Ruleguard

Ruleguard & The Investment Association

Key Takeaways from Operational Resilience: Building Robust Frameworks for the Future

1. Regulatory Messages & Expectations

The FCA highlighted varying levels of readiness ahead of the 31st March deadline.

Preparedness varies significantly across firms. While many are confident, a meaningful proportion still struggle with regulatory expectations, especially around testing and resilience documentation.

Key concerns included persistent gaps in scenario testing, third-party risk management, and lack of robust exit strategies.

Regulators are becoming less tolerant of ambiguity, more detailed, demonstrable compliance is expected.

2. Strategies for Managing Operational Disruptions

Firms face challenges in securing ongoing senior leadership engagement and cross-functional accountability.

Embedding resilience requires cultural alignment, governance structures, and leadership commitment.

Cultural shift is required to ensure operational resilience remains a long-term strategic priority. Board engagement has improved due to regulatory pressure but may wane post-deadline unless embedded into governance frameworks.

3. Minimising Customer Impact During Disruptions

Effective response planning, communication protocols, and scenario analysis were cited as critical to protecting customer outcomes.

Real-life incidents highlighted how poor communication exacerbates harm during outages.

Customer distress is a key marker of intolerable harm. Firms must move beyond technical recovery to address emotional and reputational fallout.

Incident simulations should include customer journey testing, not just internal recovery metrics.

4. Scenario Testing & Stress Testing

Debate continues over whether testing should follow a standardised approach or be tailored to each firm's context.

Importance of calibrating "severe but plausible" scenarios and exploring "test-to-failure" methodologies.

Scenario testing is maturing, with more firms moving beyond tabletop exercises. However, there's still inconsistency in approach and depth.

Regulators favour rigorous, failure-informed testing to better reveal vulnerabilities and improve recovery posture.

5. Managing IBS with Internal Dependencies

Internal dependencies must be treated as third-party risks. Without formal oversight and documentation, these create blind spots in resilience planning.

Internal services and shared group functions often receive less scrutiny than outsourced ones, despite being equally critical.

6. Leveraging Technology for Compliance and Resilience

Firms face a dual challenge: replacing legacy systems while managing the risks of emerging technologies like AI.

Compliance tooling is seen as essential, but integration and oversight remain hurdles.

Technology is a double-edged sword. It enables efficiency and control, but also introduces new vectors for failure and cyber risk.

Strategic investment in RegTech is seen as a resilience enabler—particularly platforms that support monitoring, documentation, and MI dashbaords.

7. Third-Party Risk Management & Oversight

Best practices were discussed around onboarding, monitoring, and exit planning.

Uncertainty remains about how firms should apply enhanced oversight where vendors are not yet designated as CTPs.

Third-party risk remains a persistent challenge, particularly with fourth-party and subcontractor visibility.

Firms are increasingly applying CTP-style oversight to all material vendors, regardless of official designation.

8. Future-Proofing Financial Services

Participants discussed resilience in the context of evolving risks—AI misuse, geopolitical instability, and climate events.

Future resilience will be shaped by AI, people and regulation in equal measure. Firms must prepare now for AI-driven threats (e.g. deepfakes, automation errors) as well as systemic climate or geopolitical shocks.

The importance of anticipating new vulnerabilities and aligning people, technology, and regulation was stressed.

Cross-industry collaboration and threat intelligence sharing will be vital.

9. Metrics for Success & Regulator Assessment

Uncertainty remains over how regulators will assess success.

Firms should expect increasing scrutiny, including of smaller and mid-tier firms.

Firms seek clarity on expectations for impact tolerance, resilience testing outcomes, and evidence of readiness.

Success metrics likely include reduction in high-impact incidents, clearer testing documentation, and reduced systemic concentration risks.

Action Steps

1. **Enhance Scenario Testing Approaches**
   - Adopt hybrid testing models combining standardised and bespoke scenarios.
   - Incorporate "test-to-failure" elements.
2. **Improve Third-Party Oversight**
   - Review onboarding and SLA frameworks.
   - Map third-parties and any subcontractors
   - Apply CTP principles across all critical vendors.
3. **Drive Cultural Alignment**
   - Strengthen board and executive engagement post-March deadline.
   - Integrate operational resilience into ongoing governance.
4. **Prepare for Future Risks**
   - Add AI misuse and geopolitical scenarios to risk registers.
   - Collaborate on industry-wide testing where appropriate.
5. **Leverage Technology Thoughtfully**
   - Replace manual tools with resilient, compliant platforms.
   - Monitor vendor innovation and resilience posture.
6. **Engage in Continued Dialogue**
   - Attend summer AI roundtable event.
   - Share learnings and contribute to future guidance development.

Poll Highlights:

of firms are somewhat or very confident.

% of respondents believe technology will be the key driver.

0800 408 3845
marketing@ruleguard.com
www.ruleguard.com