WORLD FEDERATION OF EXCHANGES

October 2018

WFE Response to the BoE-FCA-PRA Discussion Paper: *Operational Resilience*

Visit us at:
www.world-exchanges.org

Background

The World Federation of Exchanges (WFE) is the global trade association for exchanges and clearing houses, representing more than 200 Market Infrastructure Providers. Our members include exchange groups and standalone CCPs.[1]

Our members are both local and global, operating the full continuum of market infrastructures in both developed and emerging markets. Of our members, 36.8% are in Asia-Pacific, 42.6% in EMEA and 20.6% in the Americas. WFE exchanges are home to nearly 45,000 listed companies, and the market capitalisation of these entities is over $82.5 trillion; around $81.8 trillion (EOB) in trading annually passes through the infrastructures WFE members safeguard.[2]

The WFE works with standard setters, policy makers, regulators and government organizations around the world to support and promote the development of fair, transparent, stable and efficient markets. The WFE shares regulatory authorities' goals of ensuring the safety and soundness of the global financial system, which is critical to enhancing investor and consumer confidence, and promoting economic growth.

Cyber risk matters have been – and continue to be – a matter of great priority for our membership, and one in which significant time, effort and money has been invested. We therefore welcome the opportunity to offer our perspectives and further contribute to the dialogue in order to secure the shared objectives of fair and orderly markets that promote the safety and resilience of the global financial system.

Executive Summary

The WFE welcomes the Bank of England, FCA and PRA's discussion paper on operational resilience calling on firms to demonstrate their operational resilience in the event of a cyber-attack or IT disruption, as well as using this paper to inform their approach to building cyber resilience in the UK financial system. The key points we make in response to the questions below are: (i) the proposed approach on objectives relating to continuity of business services could be feasible and proportionate, to the extent that it recognises current practices within organisations that already have recovery time and recovery point objectives defined as part of their BCM / DR requirements; (ii) there are differing levels of key risk indicator maturity between firms for measuring risk appetite / risk tolerances; and (iii) communication processes are defined in incident management and crisis management planning.

1 The WFE membership list can be found here
2 As at end 2017

Questions

SECTION 2: OPERATIONAL RESILIENCE OF BUSINESS SERVICES

A) What are readers' views on the proposed focus on continuity of business services? Would a service rather than systems-based approach represent a significant change for firms and FMIs compared with existing practice? What other approaches could be considered?

The WFE represents a vast number of exchanges and CCPs and it is apparent that business services mapping (i.e. linking of business services, processes, systems, owners etc.) maturity tends to vary organisation to organisation. This could, in part, be driven by the automated vs. manual nature of the service management capability. For example, if an organisation uses an IT Service Management tool to manage this then the services mapping component is easier than if it is maintained in manual process maps.

A few years ago, many in the Internal Audit profession moved to a more holistic services approach to auditing (i.e. looking at the business as a whole and process and systems that support it vs. performing 'business process' and separate 'IT process / systems' audits).

Paragraph specific points:

Para 2.5 – This is an interesting point about supervisory authorities (SA's) disagreeing with the firm on priorities – the SA's would need to have a very good understanding of the organisations business to do this.

Para 2.7 – The setting / mandating of definitive service recovery timeframes needs to be balanced against the risks of bringing the service up too early (e.g. in a cyber scenario there could be concerns about data completeness, accuracy and validity even if the service has been recovered).

Para 2.9 – The building of resilient business services should also consider system design – e.g. high availability / resilient architecture.

Para 2.11 – A clarification on what is meant by an "understanding" of third-party firms' resilience is needed, as this understanding could also be linked to risk – e.g. the risk profile of a bank with many retail customers and suppliers accessing back end systems is different to a firm that deals with participants accessing services over private networks with no (or control limited) access to the back end.

The proposed approach on continuity of business services does not appear (in concept or principle) to be too far removed from current BCM / DRP planning. Organisations do this through risk assessment, business impact analysis, scenario testing, stress testing, BCP testing etc.

SECTION 3: OPERATIONAL RESILIENCE AND THE FPC

B) Would encouraging firms and FMIs to consider their contribution to the vital services that the real economy demands change the way they manage operational resilience, and if so how? What additional costs would this incur?

Paragraph specific point:

Para 3.1 – A general comment is that industry wide testing is a good idea – particularly for cyber security scenarios. This should be facilitated by relevant authorities / Government agencies (e.g. Cyber Security Centres / response teams).

We note that encouraging firms to consider their contribution to the vital services they provide is not a new concept. This is considered in current risk assessment and response planning – particularly in DR / BCP scenarios. The setting of mandated recovery times can be dangerous as it might encourage firms to recover at the expense of due diligence over data completeness, accuracy and validity. Setting business specific goals is another approach (e.g. completion of end of day settlement rather than "*systems recovered in 2 hours*") – this may mean other business processes are engaged even if the organisation's systems are not operational (i.e. state the objective in terms of business outcomes).

SECTION 4: OPERATIONAL RESILIENCE OF FIRMS AND FMIS

Paragraph specific points:
Para 4.1 – A firm's risk appetite should also be considered in the firm's operational resilience framework.
Para 4.2 – Clear standards should also include behavioural standards.
Para 4.4 – Having impact tolerances may also assist in system architectural design for new and changed systems.

Common practices (among the WFE membership) being employed – or are in the process of being employed – to meet the CPMI-IOSCO 2-hour recovery timeframe include:
- Risk assessments;
- Benchmarking of controls and processes to NIST and other frameworks;
- Enhancement to playbooks;
- External review of processes and controls;
- Scenario testing with teams and Enterprise Risk on a regular basis and with the Crisis Management team at least every 6 months;
- Penetration testing to test detection and recovery process;
- Input into system architecture design;
- Developing controls strategies (e.g. cyber security strategy) to improve prevention, detection, recovery and resolution processes;
- Better direction and response to reduce likelihood;
- Better testing and recovery strategies for extreme scenarios to reduce impact; and
- Resilience and explicit consideration for enterprise and solution architecture.

Para 4.48 – The process flow for policy development is a reasonable approach. Disruption would need to be defined per service. We note that "disruption" needs to be defined – there are many considerations such as impacts to market, customers, customer segment, regulators, the firm itself.

C) How do boards and senior management currently prioritise their work on operational resilience?

The WFE represents a vast number of exchanges and CCPs – as such, broadly speaking, senior management and board work on operational resilience involves performing risk assessments and reporting these risks and resultant actions and frameworks to the organisations relevant committee's (e.g. management working groups, senior management steering committees such as the risk committee, board audit and risk committee). Senior management and the board then approve risk frameworks. Reporting can include key risks, control assessments, residual risks and accepted risks. Actions can be tracked and monitored to resolution through the relevant committees. In addition to risk assessments, regular BCP / DR, scenario and crisis management team testing is performed with results and lessons learnt reported to committees.

D) What changes are firms and FMIs planning to make to strengthen operational resilience over the next few years? How involved are board members in the planning, implementation and embedding of any changes? What are the likely benefits and costs involved?

Some WFE member exchanges and CCPs are implementing – or are in the process of implementing – 3-5-year projects (monitored by senior management and the board) to review and improve the ERM, technology risk, incident management and enterprise architecture frameworks. These projects are driven by senior executive steering groups and are then reported up to the board.

Benefits can include new and enhanced tools (e.g. GRC, service management, incident management, crisis management tools), a holistic and contemporary enterprise risk framework, greater consistency of risk assessment and acceptance, more real time risk management, increased resources, enhanced and defined and measured KRI's and risk tolerances. Overall, improved risk management from raising a risk through to mitigation or acceptance.

SECTION 5: CLEAR OUTCOMES FOR OPERATIONAL RESILIENCE

E) What are readers' views on the possibility of firms and FMIs being asked to set impact tolerances for their most important business services?

The WFE can see some benefit in the possibility of firms being asked to set impact tolerances. We suspect that it would take considerable time to perform to the level regulators would be comfortable with. It would be worthwhile for the regulators to define a scope and framework (e.g. what impacts should be considered and prioritised – market, customer, firm, participant, regulator etc.) A framework might get some consistency between FMI's.

F) **What approach and metrics do firms and FMIs currently use**?

WFE members use a range of statistics and measures around risk assessment, KRI monitoring, threat assessment, mathematical modelling, capacity and availability, and RTO / RPO (set by BCP) as key metrics.

G) If these proposals would require some firms and FMIs to update part of their existing risk management framework, what would this involve?

We note that often in extreme scenarios of complete loss or corruption, an increased level of focus across the industry – specifically on testing – is required from a service perspective to ensure all dependencies are adequately covered. If adequate testing is not conducted, then failures can arise over the assumption that the data available is correct.

H) What are readers' views on producing an impact tolerance statement as described? What relevant operational resilience risk management documentation do firms and FMIs already produce, and how does this differ from impact tolerance statements?

- The inverse of RTO / RPO i.e. how long can an organisation tolerate the impact before the business is irreversibly damaged.
- Consideration of designing in the equivalent to 'limp home mode' i.e. what degraded state would be acceptable while a full state of operations is recovered.

SECTION 6: SUPERVISORY ASSESSMENT OF OPERATIONAL RESILIENCE

I) What operational resilience tests or scenarios do firms and FMIs already consider and undertake for their own risk management purposes? What factors do firms and FMIs take into account when devising operational resilience tests or scenarios?

-

J) How do boards and senior management currently gain assurance over the operational resilience of their firm or FMI?

-

K) What are readers' views on the proposed developments to the supervisory authorities' approach to operational resilience?

Broadly positive as long as there is a sensible and pragmatic approach to implementation. This is likely to require a significant change to the approach that the financial services and FMI industries have followed to design and build resilient systems and processes, and it will take some time to evolve operational environments.