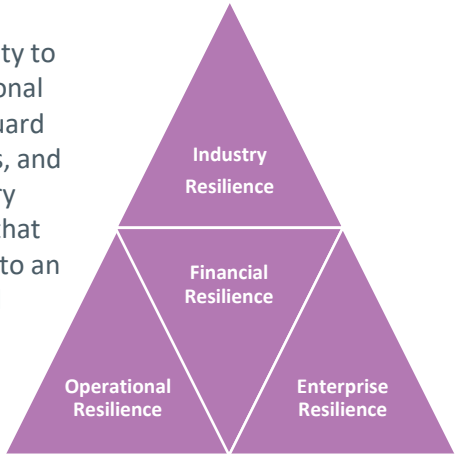
Operational Resilience Cheat Sheet

The Challenge

It's not just about adhering to FCA and PRA's March 2025 regulatory deadline, with numerous high-profile incidents including the July 2024 global Microsoft IT outage, firms are more than ever aware that robust resilience measures are fundamental to the survival of their business, to customer confidence and to success

If businesses can enhance their ability to withstand operational disruptions, safeguard customer interests, and maintain regulatory compliance, then that directly translates to an increased financial and enterprise resilience.



How Firms are Responding

1. **Scenario Analysis:** Firms are thinking more deeply, and specifically, about increasingly plausible disruptive events that could impact critical functions. Not just cyberattacks, natural disasters, system failures, but all the complexities that geo-politics and a polarised world is now presenting.
2. **Holistic Plans and Playbook:** Resilience plans are widening to include playbook approaches that define specific actions required to resolve operational failures. This helps increase business confidence levels to effectively respond and manage disruption. Organisations now realise that having a plan is not enough, it needs to be specific and much deeper.
4. **Insightful Stress Testing:** Significant but plausible events may only get worse. Organisations are looking at deeper stress testing exercises to assess the resilience of critical functions under increasingly more extreme conditions. This involves deliberately subjecting systems and processes to higher levels of stress to determine breaking points and weak links to fix.
5. **Test & Analyse Output:** Determining whether impact tolerances are being met is one thing, working out where they could fail, or could be improved is another – organisations are now shifting from satisfying regulations to maturity improvements.
6. **Horizontal Recalibration:** Recalibrating based on testing is the start. Resilience, if you truly have it "built in by design" can only be demonstrated by incremental improvement and reduction of Impact Tolerances and levels of Intolerable Harm across your processes. Organisations should continuously be striving to actively re-calibrate and reduce these thresholds. Organisations are establishing ongoing Continuous Improvement methods that seek 'marginal gains' through adjusting practices in line with the changing environments.
7. **Improvements and Review:** Organisations are implementing robust monitoring and oversight frameworks, to continuously track performance of critical functions and processes in real-time. Applying this intelligence allows them to insightfully review and update impact tolerances based on evolving business dynamics, emerging risks as well as technological advancements, and future changes in regulatory requirements.

8 Thorough Documentation and Reporting: Organisations have recognised the value of embedding these factors, not only for risk management and regulatory satisfaction but underlying commercial value too. Whether that's supporting due diligence for clients, customers or partners, being able to demonstrate a deep understanding of the resilience of your business becomes easy.

9 Full Training and Awareness: To properly embed Operational Resilience, organisations have been focused on employee training and awareness, supported by clear communication and escalation processes. Encouraging a culture of resilience throughout your organisation, does more than just promote awareness of risks and adherence to regulatory requirements, it enables improvement to your underlying business.

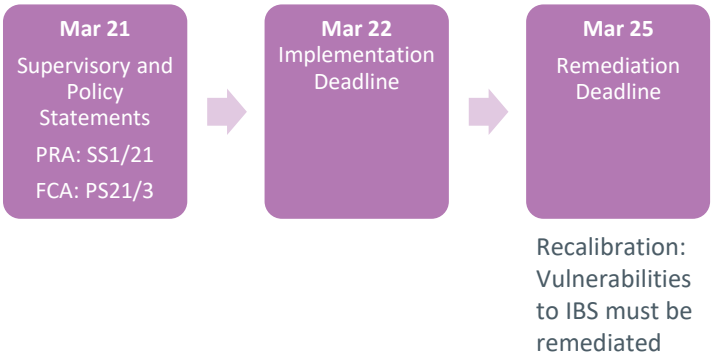
10 Awareness & Nuance: Staying up to date on emerging threats, and the subtlety of how they change over time, is not a reactive activity. Recent incidents affecting payments and communications networks show us how the emergence of more subtle and persistent threats have been developing, and from several different sources

Defining Current Position

As the 2025 deadline approaches, for firms to ensure that they are complying, then they must have assessed, tested and recalibrated their Important Business Services. To do this, we typically find that firms have re-evaluated their mapped processes, capabilities and resources. They've assessed and defined their weak links, and further evaluated their assessments of Material Suppliers as well as service providers.

Operating models are being adjusted to embed resilience approaches within business activities. Ensuring that playbooks are developed, understood and tested, alongside communication & escalation and decision-making frameworks.

The recent Critical Third-Party consultation should also give firms a real sense that the robustness of the UK's Financial Services industry is really at the forefront of the governments mind – and its need to recognise the breadth of suppliers and critical third parties that it relies on.



Recalibration: Vulnerabilities to IBS must be remediated

How can Altus help you?

Altus has a range of models and methods to easily identify Important Business Services, and those critical processes and parties involved across the breadth of your enterprise.

From customer journeys to highlight 'moments of truth', supporting processes can be mapped to relevant customer journey stages or touchpoints, helping determine all internal and external stakeholders involved, and the systems and capabilities required to fulfil those processes.

Using PEAK, our set of unique Industry Reference models, which cover the breadth of financial services, we can map your capabilities and processes, and strengthen your value chains.

Our intimate understanding of all financial service suppliers and supplier eco-systems means that Altus can define service boundaries between firms and their suppliers – in a structured and visual way, to identify and track relevant control measures both internally and externally with all your suppliers.

Find out more:
www.altus.co.uk
+44 (0)1225 438 000
enquiries@altus.co.uk