OPERATIONAL RESILIENCE: THE IMPACT OF COVID-19

REGULATORY FOCUS ON OPERATIONAL RESILIENCE

- In December 2019, the FCA released Consultation Paper 19/32, outlining the increase in regulatory expectation, requiring firms to embed operational resilience within all critical business services
- The FCA has since applied regulatory scrutiny to any firms that have experienced operational outages, resulting in fines across a number of businesses, including: RBS, NatWest, Ulster Bank, Tesco Personal Finance and TSB. Most recently, online trading platforms experienced outages in early November amid record trading volumes, exposing a lack of adequate system stress testing which will likely attract regulatory scrutiny
- COVID-19 has presented Senior Management with a significant Operational Resilience challenge in recent months, testing systems and processes. This experience will likely impact the final regulatory requirements which are due to be released imminently
- Firms are now presented with the challenge of improving business resilience to meet regulatory requirements and implementing practical learnings gained from COVID-19, all whilst satisfying the expectations of a broader set of stakeholders than may have been actively engaged in Operational Resilience previously

IMPACT OF COVID

WEALTH MANAGERS WERE ABLE TO QUICKLY TRANSITION TO REMOTE WORKING BY RAPIDLY UPDATING SYSTEMS AND PROCESSES AND BULK PURCHASING NEW INFRASTRUCTURE. HOWEVER, THIS WAS LIKELY TO HAVE LEFT MANY OF THESE BUSINESSES WITH A HIGHER LEVEL OF OPERATIONAL RISK DUE TO THE BELOW FACTORS:

RISK OF DATA LEAKAGE

In addition to regulatory scrutiny, wealth managers would face significant reputational risk and a loss of customer trust should a data breach result from the remote exchange of sensitive customer information

HEIGHTENED EXTERNAL THREAT

The National Cyber Security Centre has warned of a significant increase in cyber related crime, particularly due to fraud and extortion. Staff who feel more comfortable working from home could therefore be more susceptible to social engineering attacks and phishing emails

REDUCED DUE DILIGENCE

Delivering remote working infrastructure in unprecedented timelines could have resulted in the roll out of infrastructure with lower levels of due diligence than in BAU circumstances, leaving machines more prone to vulnerabilities

INCREASED TECH LANDSCAPE

Wealth businesses must now secure a tech landscape which has grown exponentially, with hundreds or thousands of endpoints terminating in employee's residences. This is particularly concerning when supporting high-risk activities such as those listed below

HIGH PRIORITY PROCESSES FOR WEALTH MANAGERS TO CONSIDER

- EXECUTION OF CUSTOMER ORDERS
- MAKING PAYMENTS
- MAINTAINING HIGH COMPLIANCE STANDARDS
- CYBER SECURITY
- PROTECTION OF CUSTOMER ASSETS
- ACCESS TO BUSINESS CRITICAL DATA

OPERATIONAL RESILIENCE STRATEGY

ALPHA HAS DEFINED THE BELOW STRATEGY FRAMEWORK TO SUPPORT WEALTH MANAGERS IN DEFINING AND ASSESSING THEIR LEVEL OF OPERATIONAL RESILIENCE:

HOW ALPHA CAN HELP

ASSESSMENT

Gap analysis against emerging regulatory expectations and remediation planning, leveraging existing work on BCP, Disaster Recovery and Wind Down

DESIGN

Framework or component design to meet regulatory requirements and market best practice

Tools to enable business implementation to meet regulatory requirements

IMPLEMENTATION

Support implementation and enable remediation

Awareness and training to enable business use of framework components

FOR FURTHER INFORMATION PLEASE CONTACT:

KENN TAYLOR, HEAD OF WEALTH
E: kenn.taylor@alphafmc.com
M: +44 7702 207267