WHITE PAPER

Operational Resilience: Adapt, Respond & Recover

Ruleguard

Contents

Introduction

In the UK, the supervisory bodies have collaborated to issue new requirements to build a robust infrastructure.

We have seen the UK government setting out its post-Brexit strategy for the financial services sector. One of its objectives is to maintain the UK's position as a world-leading hub for financial services (FS). To support this objective, we need to ensure that our FS framework is robust and resilient.

The shift towards operational resilience is not new. Globally, we have seen an increase in cyberattacks which prompted regulators to raise awareness of this issue and publish guidance on cyber resilience.

More recently, the regulators' focus has broadened to include cyber resilience within a wider operational resilience framework. Given the impact of the financial crisis in 2008 and other regional crises, operational resilience is a priority for supervisors worldwide. To support efforts, various global bodies such as Basel Committee on Banking Supervision (BCBS) and the International Organisation for Securities and Options (IOSCO), have issued standards to help financial services weather the storm of disruptions. It's no longer a question of planning what to do IF something happens, but what to do WHEN a risk materialises. Firms need to anticipate and spring into action when required.

Supervisory stance

“Operational resilience is the ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions.”

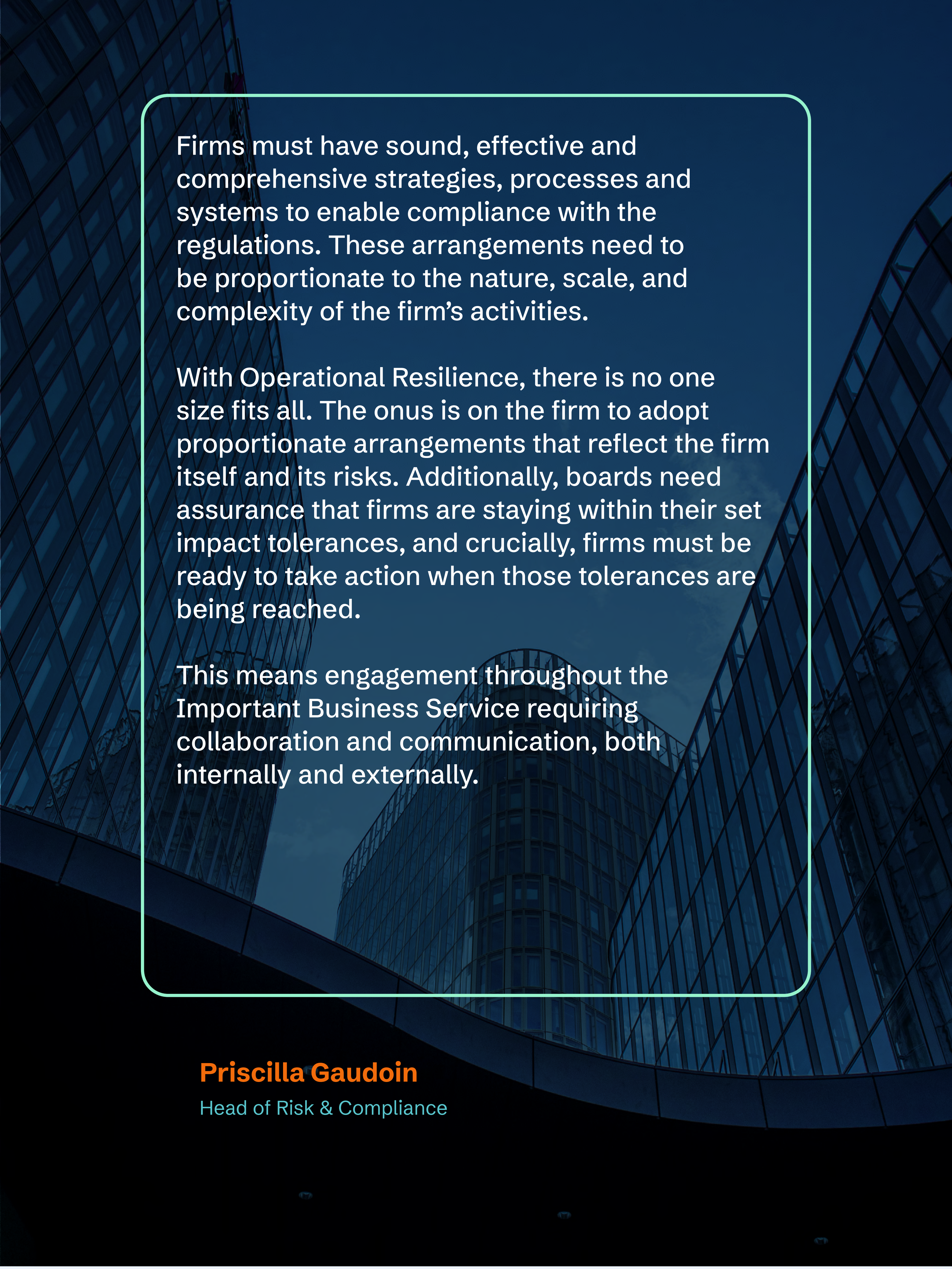
(DP1/18 Building Financial Sector’s Operational Resilience)

The aim of operational resilience is to ensure that firms can adapt to operational disruptions. The emphasis being on bending rather than breaking. Importantly, firms need to assess their ability to respond quickly in a way that does not exacerbate an incident. Regulators globally have set out their requirements to improve the resilience of firms and the financial sector. The requirements come in the form of specific rules and requirements issued by local regulators reflecting the principles and standards recommended by global bodies.

Whilst there are different approaches and terminology, there are some common characteristics:

- A clear distinction between operational risk and operational resilience
- Operational resilience as an outcome
- Financial stability for operational resilience (and customers too)
- An identification of what firms do that is important
- A concept of tolerance for disruption, or impact tolerance, to define what might be acceptable
- The use of scenario testing to assure resilience

Firms must have sound, effective and comprehensive strategies, processes and systems to enable compliance with the regulations. These arrangements need to be proportionate to the nature, scale, and complexity of the firm’s activities.



Firms must have sound, effective and comprehensive strategies, processes and systems to enable compliance with the regulations. These arrangements need to be proportionate to the nature, scale, and complexity of the firm’s activities.

With Operational Resilience, there is no one size fits all. The onus is on the firm to adopt proportionate arrangements that reflect the firm itself and its risks. Additionally, boards need assurance that firms are staying within their set impact tolerances, and crucially, firms must be ready to take action when those tolerances are being reached.

This means engagement throughout the Important Business Service requiring collaboration and communication, both internally and externally.

Priscilla Gaudoin

Head of Risk & Compliance

Proportionate application

Whilst the requirements apply to all firms in scope, how these requirements are implemented will vary between firms.

DP1/18 describes how larger firms may have multiple business services, whereas a Financial Market Infrastructure (FMI) is likely to have one business service used by multiple firms.

In this example, it's easy to see how disruption might cause significant harm.

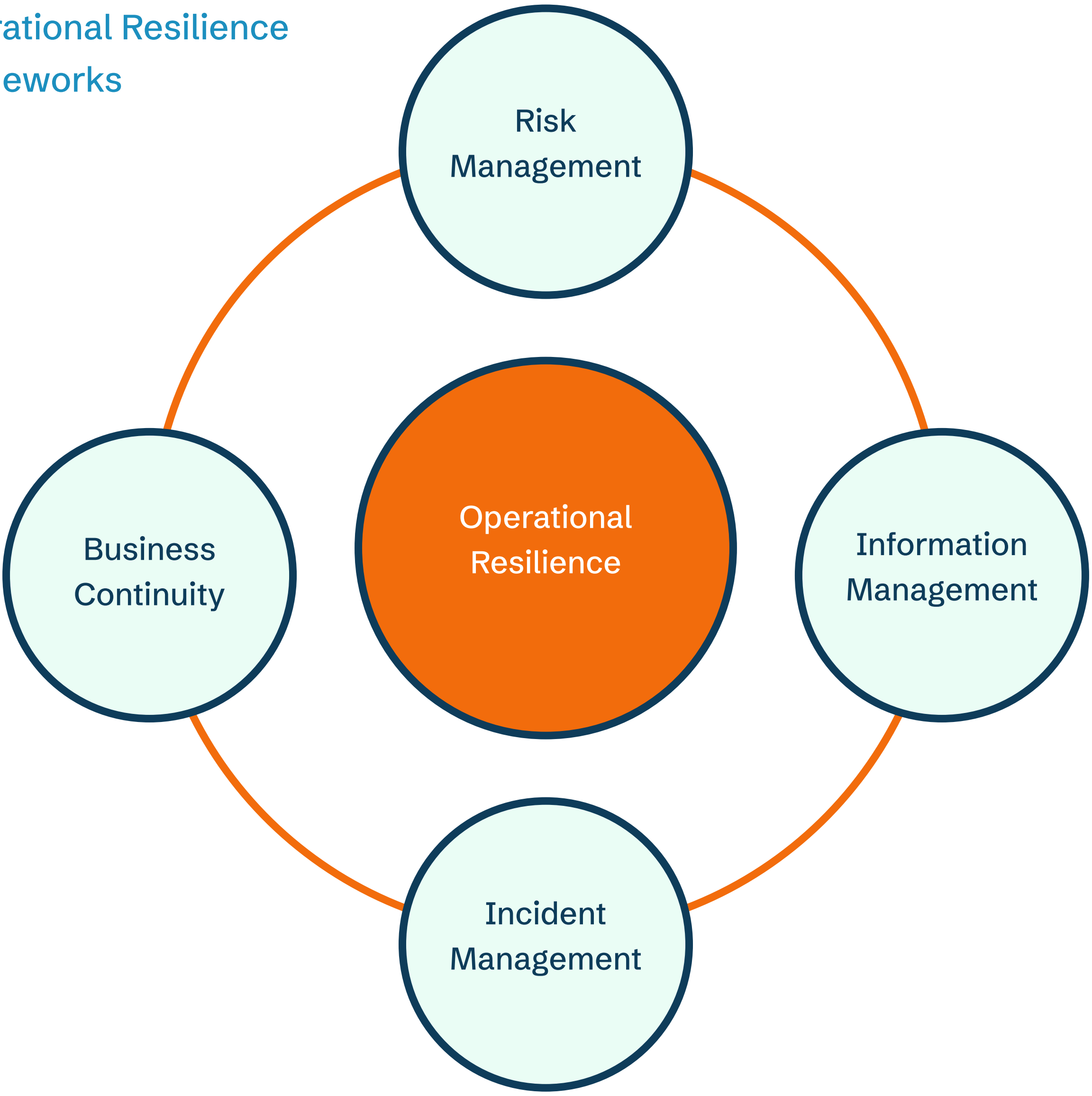
Similarly, smaller firms with only one important business service still need to identify how long they can operate without providing that service. The extent to which they need to stress test and how they do so will be less onerous than that needed by larger firms.

The regulators are encouraging firms to develop frameworks that match their business services, risks and resources. In this way, greater flexibility is allowed instead of one size fits all.

Additionally, firms must look beyond their own firm and consider the impact of third-parties and any sub-contractors upon services. Taking this holistic view helps to build a resilient framework.

In building a resilient framework, firms don't need to reinvent the wheel, but build upon existing processes.

Crucial elements of Operational Resilience Frameworks



Resilience builds on existing areas

Firms should review their current arrangements in terms of risk management, information management, business continuity and incident management. Regulatory sector reviews have highlighted that firms have these frameworks in place, but they need to be more robust.

UK requirements

The UK regulatory approach is based on the belief that businesses are likely to be more operationally resilient if the businesses are designed and managed based on the assumption that disruption will occur.

Identify:

- The most important business services
- How much disruption could be tolerated and in what circumstances

Map:

- The systems and processes that support these business services

Assess:

- How the failure of an individual system or process could impact the business service

Test:

- Using scenarios and by learning from experience, that resilience meets the firm’s tolerance

Invest:

- In the ability to respond and recover from disruptions through having appropriate systems, oversight and training

Communicate:

- Timely information to internal stakeholders, supervisory authorities, customers, counterparties and other market participants

(based on DP1/18 Building the UK financial sector’s Operational Resilience)

The UK regulators published their requirements in 2021 with firms required to:

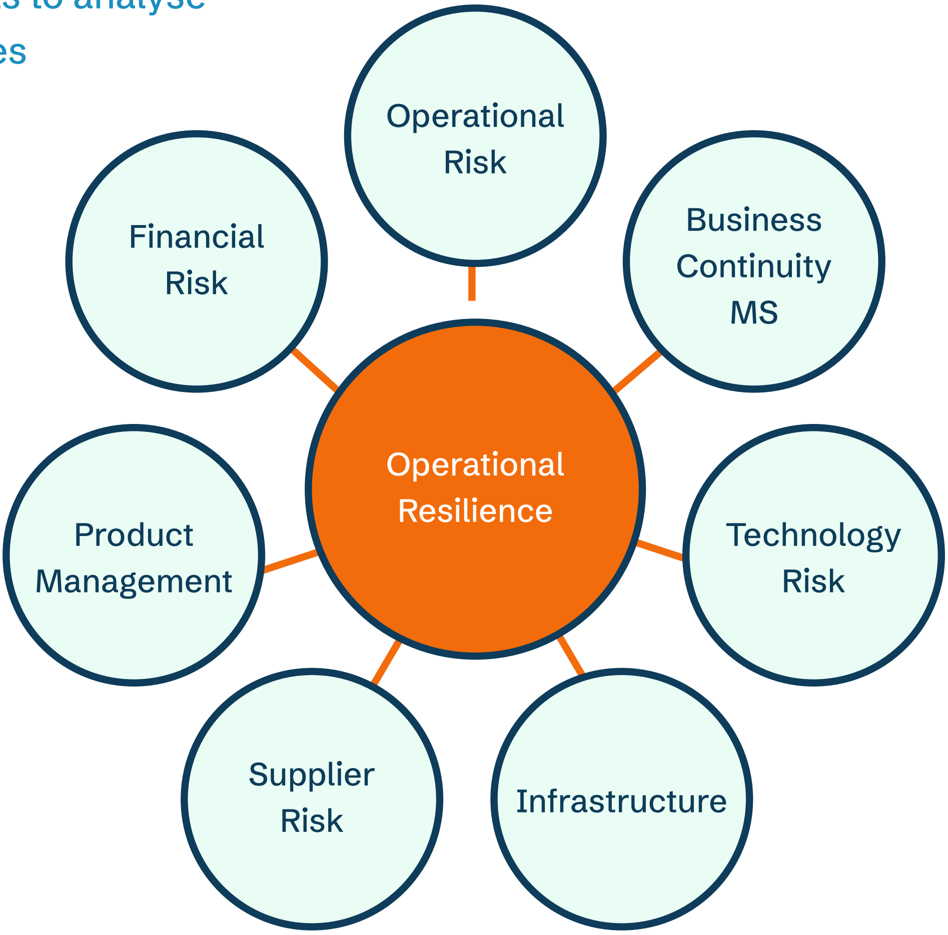
1. **Identify important business services.** Firms must consider how disruption to those business services can impact a firm's own interests as well as cause harm to customers and wider market participants
2. **Set a tolerance for the maximum disruption** to each important business service whilst ensuring that firms can continue to deliver those services. Firms must ensure that they are able to stay within their impact tolerances during severe scenarios
3. **Map and test important business services** to identify any vulnerabilities and drive change as required
4. **Conduct lessons learned** by identifying the required resources to meet operational resilience responsibilities
5. **Develop effective communication plans** to mitigate service disruptions
6. **Complete a self-assessment** to demonstrate that firms are meeting their responsibilities

Firms should note that if their business model changes, they need to reflect upon these 6 steps and demonstrate ongoing compliance.

Mind the gap!

Firms need to leverage their current processes and management information to identify weaknesses. This will help identify any gaps in their internal frameworks.

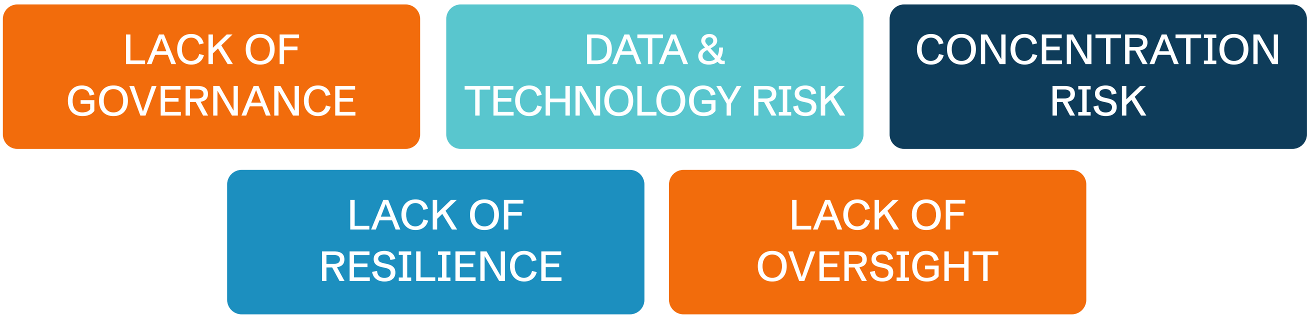
Focus areas to analyse weaknesses



By identifying important business services firms will also identify any third-parties along the journey. Firms should review contracts and investigate whether any sub-contractors are in the chain as part of regular due diligence. This appears to be another common focus for regulators worldwide.

The regulators have concerns regarding lack of control. Their concern is that firms who have outsourced processes may not have sufficient sight of vulnerabilities in those processes. Failure to understand the risks posed by outsourcing makes firms vulnerable.

Principle risks raised by the regulator



LACK OF GOVERNANCE

DATA & TECHNOLOGY RISK

CONCENTRATION RISK

LACK OF RESILIENCE

LACK OF OVERSIGHT

The supervisory bodies setting standards and requirements for the FS industry have shared their concerns. These include the following areas:

- **Technology advancements** are beneficial, but develop so quickly that it may be difficult to maintain an understanding of the risks posed. There is an increasing number of cyber incidents globally across various industries. This can make monitoring and reliance on outsourced tasks more difficult. Concern includes the uncertainty of the location of data and possible lack of understanding of cloud technology risks
- **Concentration risk**, where the sector is reliant on a small number of key suppliers, which could prove difficult to substitute
- **Lack of oversight** over supplier relationships, where firms need to understand the arrangements in place as well as any related subcontracting to third-parties and the creation of long and complex chains
- **Lack of governance** where firms fail to understand risks and monitor the effectiveness of controls

Mapping third-party processes helps identify any weaknesses in those processes impacting the regulated activities. Setting impact tolerances and monitoring the ability to stay within those tolerances demonstrates a robust process.

Where firms have embraced technology, they now need to understand any underlying dependencies to ensure the smooth running of their services.

The regulatory message is clear that firms must stay within their impact tolerances regardless of whether any third-parties are involved in the service chain. This is a message repeated by various regional and sector specific bodies. For example, IOSCO's R01/2020 Principles on Outsourcing indicates that:

> **"A regulator may impose sanctions and penalties on a regulated entity for the regulated entity's violations of statutory or regulatory requirements that have resulted in whole or in part from the failure of a service provider (whether it is regulated or unregulated)"**
>
> **IOSCO - R01/2020 Principles on Outsourcing**

FCA published its findings in 2020 relating to outsourcing in the life insurance sector. This highlighted that firms have governance arrangements, but these arrangements do not go far enough to include the full life cycle of the arrangements. Firms need to consider the escalation and follow up on identified issues as well as exit strategies. This means having contingency plans in place that include third-party failures and impacts upon services.

Impact tolerances

The regulators highlighted the need to consider the impact of the failure of other related important business services when setting impact tolerances for individual important business services. This is due to the potential sharing of common resources which support the delivery of the important business services or where simultaneous disruption could have compounding impacts on similar external end users.

The regulators confirmed that time or duration is a mandatory measure as firms must consider time-critical threats when setting impact tolerances. However, firms can use both qualitative and quantitative factors to measure impact tolerances. Thus, a firm may measure the level of service being provided at a point during the day along with the volume of complaints received. The regulators also encourage firms to use available tools, such as continuous control monitoring, to respond quickly to developing issues.

Improving third-party & outsourcing arrangements

It's worth noting that '**outsourcing**' refers to the practice of using a service provider to perform tasks, functions, processes, services or activities that it could do itself. It may also refer to onshoring, offshoring, nearshoring or right shoring.

The term '**service provider**' is also used to describe various parties. It refers to suppliers, contractors, sub-contractors as well as service providers. Equally, this may include subsidiaries or sister companies within a group.

It also includes those suppliers or third-parties who are unregulated as they may have the potential to disrupt a firm's service and cause harm to the end user. Firms should consider the following outsourcing principles:

- Due diligence in the selection and monitoring of a service provider and service provider's performance
- Having contracts in place with a service provider which include provisions relating to the termination of the contract and appropriate exit strategies
- Having appropriate measures in place to ensure a service provider establishes and maintains emergency procedures and a plan for disaster recovery with periodic testing of backup facilities
- Taking appropriate steps to require that service providers protect proprietary and confidential information about the market participant and its clients from intentional or inadvertent disclosure to unauthorised individual
- Having consideration for concentration isk relating to outsourced functions
- Ensuring the market participant, its auditors and the regulator have prompt access to the books and records of the service providers relating to the outsourced activities

Of the above, due diligence is another area of focus for regulators. For some firms this is seen as an activity that they conduct at the beginning of relationship or perhaps, annually. Often there is a lack of detail and evidence to provide a good audit trail, even lack of scrutiny. Firms need to review their due diligence processes, ensure that there is a consistent process in place.

More importantly, firms need to repeat due diligence and monitor these parties to identify any warnings.

Firms should not forget the requirements under Principle 3 and SYSC. Namely that firms must organise and control their operations responsibly; as well as implement appropriate risk management frameworks.   With outsourcing, this is a defined term and firms need to consider whether a function being outsourced is deemed to be critical or important, is material outsourcing, or involve important operational functions.

As with earlier UK operational resilience requirements, a joint discussion paper issued in 2022 has now paved the way for CP23/30: Operational resilience: Critical third parties to the UK financial sector which closed in Q1 2024 and we await further enhancements to the outsourcing obligations.

Think you're out of scope?

Like many regulators, the UK supervisors set out their requirements and indicated those firms caught within the scope of the new operational resilience regime.

In scope firms include PRA-designated investment firms, PRA-designated investment firms, banks & building societies, insurers and financial market infrastructures (FMIs).

Firms outside of the new regime who have business relationships with these affected organisations may find themselves having to assist these organisations to meet their obligations.

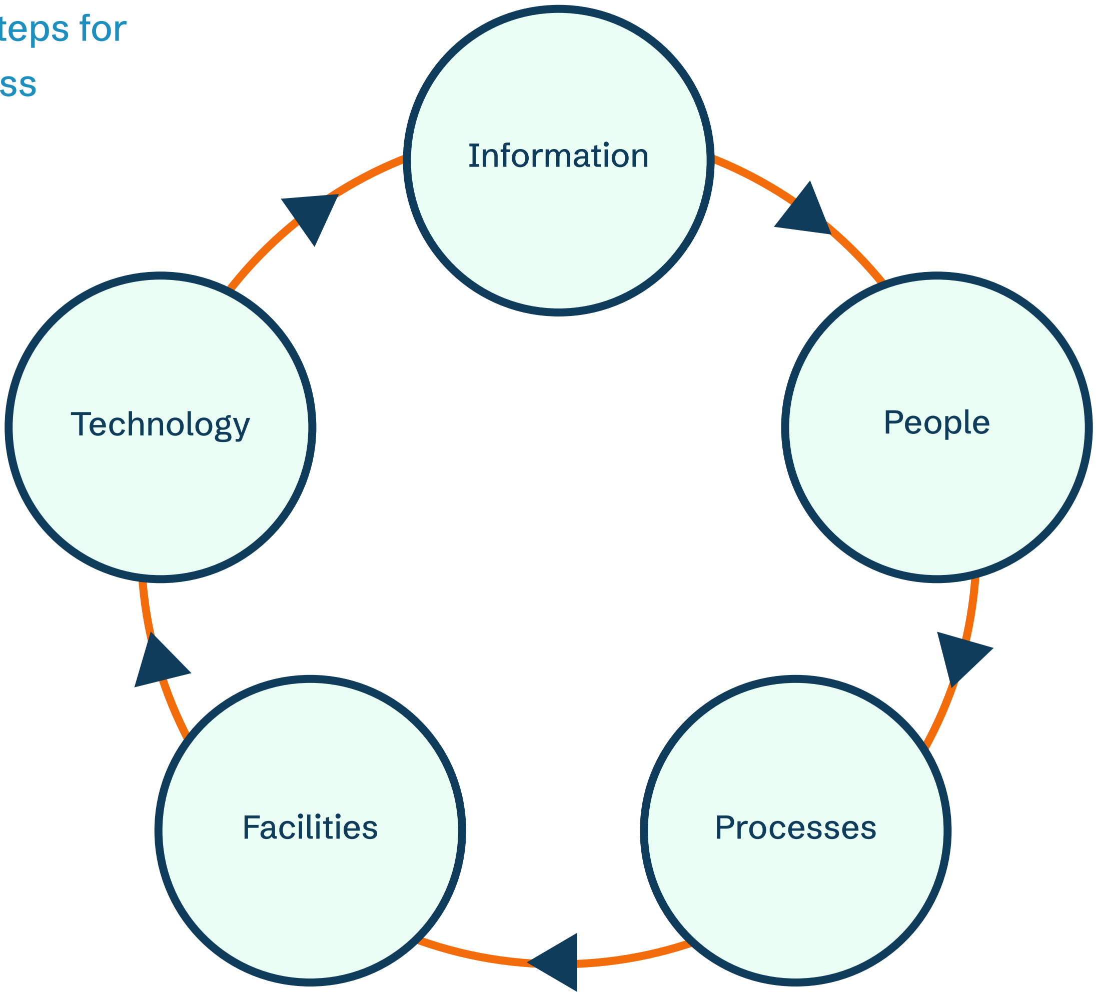
An operationally resilient firm must have a comprehensive understanding and mapping of the resources that support their business services. This includes outsourced and third-party services over which the firm may not have direct control. Firms must seek assurance from these service providers to build a resilient service chain.

Steps for success

To be successful firms need to focus on continuity and prioritise analysis, work and investment in operational resilience. Setting tolerances helps ensure processes can adapt to disruptions easily. parties to identify any warnings.

Once an incident has occurred, firms need to be able to adapt to shocks. Having a contingency plan that is designed for the entire service chain becomes invaluable.

Five steps for success



Firms need to take ownership of their operational resilience frameworks and prioritise plans and investment choices based on their impacts upon the public interest. Internally, this means boards are comprised of individuals with the necessary knowledge, skills and expertise to set effective standards.

Priscilla Gaudoin

Head of Risk & Compliance

Reporting

Firms will collate various management information according to the important business services, but also the role that the firm plays within a service too. For example, internal reporting to the board is part of good governance and enables the board to oversee its risks and make decisions. External reporting may be to another third-party in the service chain or it may be within a group structure. There will also be regulatory notifications where necessary.

The first milestone for firms was 31st March 2022. Preparation for that deadline should have included the identification of relevant reporting and and the collation of data from different parties within a supply chain. The reporting needs to be timely and accurate to enable decision making.

Often there is a tendency for management information to focus on operational performance. Firms should also focus on customer outcomes.

Firms already have a requirement to make disclosures to the regulator. Specific to operational resilience, this could include any material event which:

- Results in a significant loss of data
- Results in IT systems being unavailable or lack of control over those systems
- Affects a large number of customers
- Results in unauthorised access to a firm’s information systems

Maintaining & improving resilience

Whilst the first milestone may have been passed, it's vital that senior managers don't lose sight of their ongoing obligations. Firms should have completed most of their work by March 2022. The transitional period to March 2025 is to allow firms to test the ability to stay within their impact tolerances. This means that firms need to have identified the resources required to ensure the smooth running of the important business services.

Successful firms will not only identify the essential resources, but those that are shared resources across entities or important business services. This requires firms to review their contingency plans and key staff risks to invest and plan for the inevitable incident.

Firms also need to consider how they will:

- Review their critical systems arrangements following each material change to their critical systems, and at least annually
- Change the critical systems arrangements as required to ensure they continue to comply with the above obligations

Operational resilience

Firms should plan for extreme but plausible scenarios, modelling impact tolerances and identifying investment gaps. The upcoming regulation around operational resilience may look like a variant of standard risk management on the face of it, but firms should not be fooled.

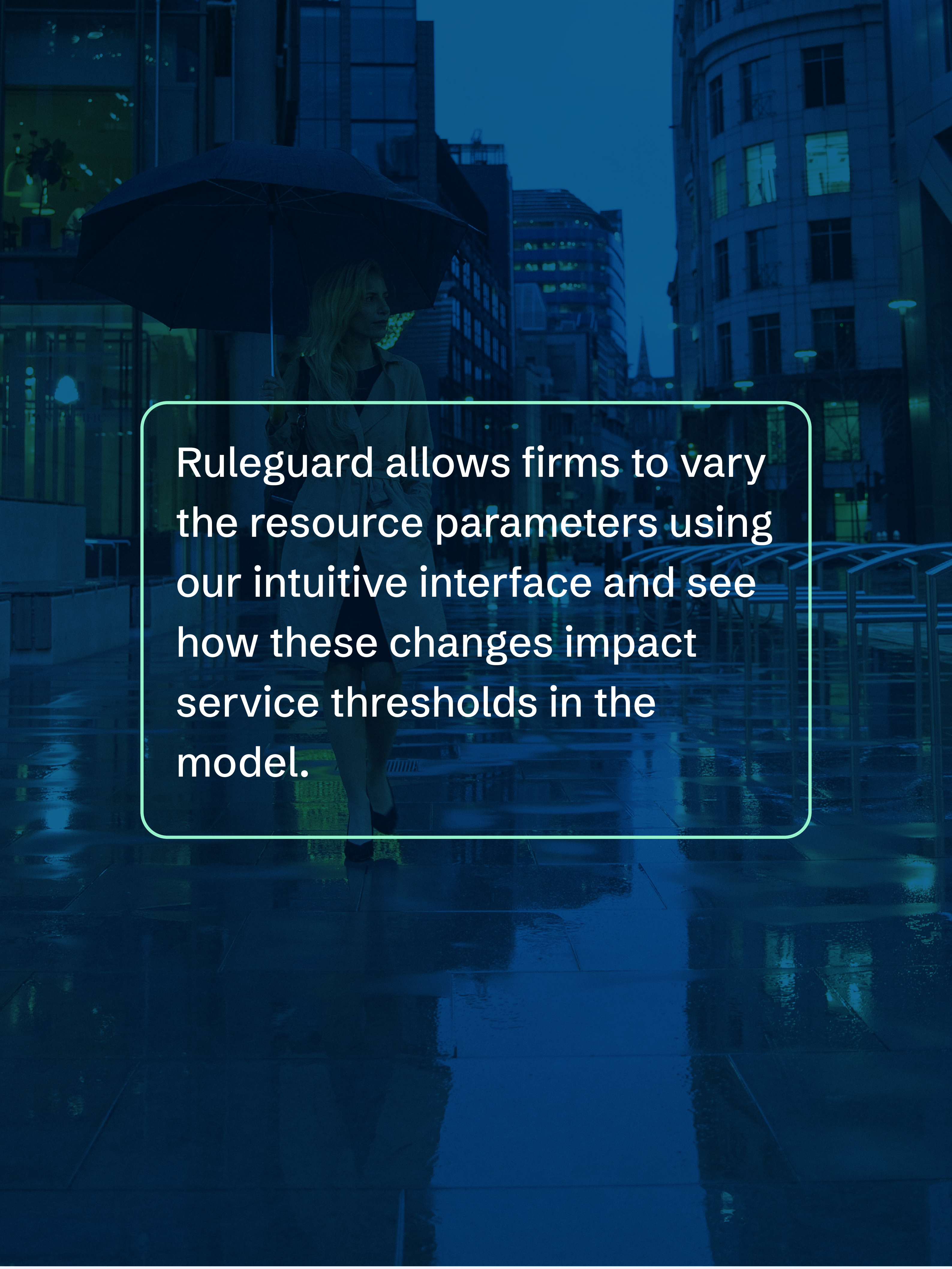
Taking a 'key services' view of operations and mapping each of the dependent resources across a group is a large undertaking for a firm of any size. Fortunately, Ruleguard now applies the power and flexibility of our industry-leading rules mapping engine to service and resource mapping for operational resilience compliance.

Firms may define service levels and tolerance thresholds for each service to define how much impact on customers and the market is acceptable in extreme but plausible scenarios.

Ruleguard allows firms to vary the resource parameters using our intuitive interface and see how these changes impact service thresholds in the model.

Firms can easily identify gaps for investment and automatically create a resilience self-assessment document for board review.

The scale of operational resilience compliance can seem daunting. Ruleguard's experience and technical design skills helps firms to quickly have it under control.



Ruleguard allows firms to vary the resource parameters using our intuitive interface and see how these changes impact service thresholds in the model.

Why Ruleguard?

Ruleguard is an end-to-end GRC software platform designed to help regulated firms manage the complex and burdensome issues associated with regulatory compliance. It has a range of solutions to help firms fulfil their obligations across the UK, Europe and APAC regions.

An ever-changing regulatory environment requires firms to identify the changes impacting their business and to adapt their processes and controls quickly to meet those requirements. It can be time consuming and overwhelming to be constantly monitoring rule changes from various supervisory bodies both in the UK and internationally. Senior Management require evidence to demonstrate that business risks are being managed effectively. Collating data from various sources to generate timely management information, enable decision making and facilitate oversight is a key requirement.

Ruleguard has been designed to help you demonstrate and evidence compliance, by using its comprehensive rules-mapping, risk and control tools, automated reporting features and powerful dashboards. At its core, Ruleguard is a single unifying solution for all your compliance processes and procedures for managing your ongoing compliance.

Our SaaS-delivered software platform, Ruleguard, has been designed to manage the complex and burdensome issues associated with regulatory compliance, especially when processes and procedures in place are manual and fragmented widely across multiple companies, departments and systems.

Using Ruleguard will enable you to show regulators and auditors how your business has complied with the rules, including providing effective governance and oversight to your firm.

Join the world's best-known banks, insurance companies, asset management firms and investment funds who trust Ruleguard to help manage their regulatory compliance.

Key sources

Please see below for the list of key materials.

- PS6/21: Operational resilience: Impact tolerances for important business services, March 2021 https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper
- PS7/21: Outsourcing and third-party risk management, https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management
- PS21/3: Building Operational Resilience, March 2021 https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf
- Bank of England policy on Operational Resilience of FMIs, March 2021 https://www.bankofengland.co.uk/paper/2021/bank-of-england-policy-on-operational-resilience-of-fmis

About Ruleguard

Ruleguard started out in 2013 as a software ‘design and build’ agency that specialised in financial services projects, particularly those with a unique requirement for data and functionality that was far from being available ‘off the shelf’.

Fast-forward to 2024 and we have established Ruleguard as one of the foremost offerings in the RegTech space, providing genuine compliance oversight to some of the largest and most complex financial institutions globally.

Most importantly, we continue to work closely with our clients to identify the most painful aspects of compliance oversight and strive to build-out our platform to improve that governance with increased efficiency and reduced cost.

Get in touch!

☎ 0800 408 3845

✉ marketing@ruleguard.com

🌐 www.ruleguard.com

Key points of contact

Priscilla Gaudoin
Head of Risk & Compliance
Priscilla.Gaudoin@ruleguard.com

Ed Buckman
Director of Commercial Strategy
Ed.Buckman@ruleguard.com

Matthew Bruce
Platform Director
Matthew.Bruce@ruleguard.com

RegTech Insight
Best solution for
Managing Operational Risk
2024

BUSINESS AWARDS UK
Fintech Awards
Best Customer Experience
2024

ICA INTERNATIONAL COMPLIANCE ASSOCIATION
ICA Technology Partner of the Year
Finalist
GRC Solutions
2024

BOOK A DISCOVERY CALL →

Ruleguard

Disclaimer:

This document is intended for general information purposes only and does not take into account the reader's specific circumstances and may not reflect the most current developments.

Ruleguard disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information.Ruleguard does not provide legal, regulatory, audit or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.