xcina Consulting
A Shearwater Group plc Company

worksmart
REGULATORY CHANGE MEETS BUSINESS ADVANTAGE

Operational Resilience & Outsourcing – New Expectations!

11.00am Thursday 5th August 2021

Contents

Background and Context

- Key priority for supervisory authorities
- Joint PRA, FCA and Bank of England Operational Resilience Discussion Paper in 2018, consultations in December 2019
- Joint covering document with their respective policy statements on 29 March 2021
- PRA's new policy statement on Outsourcing issued at the same time
- Operational Resilience policies complement various existing requirements including:
  - Recovery and Resolution Planning (RRP), Operational Continuity in Resolution (OCIR), Resolvability Assessment Framework (RAF) and Business Continuity Planning (BCP)
  - EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) and outsourcing arrangements (EBA/GL/2019/02)
- Aligned with parallel developments / convergence at international level:
  - Basel Committee for Banking Standards (BCBS) guidelines on principles for operational resilience (31 March 2021)
  - European Commission Digital Operational Resilience Act (DORA) draft proposal (Sept 2020)
  - US Joint Authorities' paper on operational resilience (Oct 2020)
- It's not just a regulatory exercise

Definitions

- **Operational resilience:** ability of firms, financial market infrastructures and the financial services sector as a whole to prevent, respond to, recover and learn from **operational disruptions**. (Bank of England, PRA and FCA).
- Regulators' approach to operational resilience assumes that: **disruptions will occur** which will prevent firms from operating as usual and providing their services for a period.
- A **business service** is a service that a firm provides which delivers a specific outcome or service to an identifiable user external to the firm. It should be distinguished from business lines, which are a collection of services and activities.
- **Important business services**: the services a firm provides which, if disrupted, could:
  - pose **a risk** to a **firm's safety and soundness** or, the **financial stability** of the UK (**PRA**)
  - potentially cause **intolerable harm** to the **consumers** of the firm's services or **risk to market integrity** (i.e. soundness, stability or resilience of the UK financial system) (**FCA**)
- **Impact tolerance:** maximum tolerable level of disruption to an important business service assuming disruption to the supporting systems and processes will occur.
- **Consumers** refer to those that are the direct consumers of the firm's services or in other ways dependent upon them. This includes both retail and wholesale market participants.

Scope: who is impacted?

The following are in scope:

- UK banks, building societies, and PRA-designated investment firms (“banks”)
- UK Solvency II firms, the Society of Lloyd’s, and its managing agents (“insurers”)
- Recognised Investment Exchanges (RIEs)
- Enhanced scope senior managers and certification regime (SM&CR) firms
- Entities authorised or registered under the Payment Services Regulations 2017 (PSRs 2017) or the Electronic Money Regulations 2011 (EMRs 2011)

Those not in the above scope (e.g. Core firms under SM&CR): given recent events and the potential future regulatory focus, they would probably benefit from familiarising themselves with the regime

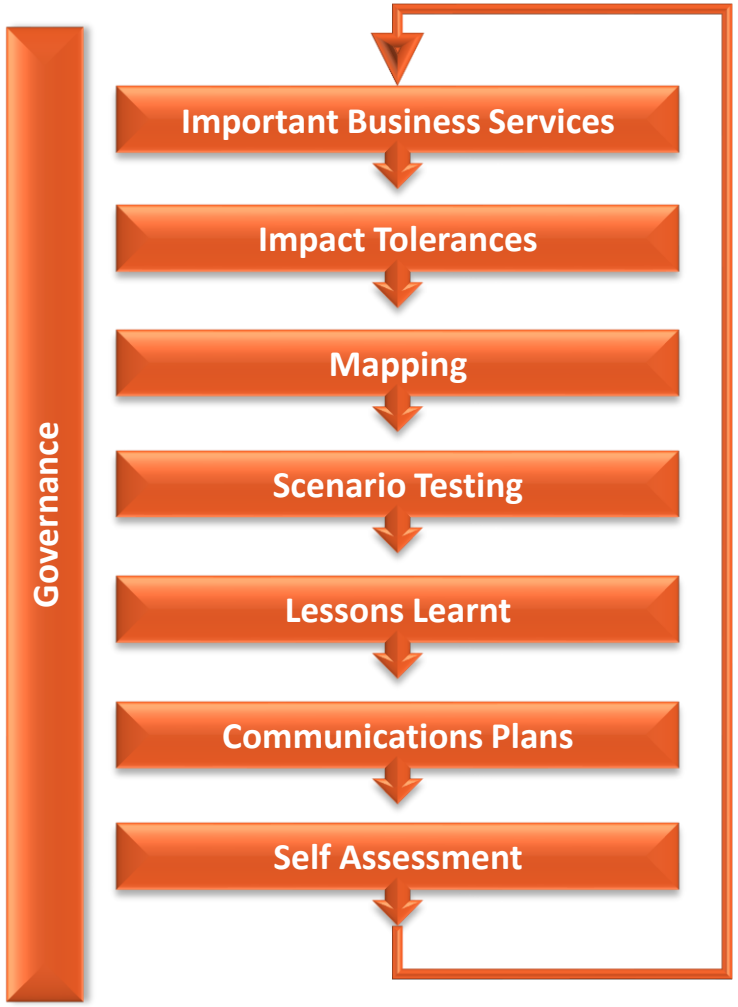
Those providing services to a firm in scope may also be impacted as they need to demonstrate resilient processes to support the client firm

Irrespective of the above, all firms should also continue to meet their existing obligations (e.g. business continuity, outsourcing, information security)

Overview of Requirements

Firms are expected to:

- Identify their **important business services (IBS)**
- Set **impact tolerances** for each IBS
- Identify and **map** the supporting resources i.e. people, processes, technology, facilities and information supporting the IBS (including any 3rd parties)
- Conduct **scenario testing** to assess the ability to remain within impact tolerances through a range of **severe but plausible** disruption scenarios
- Conduct **lessons learnt** exercises to assess, prioritise, and invest in the firm's ability to respond and recover from disruptions
- Develop internal and external **communications** plans for when important business services are disrupted
- Maintain an updated **self-assessment** document detailing the firm's operational resilience journey
- Make operational resilience a priority at Board and Executive levels (**Governance**)



Timeline

- **Effective date**: The rules come into force on **31 March 2022**
- Before 31 March 2022, firms must:
  - Identify and map their IBS
  - Set PRA and FCA impact tolerances for each IBS as appropriate
  - Carry out mapping and scenario testing
  - Identify any vulnerabilities in their operational resilience
  - Define a prioritised plan to address any vulnerabilities and set out how they will comply no later 31 March 2025.
- Their self-assessment should be documented, signed off by the Board and ready for the regulators
- After 31 March 2022, firms will need to review their IBS at least annually, or whenever there is a material change
- As soon as reasonably practicable after 31 March 2022 (on a risk basis), and no later than 31 March 2025, firms must be capable of maintaining all IBS within their respective impact tolerances in severe but plausible scenarios
- Hence, they must have made any necessary investments and remediation to enable them to operate consistently within their impact tolerances.
- After 31 March 2025, maintaining operational resilience will be dynamic. Firms should then have effective strategies, processes and systems in place to manage operational resilience.

Background and Context

The policy statement on Outsourcing & TPRM aims to leverage and complement existing requirements:

- Complements PRA's policy proposals on operational resilience
- Facilitates greater resilience and adoption of the cloud and other new technologies as set out in the Bank of England's response to the Future of Finance report
- Implements and expands on the EBA Guidelines on outsourcing arrangements (EBA Outsourcing GL), which integrated previous EBA Cloud Outsourcing Guidelines
- Takes into account other relevant international guidelines and standards, notably from:
  - EBA (Guidelines on ICT and security risk management)
  - EIOPA (European Insurance and Occupational Pensions Authority)
  - BCBS (Basel Committee)
  - FSB (Financial Stability Board)
  - MODR (Commission Delegated Regulation on organisational requirements and operating conditions)
  - IOSCO (International Organisation of Securities Commissions)
- FCA did not propose new Outsourcing requirements but reminded firms of existing rules and guidance (in particular SYSC 8 and SYSC 13.9, FG16/5 - FCA Guidance for firms outsourcing to the cloud and other third-party IT services, and EBA).

Scope

Who does it apply to?

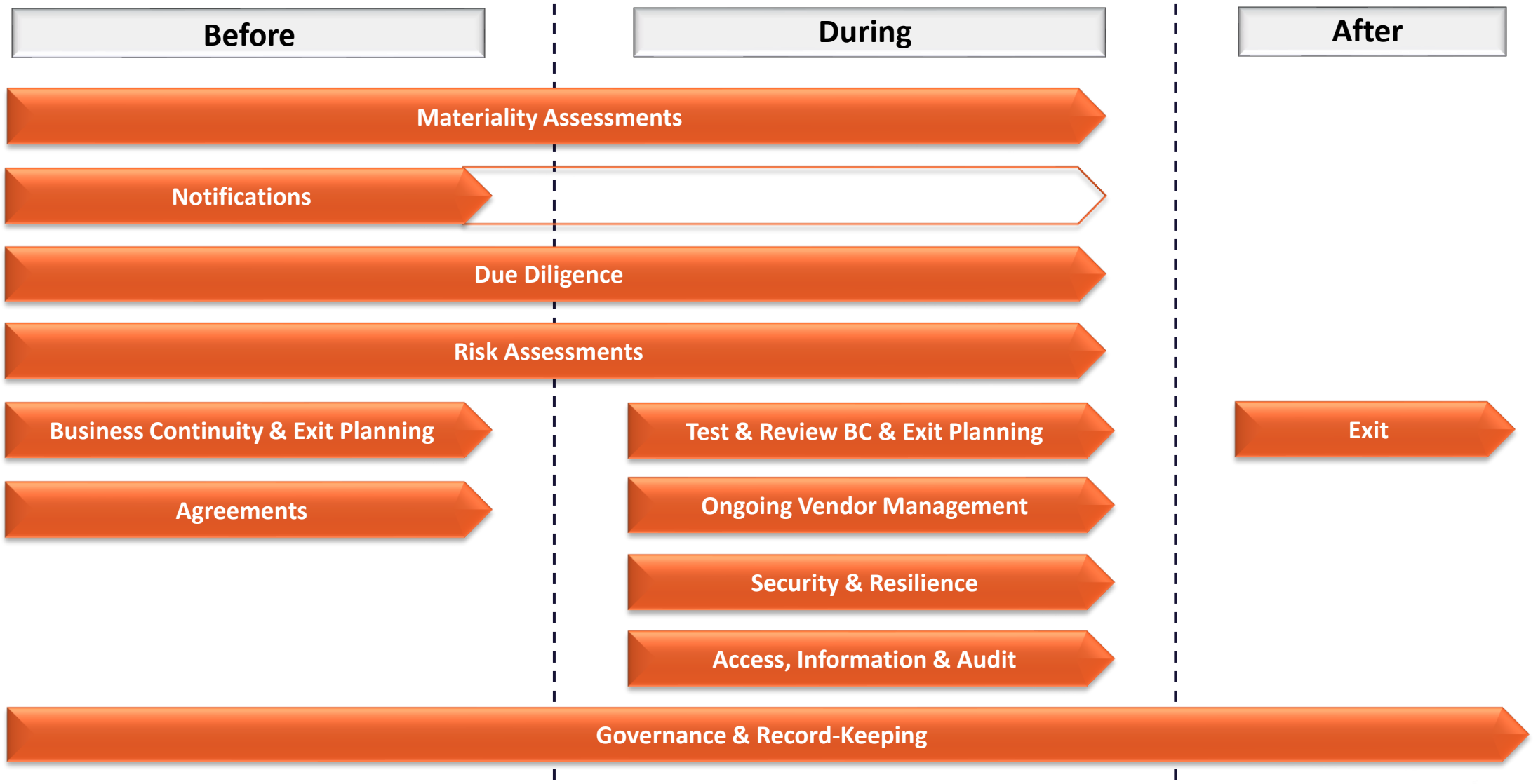
- UK banks, building societies, and PRA-designated investment firms (“banks”)
- Insurance and reinsurance firms and groups in scope of Solvency II, including the Society of Lloyd’s and managing agents (“insurers”)
- UK branches of overseas banks and insurers (“third-country branches”)

There are existing Outsourcing requirements for FCA-regulated firms set out in SYSC 8 and 13.9

Definitions

- **Third party:** any external entity that has entered into a business relationship or contract with the Firm to provide a product or service.
  - Includes suppliers, vendors, business partners and affiliates, brokers, distributors, resellers, and agents
  - Can be both upstream (suppliers and vendors) and downstream (distributors and agents)
- **Outsourcing**: an arrangement of any form whereby a service provider performs **a process, a service or an activity**, which would otherwise be undertaken by the Firm itself (PRA and FCA)
- **Non-outsourcing third-party arrangement**: Some third-party arrangements falling outside the definition of outsourcing can give rise to significant risks and should be subject to appropriate monitoring and risk-based controls.
- **Material (= Critical or Important)**: A function is regarded as material where a weakness or failure of the service would cast doubt on the Firm's:
  - **Safety and soundness**, including its financial performance, financial resilience (i.e. assets, capital, funding and liquidity), operational resilience (i.e. ability to continue providing important business services) and soundness or continuity of its regulated activities
  - Continued satisfaction of the Threshold Conditions and of the Firm's regulatory obligations.

Overview of Requirements



Timeline

Timeline

- Firms must comply with the expectations by 31 March 2022
- Outsourcing arrangements entered into on / after 31 March 2021 should meet the expectations by 31 March 2022
- Firms should seek to review and update legacy outsourcing agreements entered into before 31 March 2021 at the first appropriate contractual renewal or revision point to meet the expectations as soon as possible on or after 31 March 2022 (**PRA**)
- Where arrangements of critical or important outsourcing arrangements have not been finalised by 31 March 2022, firms should inform us (**FCA**).

What should Firms be doing (before 31/3/2022)?

Operational Resilience
Outsourcing & TPRM

Outsourcing and TPRM:

1. Assess current TPRM framework and align with new requirements (governance, policy, processes, register, MI,…)
2. Review / repapering of legacy agreements
3. Consider current operating model and capabilities and how to operate going forward to meet increased workload and increased activity

Operational Resilience:

4. Identify and map their IBS
5. Set PRA and FCA impact tolerances for each IBS as appropriate
6. Carry out mapping and scenario testing
7. Identify any vulnerabilities in their operational resilience
8. Define a prioritised plan to address any vulnerabilities
9. Prepare self-assessment document
10. Assess implications for current Governance and Operational Risk Management framework – policy, standards, guidelines, reporting and monitoring – to manage operational resilience consistently going forward

xcina Consulting
A Shearwater Group plc Company

worksmart
REGULATORY CHANGE MEETS BUSINESS ADVANTAGE

For further information,

please get in touch with the speakers:

Email: lindsey.domingo@xcinaconsulting.com

Phone: +44 (0) 795 848 1452

Xcina Consulting Limited

1 King William Street

London

EC4N 7AF

www. xcinaconsulting.com

Email: julie.pardy@worksmart.co.uk

Phone: +44 (0) 7740264483

Worksmart Limited

Beech House, Breckland,

Linford Wood, Milton Keynes,

MK14 6ES

www.worksmart.co.uk