Deloitte Audit SRL
4-8 Nicolae Titulescu Road,
East Entrance, 2nd Floor,
Sector 1, 011141, Bucharest
Romania
Tel: +40 21 222 16 61
Fax: +40 21 222 16 60
www.deloitte.ro

Deloitte Banking Alert

23 July 2018

Operational resilience - The UK supervisory approach

In May 2018, the ECB published the Framework for testing resilience to Cyber Attacks. A few days ago, the Bank of England (BoE) and the Financial Conduct Authority (FCA) have released a *Discussion Paper (DP)* on Operational Resilience.

The DP emphasises incident recovery – using the concept of "impact tolerance" – and highlights the regulators' focus on the ability of firms to resume critical business services, introducing enhanced expectations for Boards and senior management in the UK financial sector. The DP is of primary interest to CROs, COOs, CISOs, heads of operational resilience or cyber risk and Board members at financial services firms regulated by the BoE, FCA or Prudential Regulation Authority (PRA).

The DP gives a **very important indication** of how the thinking of UK regulators has evolved on **matters such as cyber risk**. It takes a broad view of the kind of incidents firms may face, and accepts that some disruptions are inevitable. In effect, if implemented, this approach asks firms to prepare for and demonstrate their resilience to a much larger range of operational scenarios, including ones that may arise in third parties that they outsource any systems or processes to.

This approach will push firms to **prioritise and invest in areas that allow them to recover their business services** after a severe disruption, and also to continue to improve the capabilities that help them maintain continuity of service through more minor incidents. For some firms this may become a significant factor in how they evaluate decisions about systems' enhancement and replacement.

Impact tolerance is an important concept in the DP. In essence, it is an upper limit for the impact to business services that a firm is prepared to tolerate as a result of a "severe but plausible" operational disruption. It is expected to be set by the Boards and senior management of firms and expressed as a set of specific metrics on the duration, volume or nature of a disruption. This is a more advanced approach than recovery time objectives (RTOs) and one that takes into account the severity of a disruption and the number of customers or

stakeholders affected. In practice firms may decide to adopt a "twin-track" approach to operational resilience. First, while continuing to prevent minor disruptions is important, firms should accept that minor disruptions will happen. Our view is that in such circumstances the regulators expect greater focus on planning for maintaining continuity of business services. Second, by applying concepts such as impact tolerance (similar to the concepts of Maximum Acceptable Outage and maximum Period of Tolerable Disruption defined in ISO 22301), the regulators believe firms will be able to make better informed decisions on investment in resilience and, more importantly, be able to prioritise the recovery of the most important business systems in more severe scenarios.

In May 2018, the ECB Published the Framework for Testing Resilience to Cyber Attacks

ECB published the European framework for Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) in May 2018, the first Europe-wide framework for controlled and bespoke tests against cyber attacks in the financial market. This framework enables European and national authorities to work with financial entities to put in place a program to test and improve their resilience against sophisticated cyber attacks.

The TIBER-EU framework facilitates a harmonized European approach toward intelligence-led tests which mimic the tactics, techniques, and procedures of real hackers who can be a genuine threat. TIBER-EU-based tests simulate a cyber attack on an entity's critical functions and underlying systems, such as its people, processes, and technologies. This helps the entity to assess its protection, detection, and response capabilities against potential cyber attacks, thus enabling it to learn and evolve to a higher level of cyber maturity. The TIBER-EU framework has been designed for national and European authorities and entities that form the core financial infrastructure, including entities with cross-border activities which fall within the regulatory remit of several authorities. The framework can be used for any type of financial-sector entity. For the purposes of the TIBER-EU framework, entities include payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector.

The UK Supervisory Approach to Operational Resilience

In publishing the DP, the **UK regulators emphasised a number of key messages**, which summarise the approach they envision:

1. Operational resilience is best managed by focusing on the **delivery of business services**, rather than on systems and processes. This includes an expectation that firms should prioritise their most important business services and be able to identify the systems and processes that support them, whether internally to the organisation or if outsourced to a third party.
2. The UK **Financial Policy Committee** (FPC) intends to set its own impact tolerance for operational disruptions to "**vital services**" that the financial system provides to the economy. The FPC's intention is to avoid disruptions that would cause "material

economic impact". The practical implication of this is likely to be a more prescriptive supervisory approach to impact tolerance for larger or systemically important firms.

3. **Boards and senior management** need to take more direct responsibility for the operational resilience of their firms and should be central to the process of setting impact tolerances and identifying which business services are prioritised. The DP notes a range of existing regulatory powers supporting this outcome, including the introduction of a Senior Management Function for internal operations and technology (SMF 24).
4. Firms should focus on improving **communications during disruptions, particularly those affecting the customer-oriented services** they provide. Noting recent high-profile disruptions in the financial services sector, the DP highlights the growing role supervisors could play in assessing the speed and effectiveness of both external and internal communications plans that firms have in place to respond to operational failures.
5. Firms will need to articulate impact tolerances for their business services based on clear metrics and outcomes, setting a **target for how they expect to recover from a severe but plausible disruption**. These impact tolerances will be relevant to the systems supporting business services, including any systems that are maintained or provided by third parties. The DP does recognise, however, that firms may sometimes not be able to meet these recovery expectations in the event of an extreme disruption scenario.
6. Supervisors will **assess the operational resilience of firms** using a number of tools, including through the use of stress tests, as announced by the FPC in its June **Financial Stability Report**. The DP also notes that supervisors will assess the impact tolerances set by firms, request changes be made to them, and may consider setting their own impact tolerances where they deem necessary.

What to Expect Next?

It is important to note that the DP does not put in place any immediate rule changes or new supervisory procedures, but is rather meant to solicit feedback from the industry on how upcoming rules should be designed and implemented.

Nevertheless, these messages represent an important initial step in what we expect to be an area of **significant supervisory activity** on the part of the authorities in the coming months. The FPC has committed to providing further detail on its 2019 cyber risk stress-testing programme by Q4 2018, and the BoE and FCA will spend this time analysing feedback received and further developing the concepts in this paper.

For impact tolerance, in particular, we see a number of **critical decisions that the authorities must make** as they put this concept into practice; namely, how prescriptive the FPC wishes to be in setting impact tolerances for systemically-important firms; and, identifying the type of "severe but plausible" scenarios that they will expect firms to plan to be able to recover from.

Feedback on the DP is encouraged by the BoE and FCA, who are particularly interested in hearing more about existing metrics that firms use to benchmark their recovery from operational disruptions. The DP is open for comment until 5 October 2018.

Deloitte.

How can Deloitte help?

We help organizations become more resilient by strengthening their operational risk programs. To that end, we offer comprehensive solutions for the:

- Development of a **resilience framework** to ensure that banks have the necessary systems, documentation, assurance and controls necessary to support their resilience efforts
- Designing the **strategy** and solutions to help clients build resilient operational risk programs.
- **Technology transformation** solutions that can change the way organizations experience operational risk management.
- Develop/Enhance the **RCSA framework** to include a complete view of risks and controls to enable the later performance,
- Support in the clear articulation of the **Risk Appetite Framework**, KRI and risk tolerances for all risks, including non-financial risks. The impact of **non-financial risks** may, at times, exceed the financial cost.
- **Integrate RCSA programs** into all operational risk initiatives and adopting standard risk taxonomies throughout the organisation.
- Use **RCSA information** to identify concentration of risk or potential control failures and support strategic budgeting. The framework can be used explain why expenditures and resources are being deployed to targeted problem areas within the organisation.
- **Cyber Risk Management and Compliance**: define tailored cyber risk management frameworks; set and implement cyber control frameworks and ensure compliance through cyber security regulations.
- **Vulnerability assessment**: assessment of the risks posed by security vulnerabilities in your systems
- **Cyber Security Continuous testing**: Penetration testing and Red Teaming
- **Cyber incident response**: Through our blend of people, methodology and technology, we can provide rapid reporting and an understanding of the systems attacked to help triage the data at risk.
- **Cyber Forensic**: predict, detect, and respond to the risks and vulnerabilities that come from global corruption, litigation, fraud, financial mismanagement, and other threats.

Deloitte.

For further questions regarding the aspects mentioned in this alert, please don't hesitate to contact us.

Dimitrios Goranitis
FSI Risk & Regulatory Advisory
Partner, Deloitte Central Europe
Tel: +40 751 250 884
Email: **digoranitis@deloittece.com**

Irina Arsinte
FSI Risk & Regulatory Advisory
Manager, Deloitte Romania
Tel: +40 730 585 755
Email: **iarsinte@deloittece.com**