MILLIMAN BRIEFING NOTE

Operational resilience in an ever changing landscape

Claire Booth, FIA, CERA
Tanya Hayward, FIA
Peter Moore, FIA
Sophie Smyth

Overview

What is operational resilience and why is it important?

Operational resilience refers to the ability of firms to prevent, respond, recover and learn from operational disruptions. Operational disruptions not only have direct impacts on your firm, employees and consumers, but also residual effects that have the potential to disrupt the wider market, especially in an increasingly interconnected world. It is therefore crucial that firms focus attention on becoming operationally resilient.

> The Bank of England (BoE) defines operational resilience as *'The ability of firms and the financial system as a whole to absorb and adapt to shocks, rather than contribute to them.'*

European law[1] states that regulated financial services firms should have an effective process to identify, assess, manage, monitor and report the risks that they are, or might be, exposed to. Firms are required to undertake appropriate contingency planning and explain how they will respond and recover following operational disruptions to ensure that adequate procedures are in place to operate on an ongoing basis.

In a constantly evolving landscape, we can expect change in the types of threats and their impact on businesses. It is important for firms to have a solid grasp on this to ensure that operational resilience strategies can adapt and remain appropriate and effective.

Advances in technology have enabled a dynamic digital world in which insurers can operate. Counterintuitively, a reliance on technology, cloud-based platforms, outsourcing and remote working increases a firm's vulnerability to some types of risk. This interconnected system allows risks to spread and increases exposure to single points of failure. This environment has caused a surge in the number of cyberattacks, and so it is increasingly important for firms to have processes in place to detect, respond to and rapidly recover from such events.

Regulations and guidelines

As the pace of innovation and technology continues to accelerate, commensurate regulations and guidelines are required to help organisations develop consistent frameworks for operational resilience in light of emerging risks.

Operational resilience appears to be firmly on the regulatory agenda. Multiple regulatory and industry bodies have recently released discussion and consultation papers on the topic. For example, the Basel Committee on Banking Supervision has recognised that operational resilience should be approached beyond the scope of typical operational risk management and minimum capital requirement considerations and has established an Operational Resilience Working Group. The Basel Committee has released a paper[2] on cyber resilience as a precursor to further work on operational resilience.

In a speech[3] at the Operational Resilience in Financial Services Conference in September 2018, Slavka Eley from the European Banking Authority (EBA) mentioned that the operational resilience regulatory and supervisory framework is centred on three core elements: regulation; supervision; and resilience testing. She highlighted a few of the key guidelines that the EBA has published in this area. For example, the EBA Guidelines on Internal Governance were published early in 2018 and specify internal governance arrangements such as risk management, business continuity and outsourcing. The EBA Recommendations on Outsourcing to Cloud Service Providers were developed in response to uncertainty regarding cloud adoption. The EBA has also published guidelines on security measures for operational and security risks, guidelines for the notification of major operational and security incidents and guidelines on fraud reporting requirements. These guidelines are due to be accompanied or replaced by two important policy products: firstly, Guidelines on Outsourcing Arrangements (currently under consultation) and secondly Guidelines on Information and Communications Technology (ICT) and security management, including expectations on resilience testing. The guidelines will be applicable to all regulated institutions under the remit of the EBA with the aim of

[1] Solvency II Directive (2009/138/EC), Capital Requirements Directive (2013/36/EU) and Capital Requirements Regulation (575/2013).

[2] Basel Committee on Banking Supervision (Decembe 2018). Cyber-Resilience: Range of Practices. Bank for International Settlements. Retrieved 28 February 2019 from https://www.bis.org/bcbs/publ/d454.pdf.

[3] Eley, S. (27 September 2018). Regulatory Framework for Mitigating Key Resilience Risks. Retrieved 28 February 2019 from https://eba.europa.eu/documents/10180/2373079/Slavka+Eley+-+Speech+on+the+Regulatory+Framework+for+Mitigating+Key+Resilience+Risks+270918.pdf.

strengthening governance and security arrangements. Eley concluded the speech by remarking that a coordinated approach is essential for tackling resilience-related threats with timely and appropriate regulatory and supervisory responses.

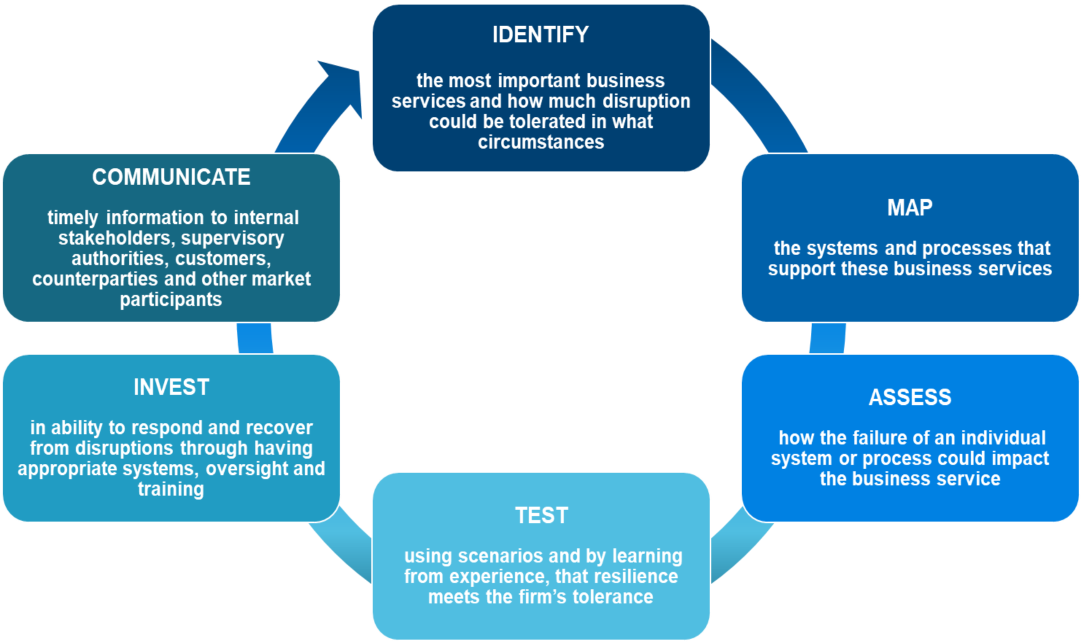
When comparing the range of observed bank, regulatory and supervisory cyber-resilience practices across various jurisdictions, the Basel Committee found that 'most supervisors leverage previously developed national or international standards – principally the NIST framework,[4] ISO27000 series[5] and CPMI-IOSCO guidance.'[6]

Regulatory bodies are becoming increasingly active in the operational resilience space and firms should be assessing and developing their operational resilience capabilities to get ahead of the curve.

Improving operational resilience

The Bank of England (BoE), Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) issued a discussion paper (DP) in July 2018 sharing their collective thinking regarding operational resilience.[7] This DP proposes the process shown in Figure 1, which provides a framework within which firms can begin to develop, or enhance, their operational resilience.

FIGURE 1: PROCESS TO IMPROVE OPERATIONAL RESILIENCE


IDENTIFY
the most important business services and how much disruption could be tolerated in what circumstances
MAP
the systems and processes that support these business services
ASSESS
how the failure of an individual system or process could impact the business service
TEST
using scenarios and by learning from experience, that resilience meets the firm's tolerance
INVEST
in ability to respond and recover from disruptions through having appropriate systems, oversight and training
COMMUNICATE
timely information to internal stakeholders, supervisory authorities, customers, counterparties and other market participants

In the sections that follow, we look at each of the steps of the process and provide our insights gained from our experience in helping clients to improve their operational resilience.

[4] The National Institute of Standards and Technology (NIST) is a voluntary framework that consists of standards, guidelines and best practices to manage cybersecurity-related risk. For more information, see the NIST website at https://www.nist.gov/cyberframework.

[5] The International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) 27000 series is a set of standards to help organisations manage security of assets and information. For more information, see https://www.iso.org/isoiec-27001-information-security.html.

[6] The Committee on Payments and Market Infrastructure (CPMI) and the International Organisation of Securities Commissions (IOSCO) work together to enhance coordination of standard and policy development and implementation regarding clearing, settlement and reporting arrangements, including financial market infrastructures (FMIs) worldwide. For more information, see https://www.iosco.org/about/?subsection=cpmi_iosco.

[7] BoE/FCA (July 2018). DP01/18: Building the UK Financial Sector's Operational Resilience. Retrieved 28 February 2019 from https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A.

Identify

As with most areas of risk management, the first step is to define a risk appetite around which a framework can be built. Risk appetite statements should be defined around all important business services, and can be supported by impact tolerance statements specified in terms of metrics.

Important business services, as defined by the BoE, are those which, if disrupted, would do one or more of the following:

- Threaten a firm’s ongoing viability
- Cause harm to consumers
- Undermine financial stability

An impact tolerance is an upper limit where '*a breach is to be avoided in all but the most extreme scenarios*.'[8] This is a fairly difficult level of tolerance to set, given that it is not particularly straightforward to measure or define a 'level' of operational disruption.

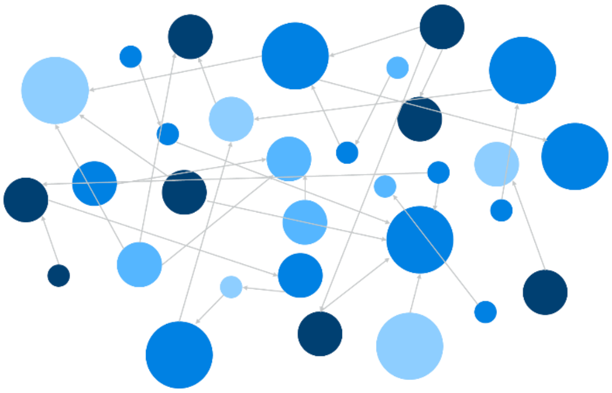
The firm will need to come up with specific relevant metrics or outcomes to define its impact tolerances. They may include metrics such as outage durations, the level of disruption, the number of customers or services affected, the number of information security incidents, the geographic area affected by the disruption and reputational damage. We have found that workshops with employees involved in each business service area are useful when first setting out on this process. These workshops can be used to assess potential severe outcomes, scenarios which could lead to them and ways of measuring such outcomes.

Once tolerances over the level of acceptable disruption have been set, they can be summarised in an 'impact tolerance statement,' which would outline the tolerances, how they were decided upon and why they are reasonable.

We anticipate that there will be further development of market practice in this area in the future, with the Global Financial Markets Association (GFMA)[9] highlighting the need for global consistency in the industry-wide metrics used to provide measures of operational resilience, and the need for clear definitions of 'business services' and 'impact tolerance' and how they should be derived.

Map and assess

Workshops are also helpful, in our experience, when it comes to mapping the systems, people and processes that support the important business services, and determining how disruption caused by one of these dependencies impacts the business services. It is important to ensure that the mapping process is extended to dependencies outside of the firm (e.g., suppliers, outsourcers and competitors) and those in other geographical locations (if they exist).



Test

Testing can then be done using scenarios derived from your own experience (successes, 'near misses' and incidents), the known experiences of others, audits or regulatory scenarios that may be required to be tested in the future. The PRA, FCA and Bank of England are considering setting scenarios for firms to test, in order to assess which firms need to develop their operational resilience further.

CPMI-IOSCO principles for financial market infrastructure (FMI) indicate that an FMI should design and test its systems and processes to aim for the safe resumption of critical operations within two hours of a disruption (principle 7).

Invest

A firm can then use the results of the testing to identify and implement appropriate risk management solutions to ensure that the most suitable responses and management actions will be deployed under operational disruption. For example, a firm could define alternative processing procedures that can be deployed in the case of disruption to systems and processes in order to remain within its impact tolerance level.

The solutions implemented should allow a firm to switch between planned responses and adaptive actions as necessary, and adapt its activities, structures and actions appropriately for the new environment, while retaining its core purpose and values.

[8] BoE/FCA DP01/18, op cit.

[9] GFMA (27 September 2018). Outreach Meeting, London. Retrieved 28 February 2019 from http://www.gfma.org/WorkArea/DownloadAsset.aspx?id=1029.

Communicate

The final step of the process is to ensure that appropriate strategies are in place for communicating with all the relevant internal and external stakeholders. This could include ensuring cooperative communication between all relevant business areas and any third-party providers, and making available the appropriate information and guidance to customers.

The supervisory authorities are currently considering whether they should specify rules or further guidance regarding the content of communications plans.

Feedback loop

In order for the process to be effective in improving and maintaining operational resilience, it needs to be repeated regularly, with the lessons learned being integrated into subsequent iterations. A crucial point with respect to responses is to ensure that any successes, incidents or 'near misses' are reviewed honestly and openly within the firm. Practices, planned responses and monitoring should be adjusted to take into account any learnings gained through incidents and experiences, in order to ensure that the resilience of the firm is constantly evolving in response to events.

How Milliman can help

Milliman's deep expertise in risk management derives from our cutting edge research and practical experience of working with clients to assist them with their risk management and modelling needs. Our clients know that they can have confidence in us to provide an excellent service and innovative, effective and dynamic solutions that fully meet their needs. We don't believe that all companies are the same, so our approach enables us to ensure that the solution each client receives is tailored to its precise circumstances and maturity level.

In the operational resilience area, we offer assistance with:

- Review of existing risk management frameworks
- Gap analysis review
- Development of risk appetite statements and articulating them in terms of impact tolerances
- Design and build of operational risk models to facilitate understanding and quantification of risks
- Development of risk management frameworks which improve operational resilience

If you have any questions or comments on this paper, or on any other issues affecting operational resilience, please contact any of the consultants below or your usual Milliman consultant.

Milliman

Milliman is among the world's largest providers of independent consulting. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

Milliman maintains a strong and growing presence in Europe with over 350 professional consultants serving clients from offices in Amsterdam, Brussels, Bucharest, Dublin, Dusseldorf, London, Madrid, Milan, Paris, Warsaw, and Zurich.

uk.milliman.com

CONTACT

United Kingdom

Claire Booth
claire.booth@milliman.com

Tanya Hayward
tanya.hayward@milliman.com

Peter Moore
peter.moore@milliman.com

Sophie Smyth
sophie.smyth@milliman.com

Milliman does not certify the information in this paper, nor does it guarantee the accuracy and completeness of such information. Use of such information is voluntary and should not be relied upon unless an independent review of its accuracy and completeness has been performed. Materials may not be reproduced without the express consent of Milliman.
Milliman is not a law firm. Nothing in this paper should be considered legal advice. Please consult your legal adviser for advice specific to your legal scenario.