Building Operational Resilience in Regulated Industries

Regulatory bodies are increasingly scrutinizing how organizations manage risks and ensure service continuity. Standards like the Financial Conduct Authority's (FCA) **Operational Resilience** framework set new compliance requirements in critical areas:

- **Identifying Critical Business Services:** Precisely define the scope of your operations and prioritize critical functions and services that are essential for customer well-being. Consider all relevant factors and justify exclusions
- **Impact Analysis and Scenario Testing:** Conduct thorough assessments to understand how potential disruptions could impact your operations. Testing should increase with severity over time to fully evaluate plans. Run "what-if" scenarios to test your preparedness for various situations. Consider metrics like customer harm, transactions types and losses – not just time.
- **Developing Response Plans and Recovery Time Objectives (RTOs):** Establish clear response plans for different disruption scenarios. These plans should define roles, responsibilities, and Recovery Time Objectives (RTOs) – the maximum acceptable downtime for critical services. Define RTOs to recover services well within any impact tolerances.
- **Embedding Best Practices:** Integrate operational resilience best practices into existing processes and systems. This ensures resilience is embedded in everyday operations, not an afterthought. Ensure third parties can also support important services.
- **Continuous Review and Testing:** Regularly assess and test your resilience arrangements through an evolving programme including lessons from real events. Conduct drills and simulations to identify any weaknesses and refine your plans accordingly.
- **Reporting Operational Incidents and Resolution Progress:** Regulators require transparency. Be prepared to report operational incidents and the progress made in resolving them.

Building a Strong Foundation: A Structured Approach

Regulated entities must adopt a holistic and proactive approach to achieve their operational resilience goals and satisfy regulatory requirements. Here's a structured framework to consider:

1. **Map Your Services:** Clearly define the scope of your operations and prioritize critical functions and services. Understand the interdependencies between different services and how they impact each other. Be sure to map third party arrangements.
2. **Assessment & Testing:** Conduct comprehensive impact assessments and risk evaluations to identify potential threats and vulnerabilities. Use scenario testing to simulate potential disruptions and assess their potential impact. Test response plans empirically, including penetration testing for key systems.

3. **Building in Flexibility:** Don't put all your eggs in one basket. Develop alternative strategies, workarounds, and redundancies in your systems to ensure service continuity even during disruptions.
4. **Automated Monitoring:** Leverage technology to your advantage. Implement tools that can proactively identify and diagnose potential problems before they cause disruptions.
5. **Predefined Response Plans:** Develop detailed playbooks for different incidents. These plans should clearly outline protocols, roles and responsibilities, and RTOs for various scenarios.
6. **Governance and Review:** Establish clear oversight for operational resilience initiatives. Embed resilience best practices into your existing processes and governance frameworks.
7. **Validation & Refinement:** Regularly test your resilience plans through drills and simulations. Use the insights gained from lessons learned to identify and address any gaps in your strategy.
8. **Reporting and Demonstration:** Maintain transparency with regulators. Regularly report on your operational resilience initiatives and demonstrate the improvements you've made.
9. **Vulnerabilities Management**: Prioritize vulnerabilities, test remediation plans, and verify fixes through repeated scenario testing.
10. **Horizon Scanning**: Refresh risk assessments considering new and emerging threats.

The Benefits of Proactive Management

By adopting a rigorous yet agile framework for operational resilience, you can future-proof your organization. This approach allows you to:

- **Withstand Disruptions:** Be prepared to weather unexpected events and minimize the impact on your customers and operations.
- **Maintain Regulatory Compliance:** Proactive management helps you meet regulatory requirements and avoid potential penalties for non-compliance.
- **Enhanced Reputation:** Building a strong operational resilience culture fosters trust with regulators, customers, and other stakeholders.
- **Improved Business Continuity:** By anticipating and mitigating risks, you can ensure smoother business operations, even during challenging times.

By adopting a rigorous operational resilience program, organizations can withstand disruptions, maintain regulatory compliance, enhance reputation, and ensure business continuity. Proactive risk management is key in regulated environments.

Not a Phundex user yet? Dive into a world of enhanced productivity – sign up for a free trial today and experience firsthand how Phundex can revolutionize your workflow **Phundex Limited** Work smarter, work faster with Phundex!

You can find more articles on our website, at **Phundex Knowledge Hub,** on LinkedIn at **Phundex LinkedIn**, or for other questions, please email us at: **hello@phundex.com**.

Not already a member of the Phundex LinkedIn Group? Join now for early updates **Phundex LinkedIn Group**

To book a demo or do a trial, you can either use the link on our website or email **support@phundex.com**, and they will be happy to set it up for you.