Osborne Clarke Future of Financial Services Week

Stronger regulation – operational resilience

26 January – 3 February 2022

Speaking with you today

Paul Harris
Partner
United Kingdom

T +44 207 105 7441
paul.harris@osborneclarke.com

Mark Taylor
Partner
United Kingdom

T +44 20 7105 7640
mark.taylor@osborneclarke.com

Nick Price
Associate Director
United Kingdom

T +44 207 105 7496
nick.price@osborneclarke.com

1 What operational resilience requires

Operational Resilience

What is operational resilience?

The ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions.

What prompted the new rules?

- Increasing occurrences of cyber attacks, IT failures and power failures
- Covid-19 pandemic

Who do the rules apply to?

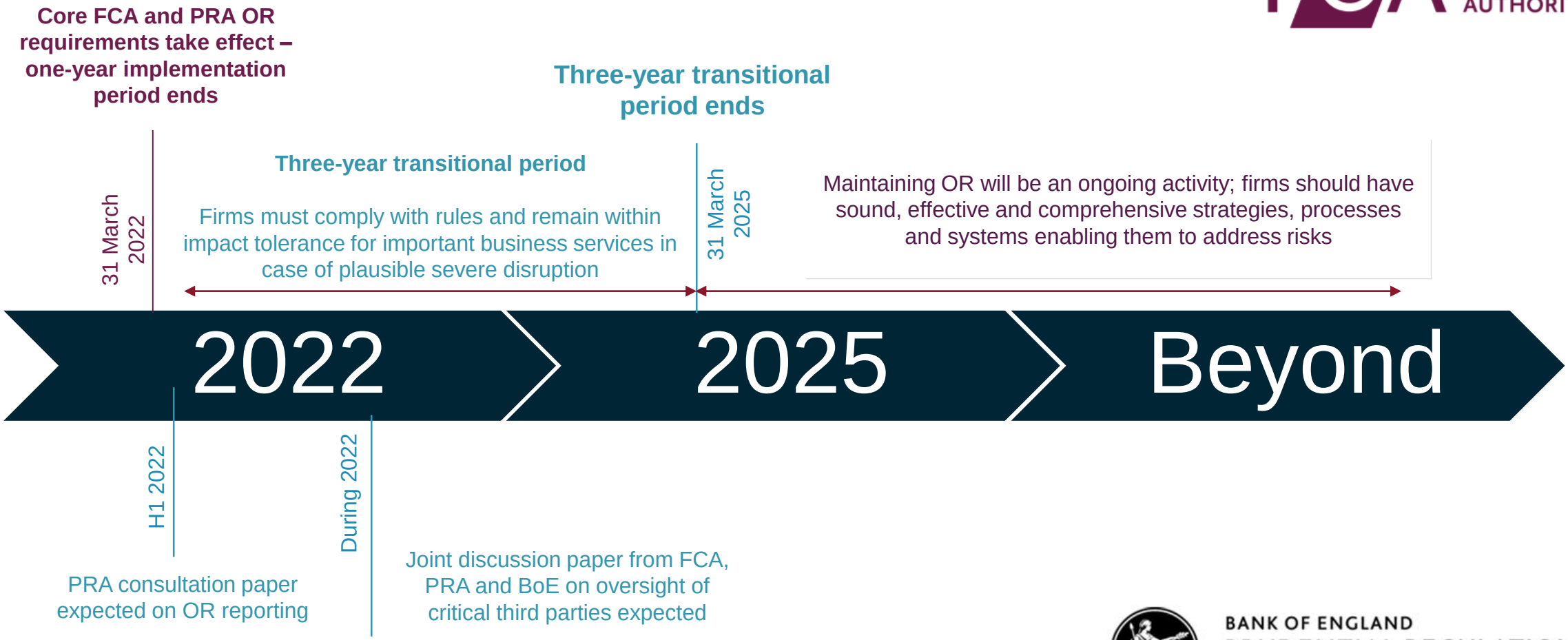
The FCA and PRA operational resilience rules will apply to:

- UK banks, building societies, PRA-designated investment firms, UK Solvency II firms, the Society of Lloyd's and its managing agents;

The FCA operational resilience rules will apply to:

- UK recognised investment exchanges, enhanced firms under the Senior Managers & Certification Regime and entities authorised under the Payment Services Regulations 2017 and Electronic Money Regulations 2011

Timeline


Core FCA and PRA OR requirements take effect – one-year implementation period ends
Three-year transitional period ends
31 March 2022
Three-year transitional period
Firms must comply with rules and remain within impact tolerance for important business services in case of plausible severe disruption
31 March 2025
Maintaining OR will be an ongoing activity; firms should have sound, effective and comprehensive strategies, processes and systems enabling them to address risks
2022
2025
Beyond
H1 2022
PRA consultation paper expected on OR reporting
During 2022
Joint discussion paper from FCA, PRA and BoE on oversight of critical third parties expected

Core requirements due by 31 March 2022

Boards and senior management must give certain approvals and review their operational resilience documentation

Progress on implementing operational resilience and potential areas of supervision

Firms should be well advanced in their mapping and scenario testing which enables firms to:

- Identify **important business services**
- Setting **impact tolerances** for each **important business service**
- Identify vulnerabilities in sufficient time and take measures to remediate them.

The speed at which vulnerabilities are identified and remediated will be an area of supervisory focus.

Firms are responsible for accurately mapping any relationship with outsourced providers.

The supervisory authorities anticipate scenario testing as being an area for supervisory discussion as best practice develops.

The self-assessment document is a snapshot to demonstrate a firm's operational resilience at a specific point in time and must be available if and when requested.

2 Outsourcing and third parties

Outsourcing and third parties

- Focus of operational resilience rules is on outcomes
- Practical importance of outsourcing / third parties to regulated firms
- FCA expectations around operational resilience:
  - comprehensive understanding and mapping of people, processes, technology, facilities and information required to deliver each IBS
  - assessing the risks and controls in place

Interaction with outsourcing requirements

- Existing rules in place regarding outsourcing and IT services for regulated firms
  - e.g. under MiFID II, SYSC, FCA Guidance 16/5, EBA outsourcing guidelines
- Outsourcing generally defined as those arrangements which regulated firm would usually provide themselves
  - not all inputs from third parties necessarily caught
  - "fourth party" risk

➢ Some arrangements not covered by existing outsourcing guidelines etc still potentially important from operational resilience perspective

  - enhancements to these arrangements required?

Other considerations

- Intra-group arrangements – no special treatment
- Offshore arrangements can pose additional risks
- Outsourced data
  - e.g. where stored, processed or transmitted by third party providers
- Sub-outsourcing arrangements
  - importance of identifying it
  - managing risks associated with sub-outsourcing
- EU Digital Operational Resilience Act (DORA)

3 Supervision and Enforcement

Examples of recent operational disruptions and enforcement action by the Regulators

2014: Joint enforcement action was taken by the FCA and PRA to fine Royal Bank of Scotland Plc, National Westminster Bank Plc and Ulster Bank Ltd £42 million for IT failures which occurred in June 2012 and resulted in the Banks' customers being unable to access banking services.

2018: The FCA fine Tesco Personal Finance plc £16.4 million for failing to exercise due skill, care and diligence in protecting its personal current account holders against a cyber attack which took place in November 2016.

2018: TSB migration failure which caused extensive service disruption and instability for TSB customers. The migration failure cost the bank £330 million and the loss of 80,000 customers.

2019: Joint enforcement action was taken by the FCA and PRA against R. Raphael & Sons plc, resulting in a combined fine of around £2 million, for failing to manage its outsourcing arrangements properly between April 2014 and December 2016.

2021: Internet outages in July 2021 affected customers from PayPal, Tesco Bank, Sainsbury's bank, HSBC, Lloyds, Barclays, American Express and TSB.

Governance and enforcement

Boards and senior management must be able to guide their businesses through an operational disruption.

The individual accountability provisions under the SM&CR will also be relevant to the senior manager responsible for implementing operational resilience and any failure to ensure compliance.

The regulators can:

- Provide individual guidance to firms on whether their compliance with the operational resilience rules is adequate.
- Require a firm to take action or steps to address any failure to meet the operational resilience rules.
- Exercise their powers to vary or cancel a firm's Part 4 A permission on its own initiative in order to require the firm to take specific steps in line with its view to comply with the operational resilience rules.

Reporting an operational incident

The FCA expects firms to report "material" operational incidents under Principle 11 of the FCA's Principles for Businesses and, if dual-regulated, under Fundamental Rule 7 of the PRA's Fundamental Rules.

An incident may be material if it:

- results in a significant loss of data;
- results in the unavailability or control of IT systems;
- affects a large number of customers;
- results in unauthorised access to information systems

A breach of an impact tolerance must also be reported to the FCA.

The FCA can impose a fine for breach of Principle 11 and additional notification requirements in the Supervision (SUP) sourcebook of the FCA Handbook.

4 Concluding Remarks

Any questions?