BDO IDEAS | PEOPLE | TRUST

FINANCIAL SERVICES

OPERATIONAL RESILIENCE

February 2020

OPERATIONAL RESILIENCE

Operational disruption and the road to resilience - A key priority of both the PRA and FCA is to put in place a stronger regulatory framework to promote operational resilience of firms and financial market infrastructures.

In December 2019, the PRA and FCA published their Consultation Papers on Operational Resilience.

Operational disruptions to products and services that firms provide have the potential to cause significant harm to consumers, market participants and, in some instances, the stability of the financial system. Therefore, it is vital that firms have the ability to prevent, adapt and respond to, and recover and learn from operational disruption.

The PRA and FCA consider that managing operational resilience is most effectively addressed by focusing on business services. In order to build and deliver resilient business services, firms need:

- The ability to prevent disruption occurring, as far as possible
- To adapt systems and processes to continue to provide services in the event of a disruptive incident
- To return to business as usual promptly when the disruption is over
- To learn and evolve from both incidents and near misses.

It is imperative that firms pay equal to attention to all of these aspects.

Firms must therefore not only focus on minimising the likelihood of a disruptive event occurring, but also assume that disruptions will inevitably occur and put robust response plans in place to minimise the level of disruption. Firms must also implement processes to ensure that lessons are learned from disruptive events and put in place remedial plans or additional investment to reduce the likelihood of reoccurrence. As such, to deliver operational resilience there are several components which firms need to address.

Firms should consider their arrangements/frameworks with respect to the following:

- Third Parties/Outsourcing of critical functions
- Cyber Security
- Change Management
- Communication Plans, in the event of disruption
- Incident Management
- Business Continuity/Disaster Recovery.

Firms should also be looking to enhance and develop the current Management Information ('MI') reported in order to provide senior management with oversight of the robustness of the firm's operational resilience capabilities.

Given the increased regulatory focus on operational resilience, firms should be taking steps to assess their level of resilience and make enhancements where required. It is also vital that firms do not underestimate the amount of work required to deliver operational resilience.

BDO's Financial Services team and Technology Risk Advisory team are ideally placed to support firms in addressing their operational resilience needs. We are experienced in designing and implementing operational resilience frameworks.

OPERATIONAL RESILIENCE COMPONENTS

01

Third Parties

Robust outsourcing arrangements to ensure effective oversight of critical service providers.

02

Business Continuity/Disaster Recovery

Established arrangements for ensuring business continuity in the event of unforeseen events.

03

Incident Management

Incident response processes to identify, analyse and respond to incidents.

04

Communication Plans

Clear communication plans in the event of business disruption.

05

Change Management

Well governed and documented change processes to ensure resilience is embedded in change control arrangements.

06

Cyber Security

Cyber resilience mechanisms to prevent, detect, respond and recover from cyber-related threats.

PROPOSITIONS

Training and awareness

Provision of training to provide an overview of regulatory expectations on operational resilience and the different approaches firms can take to deliver operational resilience. Our training can be tailored for all levels of staff within your firm.

Management Information

A review of your firm's current operational risk MI reported to the Board and senior management to identify where enhancements could be made with respect to oversight of resilience capabilities.

Deep Dive

A deep dive on one of the specific components on operational resilience to focus on the design and operating effectiveness of the systems and controls in relation to:

Third Parties/Outsourcing of critical functions | Cyber Security | Change Management | Communication Plans - in the event of disruption | Incident Management | Business Continuity/Disaster Recovery.

Gap Analysis

A gap analysis of your arrangements with respect to the following to identify where additional enhancement is required:

Third Parties/Outsourcing of critical functions | Cyber Security | Change Management | Communication Plans - in the event of disruption | Incident Management | Business Continuity/Disaster Recovery.

As part of this, we can assist in how to link the above aspects under a single operational resilience framework.

Design and Implementation

Support your firm with the end-to-end design and implementation of an operational resilience framework through:

- Identifying key business services
- Mapping the supporting systems, people, processes and third parties
- Identifying severe but plausible scenarios that could cause disruption to a key business services
- Assessing the impact of the scenario and set tolerance thresholds i.e. quantify the level of disruption that could be tolerated
- Developing a testing approach for each scenario to allow monitoring of impact tolerance
- Formalising an operational resilience framework and strategy to prescribe guidance on the above steps
- Enhancing your firm's current suite of operational risk MI to ensure exposure to causes of disruption can be monitored on an ongoing basis.

FOR MORE INFORMATION:

RICHARD BARNWELL

+44 (0)207 893 3292
richard.barnwell@bdo.co.uk

STEVE DELLOW

+44 (0)207 893 2723
steve.dellow@bdo.co.uk

ANEESH SUBHRA

+44 (0)758 313 0698
aneesh.subhra@bdo.co.uk

www.bdo.co.uk

42005031