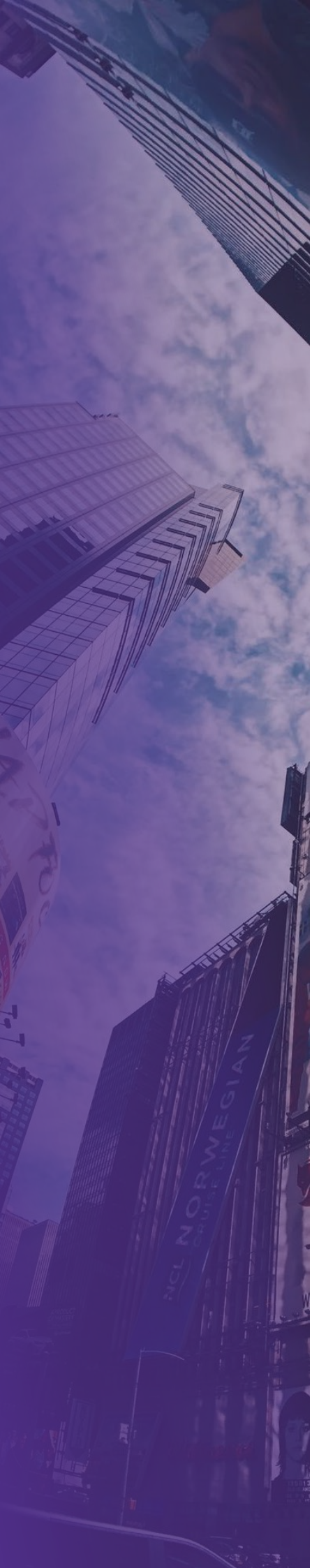
Again, this is an important step as the regulators will for the first time be able to directly oversee and enforce against a third party and potentially a third party that is not a regulated firm within the usual regulatory orbit. Such proposals will 'allow the financial regulators to require critical third parties to take part in a range of targeted forms of resilience testing, to assess whether these standards were being complied with'.

Continued...

We have started to see some cloud providers adapting their service offerings to financial firms to be 'compliant' out of the box in respect to existing regulatory obligations but these adaptations and service evolutions will not directly address concentration risk where a small few providers are undertaking a large proportion of core services for financial firms.

Therefore, the proposed regime and framework will present changes in the way third parties (that are designated as 'critical') manage and govern 'material services' in a way that is not done today. Direct regulator oversight and enforcement powers will likely force a change.

However, further clarity on the exact criteria to be proposed during primary and secondary legislation will be needed to determine what minimum standards, thresholds, and data will be required to designate a third party as 'critical' for the purposed of the new regime. HM Treasury has stated that there the designation regime will be 'flexible and proportionate'.



What will the new Regime mean for Financial Firms?

Financial firms will still be responsible for their current obligations in respect to outsourcing and operational resilience requirements which HM Treasury confirmed in the Policy Statement.

Again, we will need to see the detailed criteria to be set out in primary and secondary legislation to understand the full extent of the proposed framework. However, we will likely see financial firms re-visiting their cloud outsourcing strategies and Third Party Risk Management approaches where third parties are designated as critical in order to assess any potential impacts if a critical third party breaches their direct obligations and what potential regulator enforcement action might mean for a financial firm.

Acknowledgments

AUTHORS

Mathew Wells
Senior Manager

Mathew is a well-rounded professional with a experience helping financial institutions understand and implement strategic operational and regulatory change.

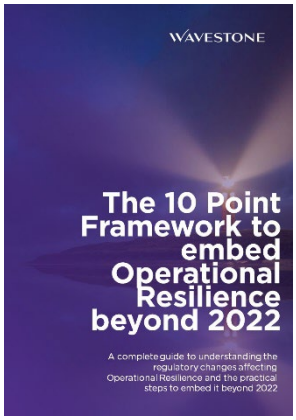
The core areas of change Mathew is currently focusing on includes currently include: Digital Transformation, Operational Resilience, Climate Change, Digital Risk, and Operating Model Optimisation.

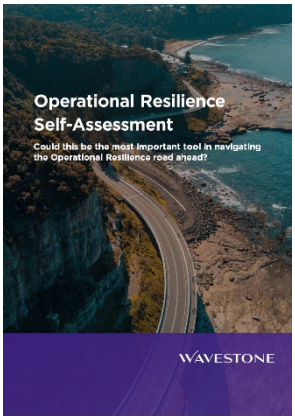
Euan Briggs
Consultant

Euan has an academic background in political science with a focus upon technology policy and geopolitics. This created a passion for researching and understanding the cybersecurity regulatory environment.

His areas of expertise include Information Technology Assurance and Risk Management, which he brings to his client engagements.

Our publications





Wavestone is a leading independent, global technology and management consultancy, helping our clients master their key digital, competitive, and environmental challenges. We draw on a strength of resource and expertise of over 3,500 consultants, deployed throughout the world. Wavestone is also marked by our style, which we call “The Positive Way.”

In the UK, our client focused approach allows us to bring deep business and technology expertise to add value to an organisation’s agenda. We support our clients across operational resilience, cybersecurity and technology advisory topics.

The Positive Way

WAVESTONE

www.wavestone.com