House of Commons

Treasury Committee

IT failures in the financial services sector: Government and Regulators Responses to the Committee's Second Report of Session 2019

First Special Report of Session 2019–21

Ordered by the House of Commons to be printed 10 March 2020

HC 114
Published on 13 March 2020
by authority of the House of Commons

The Treasury Committee

The Treasury Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of HM Treasury, HM Revenue and Customs and associated public bodies.

Current Membership

Mel Stride MP (Chair) *(Conservative, Central Devon)*

Rushanara Ali MP *(Labour, Bethnal Green and Bow)*

Mr Steve Baker MP *(Conservative, Wycombe)*

Harriett Baldwin MP *(Conservative, West Worcestershire)*

Anthony Browne MP *(Conservative, South Cambridgeshire)*

Felicity Buchan MP *(Conservative, Kensington)*

Ms Angela Eagle MP *(Labour, Wallasey)*

Liz Kendall MP *(Labour, Leicester West)*

Julie Marson MP *(Conservative, Hertford and Stortford)*

Alison McGovern MP *(Labour, Wirral South)*

Alison Thewliss MP *(Scottish National Party, Glasgow Central)*

Powers

The committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/treascom and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are Emily Buckland (on secondment from the Bank of England), John-Paul Flaherty (Second Clerk), Sarah Goodwin (on secondment from the Prudential Regulation Authority), Rachel Kift (on secondment from the National Audit Office), Dan Lee (Senior Economist), Gosia McBride (Clerk), Aruni Muthumala (Senior Economist), Matt Panteli (Senior Media and Policy Officer), Yasmin Raza (on secondment from the Financial Conduct Authority), Baris Tufekci (Committee Support Assistant), Adam Wales (Chief Policy Adviser), Maciej Wenerski (Senior Committee Assistant), Marcus Wilton (Senior Economist), and Tony Verran (on secondment from HM Revenue & Customs).

Contacts

All correspondence should be addressed to the Clerk of the Treasury Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 5769; the Committee's email address is treascom@parliament.uk.

You can follow the Committee on Twitter using @commonstreasury.

First Special Report

On 28 October 2019, the Treasury Committee published its Second Report of Session 2019, *IT failures in the financial services sector* (HC 224). On 10 January 2020 we received the Regulators (Financial Conduct Authority, Bank of England and Prudential Regulation Authority) response to the report, and on 14 January 2020 we received the Government Response, both of which are appended below.

Appendix 1: Regulators Response

IT failures in the Financial Services Sector – Second Report of Session 2019

We welcome the Treasury Select Committee's (the Committee's) report dated 28 October 2019 regarding IT failures in financial services. We agree with the Committee's observation that improved operational resilience will reduce the number and the impact of IT or operational incidents. We also welcome the Committee's recommendations for improving operational resilience in the financial sector. This is an important area for the Prudential Regulation Authority (PRA), the Financial Conduct Authority (FCA), the Bank of England ('the Bank') in its capacity of supervising financial market infrastructures (FMIs) (collectively 'the Authorities') and the financial sector. We are well into the process of developing and implementing major changes to our regulatory framework for ensuring adequate operational resilience. The Committee has raised some important issues which we will take forward as we develop that regulatory framework.

When the Authorities gave evidence to the TSC enquiry, we had not yet published our Consultation Papers setting out our proposed framework of operational resilience policies. These were published on 5 December 2019. The proposals are consistent with the recommendations made by the Committee and represent an important milestone in our approach to embedding operational resilience into the regulatory framework for the financial sector. The consultation period closes on 3 April 2020, and subject to the outcome of that consultation the Authorities expect to publish final policy during the second half of the year.

The annex to this letter sets out how under our existing supervisory approaches and once the new operational resilience policy is in place, through additional supervisory scrutiny, we plan to address the Committee's recommendations. We also set out thoughts on areas that will require further work, both by industry and the Authorities.

We would like to highlight four key areas that will contribute to greater operational resilience in the finance sector:

1. **Supervisory approach and tools:** we agree that effective supervision by the Authorities is an important element of improving the operational resilience of firms and FMIs. Our proposals include clear standards for operational resilience, connecting requirements and expectations to the Authorities' public interest objectives. These proposals allow for supervisory action if firms or FMIs do not meet the standards set out in the policy.

2. **Incident reporting and management:** there are existing obligations on firms and FMIs to report certain operational incidents to the Authorities. However, there is a lack of consistency in the way incidents are reported to the Authorities, reflecting the complex and evolving environment in which firms and FMIs operate. This is an area that the Authorities and industry are currently tackling and further work will be needed. The Committee's recommendations will be helpful in shaping our approach. On incident management, we propose that firms and FMIs test their incident management procedures to ensure they can remain within impact tolerances. The focus on being able to resume an important business service within an impact tolerance should also concentrate board and management attention on what matters most in the event of an incident, including when and how to contact customers and Authorities.

3. **Third parties and new technology:** our proposed new framework specifies that a firm or FMI's operational resilience should not be undermined when it relies on a third party, wholly or in part, for the delivery of an important business service. Supporting this principle, and in line with the Bank's commitments in its response to the 'Future of Finance Report' earlier this year, a dedicated PRA Consultation Paper on 'Outsourcing and third party risk management' (included in the package of consultation papers) modernises and strengthens the regulatory framework for the management of outsourcing and third party risk, including in respect of data security. The FCA Operational Resilience Consultation Paper contains a chapter outlining the importance of outsourcing and other third party service provision to operational resilience and subsequent expectations of firms. In addition, the Authorities are undertaking work to enhance the monitoring of systemic concentrations in the provision of third party services to firms and FMIs (enabled by new regulatory data). HM Treasury now has the power to specify service providers to recognised payment systems, which can bring service providers under the Bank's direct supervision, and it has already exercised this power for one service provider. Regarding new technology the Authorities are also engaged significantly in work to improve our understanding of the use of artificial intelligence and machine learning in financial services, which will help us develop further policy in the future and address the TSC's recommendations in this area.

4. **Co-operation between the Authorities and industry:** we fully agree that the approach to operational resilience should be co-ordinated across the Authorities. That is evident in the joint consultation papers and the response. We are working closely together to ensure a consistent approach to operational resilience and our intended outcomes are aligned. This positive working relationship will continue into the implementation phase of our final policy and the ongoing supervision of firms and FMIs. When incidents occur, we have a longstanding coordinated approach through the Authorities Response Framework. The financial services industry has an established collaborative approach to incident management, which is regularly tested through sector-wide simulation exercises. We also agree that collaboration between the Authorities and industry will lead to better outcomes and stronger industry wide operational resilience, and we are therefore working with industry to develop new capabilities, for example, through the

work of the Cross Market Operational Resilience Group (CMORG) to advance the development of collective solutions to support system recovery in the event of a severe operational incident.

In relation to your recommendation on **providing an account of the TSB IT failure**, we are not able to give any public commentary at this stage because enforcement investigations are ongoing. However we would like to reassure the Committee that the Authorities have a suite of supervisory and enforcement tools for holding firms, FMIs and individuals, where relevant, to account for operational resilience failures.

We have also reflected carefully on the Committee's recommendation to increase **financial sector levies**. We have and continue to build technical expertise within the Authorities and we are upskilling our supervisors via training programmes. We are also using external expertise where appropriate, for example via reviews by skilled persons. At this stage it has been possible for the Authorities to increase resources on operational resilience without a special levy, and we are mindful of the need to use our resources effectively and to balance costs to supervised firms against the benefits of meeting our objectives. We will keep the possibility of raising the levy in the future under review.

We have provided a more detailed response to all of your recommendations in the Annex to this letter. We note that the package of consultation papers published on 5 December and our ongoing supervisory work is very much consistent with your report and recommendations, and we look forward to continuing to discuss these important issues with the Committee.

Andrew Bailey

Chief Executive, Financial Conduct Authority

Jon Cunliffe

Deputy Governor, Financial Stability, Bank of England

Sam Woods

Deputy Governor, Prudential Regulation and Chief Executive, Prudential Regulation Authority

Annex to Appendix 1: Annex to the Regulators Response: Detailed response to the TSC report on IT failures in the financial services sector[1]

Supervisory approach and tools

Operational resilience policy development

The Committee asked the Authorities to set out guidance on the expectations of the definition of business services and impact tolerance and to ensure that firms and Financial Market Infrastructures (FMIs) set impact tolerances at the correct level (12). They also asked the Authorities to provide guidance on how the policy proposals interact with other operational resilience policies (8) and in what situations firms and FMIs would not have to remain within their impact tolerances. (13)

The new policy framework proposes new expectations on firms and FMIs. Our approach to improving operational resilience is that policy should drive change where it is needed by prioritising the things that matter, setting clear standards for operational resilience and investing to build resilience. The policy proposals aim to achieve this by building the approach into formal policies for each supervisory authority. Under the policy, firms and FMIs would be required to identify their important business services. These new expectations are to be determined with reference to the potential impact that disruption to these services would have on: (i) harm to consumers or market participants; (ii) harm to market integrity; (iii) the threat to policyholder protection; (iv) safety and soundness; or (v) financial stability. Firms and FMIs will be required to set impact tolerances for each of their important business services, which are clear metrics specifying the maximum tolerable level of disruption to these services, including in severe (or in the case of FMI's extreme)[2] but plausible scenarios. (12)

The 'severe/extreme but plausible scenario' benchmark for being able to remain within impact tolerances has been proposed in order to drive investment in operational resilience. The Authorities acknowledge in their Consultation Papers (CPs) that a firm or FMI may not be able to remain within its impact tolerance. For example, in the PRA CP it gives the example of a widespread (national) outage of essential infrastructure such as power, transport or telecommunications. However, in such circumstances we would expect firms and FMIs to have adequate business continuity and disaster recovery plans in place. In respect of FMIs, whilst we would seek to take a proportionate approach to such scenarios, the internationally-agreed Principles for Financial Market Infrastructure state that an FMI should aim to be able to resume operations within two hours following disruptive events. The relevant EU regulations go further in requiring central counterparties (CCPs) and central securities depositories (CSDs) to be able to be able to achieve a two-hour

1 For ease of review the numbers in brackets relate to the TSC recommendations.

2 The consultations for FMIs use the terminology extreme but plausible to keep terminology consistent with international standards for FMIs.

recovery time objective for their critical services or operations.[3] CCPs and authorised CSDs should already be in a position to meet this requirement in extreme but plausible circumstances. In the event of such an incident crystallising for firms or FMIs and if necessary, the Authorities' Response Framework would be invoked to support financial stability and protect consumers. (13)

The Authorities' CPs also set out information on existing policies such as business continuity planning in the light of the proposed new operational resilience rules and expectations. (8)

We share the Committee's concerns that firms and FMIs must not set impact tolerances too high. The CPs explain the factors firms and FMIs should consider in setting impact tolerances and illustrative examples are also provided. As part of our future supervisory processes, we will challenge firms and FMIs, including if they did not identify important business services appropriately and if we judged their impact tolerances to be set inappropriately. Subject to the policy being in place supervisors would also be able to undertake supervisory action where firms or FMIs have not adequately met the requirements or expectations set out in the proposed policy. (12)

Supporting this, as part of its macroprudential work, the Financial Policy Committee (FPC) is looking at establishing its impact tolerance which describes how quickly critical financial services companies must be able to restore vital financial services following a severe but plausible cyber incident.[4] Consistent with the FPC's remit, these would be calibrated to ensure financial stability and avoid material economic harm. As set out in the June 2018 Financial Stability Report (FSR), the Bank will test whether firms would be able to meet the FPC's standards for recovering services in severe but plausible scenarios.[5] (12)

Operational resilience policy implementation

The Committee asked the Authorities to reflect on whether the current approach to supervision needed to evolve, namely whether operational resilience would need to be supervised in a different way to prudential or conduct risks and whether it could adapt as technology changed. (7)

The operational resilience polices in our consultation papers are drafted in such a way that enables the proposed policy to adapt as risks to operational resilience change, for example a rapidly evolving technological landscape. The policy proposals are consistent with the Authorities' judgement-based approach to supervision. The Authorities are already developing additional tools to support supervisors on the proposed policy and we will continue to review our supervisory approaches and resources. (7)

The Committee encouraged the Authorities to continue to engage with industry as the policy is developed (8) and to set out timings for the CP. (10)

3 European Market Infrastructure Regulation (EMIR) for CCPs and Central Securities Depositories Regulation (CSDR) for CSDs.

4 See June 2018 Financial Stability Report.

5 www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2018/june-2018.pdf?la=en&hash=9D057C7302B80EF57D634020F50C6F46D782904C and https://www.bankofengland.co.uk/-/media/boe/files/record/2018/financial-policy-Committee-meeting-june-2018.pdf?la=en&hash=18E86971BBB62E98ABF5E5939FDC6B8874D093D3

We have engaged with the finance industry throughout the development of the policy. Industry feedback on the Discussion Paper was very positive. During the consultation period the Authorities will seek further feedback from industry on the proposals, through industry roundtables, supervisory engagement and written responses. We will explain how feedback to the CP has been taken into account and publish this alongside the final operational resilience policy. (8)

The consultation closes on 3 April 2020. Subject to the outcome of the consultation, the Authorities currently expect to publish final policy during the second half of the year, with requirements coming into force 12 months later (for firms and FMIs subject to requirements). (10)

Assessing operational resilience policy effectiveness

The Committee asked the Authorities to set out publically how the effectiveness of the future policy will be measured. (9)

We recognise the importance of evaluating the impact of our operational resilience policy, although we do not have a 'one size fits all' approach to evaluating the impact of our interventions. There are challenges to ensuring that enough time has passed since the intervention to allow any remedies to have been implemented and identifiable changes in behaviour to take effect, but, not so long to have passed that things have moved on too much. (9)

In the first instance, the Authorities expect to measure effectiveness through routine supervisory work, which will be proportionate to the specific firm. For example, supervisors could review operational resilience strategies adopted by boards and senior management or new investments in updating legacy technology. They may also look for evidence of changes in governance aimed at supporting more effective management of operational resilience. Or they may look at work in progress to map and test important business services. Supervisors could also assess the quality of firms and FMIs' implementation of the policy, for example by assessing: which business services they have identified as important; the level they have set their impact tolerances; and the actions they have taken to be able to remain within those tolerances. (9)

Under the proposals firms and FMIs would need to make their operational resilience framework available to the Authorities on request. In addition, the PRA will consider regulatory reporting requirements for operational resilience. (9) (See paragraph 45)

Current approach to operational resilience supervision

The Committee made specific recommendations to Authorities on increasing supervisory capability, particularly at a senior level, and increasing supervisory resources/budgets. (22, 23)

The Authorities keep supervisory resources under review to ensure that we have the appropriate level and skills. The Authorities' current approach draws on existing supervisory expertise, supported by specialist technical support. At this stage it has been possible for the Authorities to increase resource on operational resilience without a special levy. The Authorities need to manage effective use our resources and balancing costs to

supervised firms with benefits of meeting our objectives. The Authorities expect this is an area for further investment and will keep the possibility of raising the levy under review. (23)

For front-line supervisors, providing challenge, looking for assurance and requiring firms and FMIs to take action are already core supervisory skills and form part of the core supervisory training. Furthermore, supervisors already focus on ensuring that firms and FMIs have robust governance and risk management procedures in place. (22)

The Authorities are investing in providing new tools and training to allow front-line Supervisors to increase their ability to assess operational resilience. As set out in our initial response to the Committee, the Authorities have technical experts in operational resilience, many of whom are drawn from industry, who provide senior input, support supervisors and share expertise. The Authorities commit resources to training these individuals and maintaining their technical expertise. (22)

As noted in the section below on supervisory tools the Authorities also have a statutory power to require or commission independent skilled person or expert reviews where considered necessary. This is an important way to access senior specialist technical support if needed by supervision. (22)

Assessing IT change management and legacy systems

The Committee was particularly interested in how firms manage IT change and legacy systems and how the Authorities supervise these. The Committee made several recommendations on reviewing the supervisory approach to these issues and disseminating best practice. (25, 26, 29, 30)

Our current supervisory practice for IT change, including to legacy systems, is that firms and FMIs must notify the Authorities when they are going through material change (for example, whether upgrading their critical infrastructure would impact critical functions or whether they are outsourcing some or all infrastructure supporting critical or important operational functions). The Authorities have an established approach to assessing change and its execution, which can use both supervisors and IT specialists. There is a link to the senior managers' regime, where currently applicable, whereby firms are expected to ensure that there is an accountable executive for change programmes. Where things do go wrong, the authorities can act through focused supervisory work. (26)

The Bank has set out in detail how it expects to supervise significant IT transformation in systemic payments systems and the outcomes it seeks. The Bank expects FMIs to consider the outcomes at all stages of the development process from design through to delivery and it will assess the infrastructure projects at key decision points, such as: when the design principles are agreed; the procurement strategy is approved; and the building and testing plan is developed.[6]

All authorities have future work planned in relation to change management and will consider what more can be done in this space. The FCA is carrying out a focused review

6 Please see https://www.bankofengland.co.uk/-/media/boe/files/annual-report/2019/supervision-of-financial-market-infrastructures-annual-report-2019.pdf?la=en&hash=6DB9A3FEC02109153BA400F07072DB6D3F2D0151 and https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-journey-to-best-in-class-payments-speech-by-david-bailey.pdf

with a selection of firms to understand better their current approaches to IT change management and what lessons can be learnt. The Bank intends to undertake a thematic review of IT Change Management in a sample of FMIs in 2020. The review scope is proposed mainly to focus on routine IT changes rather than wholesale upgrades. What constitutes best practice is different for different firms, but the FCA and PRA will consider how to integrate our expectations into firms' practices (eg working with industry co-ordination groups, publishing a report detailing the findings, or via a Dear CEO letter). (29, 30)

In light of the Committee's recommendations and given the ongoing work, the Authorities will consider whether there is more that could be done around the supervision of IT change management and clarifying expectations on firms and FMIs. On legacy systems the operational resilience CPs propose that firms identify where they should focus investment to become more operationally resilient and the CPs make clear this includes considering the risks around legacy systems. (25)

Scope of current supervisory work

The Committee asked for information on how risks from other areas of the financial services sector (outside of banking and payments) are being identified and mitigated. (42) The Committee also commented that the Authorities should ensure firms are focussed on recruiting the right skills and experience for their boards and senior management in relation to operational resilience. (45)

At present, the insights the Authorities gain from proactive and reactive supervisory work help to understand the risks in regulated firms and FMIs across different sectors. (42)

Two good examples across the financial sector are: 1) The FCA shares incident trends with firms at Cyber Coordination Groups to encourage discussion about cause and mitigation. The FCA also share information between regulators and other authorities, including the National Cyber Security Centre (NCSC). 2) In November 2019, the FCA and PRA published the cyber self-assessment questionnaire (CQUEST) on their websites, which allows firms of all sizes and types to self-assess their maturity in a range of cyber capabilities, including their ability to respond and recover from incidents. (42)

The future operational resilience framework is intended to cover a wide range of regulated firms and FMIs and the Authorities encourage all firms to consider how the proposed concepts in the CPs may help to improve their operational resilience. (42).

Supervisors already focus on ensuring that firms from all sectors have robust governance and risk management procedures in place, as existing governance rules require firms' boards to have an appropriate level of collective and individual expertise and appropriate diversity, including of professional experience. Existing FCA and PRA governance rules require firms' boards to have an appropriate level of collective and individual expertise and appropriate diversity, including of professional experience. The CPs propose that management bodies need to have sufficient knowledge, skills and experience to meet their operational resilience responsibilities. Where the Senior Managers and Certification Regime (SM&CR) regime applies, the CPs proposals seek to clarify the interaction between Senior Management Function (SMF) 24 and our operational resilience proposals. (45)

Tools and enforcement

The Committee was keen to see the Authorities use the tools at their disposal, such as remuneration and SM&CR, and ensure that in cases of non-compliance Authorities were able to use enforcement powers. (15, 16, 17, 18, 19, 55).

The Authorities actively use a variety of supervisory and enforcement tools in order to hold firms, FMIs and individuals accountable and have set out below how these tools are being used for the supervision of operational resilience, including consideration of the proposed new policy. The tools have and will continue to evolve.

Reviews by skilled persons and information-gathering powers

The Authorities have statutory powers under Sections 166 of the Financial Services and Markets Act 2000 (FSMA) and Section 195 of the Banking Act 2009, to commission reviews by independent experts (known as skilled persons) to review predetermined areas or activities in firms and FMIs to diagnose, monitor, prevent and/or remediate risks.[7] The Authorities use this tool frequently, including on IT infrastructure. (26)

The Authorities also have extensive information-gathering powers. For instance, Section 165A of FSMA (known as 'the financial stability information power') empowers the PRA to require a wide range of persons, including service providers to firms to provide information that the PRA consider is or might be "relevant to the stability of one or more aspects of the UK financial system.[8]

The Senior Managers and Certification Regime (SM&CR)

The Senior Managers and Certification Regime (SM&CR) seeks to strengthen individual accountability and corporate governance in firms. The SM&CR has been in force for banks since 7 March 2016; for insurers since 10 December 2018 and for FCA solo-regulated firms since 10 December 2019. (16) The SM&CR regime is primarily used as a supervisory tool, the PRA and FCA can take enforcement action in relation to breaches under SM&CR rules. Under the SM&CR firms should clearly allocate responsibility for "material change management or transformation projects, including but not limited to a significant overhaul of a firm's IT systems" to one or more senior individuals approved by the PRA and/or FCA to perform a Senior Management Function (SMF).[9] A clear allocation of responsibilities can facilitate independent oversight and challenge by firms' boards and gives the Authorities a clear, senior executive to hold accountable for relevant projects. More generally the regime can have a preventative effect by ensuring the SMF focuses on the PRA and/or FCA's operational resilience objectives, including advocating for investment decisions. (16)

7 See PRA Supervisory Statement (SS)7/14, 'Reports by skilled persons' https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2015/ss714-update.pdf?la=en&hash=B6CF68E69A14E9CC68BE45A6DD23EFBFBFD289D0

8 See PRA Statement of policy 'The financial stability information power' June 2014, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/statement-of-policy/2014/the-financial-stability-information-power-sop

9 See SS28/15 'Strengthening individual accountability in banking' https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2018/ss2815update.pdf?la=en&hash=39EC46AE5FD217724BB307C420B80A4E09F42A24

The Bank does not currently have SM&CR or remuneration powers for FMIs. Extending these to FMIs would require primary legislation and is therefore ultimately a decision for HM Government. However, as the Financial Policy Committee (FPC) noted in the July 2019 Financial Stability Report (FSR) "FMIs' governance arrangements and risk culture should reflect fully the vital services they provide to the financial system and the economy". Therefore, "there is a strong case for extending the SM&CR to FMIs. This would help the Bank to ensure that individuals in key positions of influence within FMIs have suitable skills, experience and understanding of the systemic importance of FMIs." (19)

Enforcement (15)

The Authorities have a range of enforcement tools, in addition to the supervisory tools above, which they can and will use where warranted, including in response to operational outages. As a previous example, in May 2019 the PRA and FCA fined Raphaels Bank for inadequate systems and controls supporting the oversight and governance of its outsourcing arrangements following the failure of the authorisation and processing services at Raphaels' outsourced card processor, which lasted over eight hours.

The current pipeline of enforcement investigations includes examples falling broadly under the banner of operational resilience, with both firms and senior individuals being held to account for their actions. As at end November 2019, the FCA and PRA have 4 open enforcement cases linked to operational resilience failings.[10] The Bank has also undertaken supervisory action (which does not constitute enforcement action) with regards to outage incidents in payment systems, using its statutory powers under Part 5 of the Banking Act 2009.

The Committee asked the PRA and FCA to provide their report on the TSB IT failure or set out the timelines to do so. As these enforcement investigations are ongoing, the Authorities are presently unable to give any public commentary on this case. (17)

Remuneration requirements

PRA and FCA regulated firms are subject to regulatory requirements relating to the variable remuneration of (in particular) top executives and material risk-takers. These requirements seek to promote internal accountability and align performance, risk and reward. The PRA and FCA require that performance metrics used to set variable pay have an adequate balance of financial and non-financial criteria and include adjustments for all types of current and future risks, which include operational risk. The PRA and FCA also require that variable remuneration can only be paid, or vest, where justified on the basis of the performance of the firm, the business unit and the individual concerned. The PRA has set out its expectations that a material failure of risk management should lead to a downward adjustment in variable remuneration. Over the last year, the PRA and FCA have written to firms explaining that core risks, identified as supervisory priorities, are to be reflected in the pay awards of Senior Managers designated to manage those risks, and supervisors monitor this.[11] (18)

10 The PRA's approach to enforcement – speech by Miles Bake, 16 July 2019 https://www.bankofengland.co.uk/-/media/boe/files/speech/2019/the-pras-approach-to-enforcement-speech-by-miles-bake.pdf?la=en&hash=DB4A4DCFF019C37C7D60AF063135A4E5D7D53A34

11 From a shared (PRA/FCA) letter to RemCo Chairs. See also Sam Woods speech: https://www.bankofengland.co.uk/-/media/boe/files/speech/2019/the-pras-approach-to-enforcement-speech-by-miles-bake.pdf?la=en&hash=DB4A4DCFF019C37C7D60AF063135A4E5D7D53A34

Incident reporting and management

Incident reporting

The Committee requested the Authorities assess the accuracy and consistency of incident reporting data, clarify standards guidance and definitions for industry and consider the need to expand current reporting requirements. (5) The Committee recommended more prominent public reporting on incidents. (6)

FCA regulated firms have existing incident reporting requirements[12] and the FCA will continue to remind firms of their existing obligations to report material incidents. In addition, the FCA is the competent authority for payment firms reporting incidents under the Payments Systems Directive 2 (PSD2) thresholds. Where firms do not meet these requirements, the FCA will take action where necessary. (5)

Currently the PRA asks firms to disclose to the PRA anything relating to the firm of which the PRA would reasonably expect notice, which includes incidents.[13] (5)

The Principles for Financial Market Infrastructure (PFMIs), which underpin the Bank's supervisory approach to FMIs state that 'an FMI should have a plan in place for communication with regulators, services providers, and where relevant, the media. The Bank, under Part 5 of the Banking Act 2009, requires incident reporting by recognised payments system operators on a 'best endeavours basis'. (5)

The Authorities also have a number of pieces of work underway at both cross-regulator and cross-industry levels that will help to address the Committee's recommendation. The PRA plans to consider the regulatory reporting requirements for operational resilience, including whether new quantitative information should be submitted by firms and what information should be submitted when operational incidents occur. This work would take in to account existing reporting requirements, including those for dual-regulated firms. (5)

There is already a considerable amount of information available to consumers about the operational resilience of banks. Since 2018, banks are required to publish the number of major operational and security incidents they experience.[14] Banks publish information about operational and security incidents on their websites and on the FCA website[15] including complaints data, FAQs and data detailing the total number of incidents, and incidents impacting telephone banking, mobile banking and internet banking. Additional requirements apply to large retail banks, which must provide a service status web page, so customers can gather updates on impacted services during a live incident or planned maintenance outage.[16] (6)

Incident management and communication during an incident

The Committee made a number of recommendations relating to incident management. The Committee wanted the Authorities to take action in incidents (14) and assess

12 Under Principle 11 and Sup 15.3 (of the Handbook?)
13 PRA fundamental rules
14 https://www.fca.org.uk/data/mandated-voluntary-information-current-account-services
15 https://www.fca.org.uk/data/mandated-voluntary-information-current-account-services/interpreting-data
16 FCA BCOBS 7

firms' incident management response and exercising (51). They also stated that firms should ensure customer communication is clear and timely (52), that the Authorities should also consider a centralised portal with incident information (54) and that the Authorities should approve information not being shared (53). The Committee asked for reports to be shared with industry promptly after exercises. (50) The Committee recommended that the FCA ensures firms are resolving complaints and awarding compensation quickly, taking action where this is not the case. (55)

The Authorities have tools in place to ensure that firms and FMIs are prepared for incidents, that the Authorities are able to co-ordinate and take action, and that communication and information is managed. This includes work that the Authorities do jointly with industry and internationally with partners such as the G7 nations.

Ultimately firms and FMIs are responsible for managing their incidents and the Authorities expect firms and FMIs to implement effective recovery plans and deploy customer communications strategies in the event of an incident. This is supported by the Authorities' supervisory approach, which includes a focus on incident management and planning, for example by assessing firms' business continuity plans. There is also training for supervisors on their role during an incident. (51)

The new operational resilience CPs propose that firms and FMIs develop communications plans for use when important business services are disrupted, featuring prompt and meaningful communication arrangements for internal and external parties, including Authorities, clients and the media and that these would be supervised against. The Authorities think it is important to share information with consumers during an incident, not least so that consumers can potentially mitigate the impact themselves (eg by using another channel). (51, 52)

Alongside the supervisory work there is an established sector exercising programme, run in partnership with the finance sector. This provides an environment for incident responders to gain experience of the response framework and pressured decision-making as well as identifying vulnerabilities associated with realistic scenarios. (50)

Reports following exercises have and will continue to be shared with exercise participants and, where possible without increasing risks, will be shared publically. Lessons learnt and any industry capability developed, including best practice, are shared across the industry. For example, the Bank recently published a SIMEX report setting out the key findings and recommendations of the 2018 exercise, which ran a scenario of a prolonged and broad cyber attack and included 29 of the most systemically important firms and FMIs plus the Authorities. (50)

The Authorities manage and coordinate their response to major incidents through the Authorities' Response Framework (ARF), which is exercised throughout the year. The framework has also been tested in an international context and is supported by specific protocols that manage and support collective communications as well as identified contingency plan capabilities. (14)

Co-ordinated communication between the Authorities and industry is delivered through the Cross Market Business Continuity Group (CMBCG) call. The ARF and the CMBCG ensure that communications are joined up and that the regulators are aware if industry

decided to limit communications (for example if communication could reveal potential IT vulnerabilities). In addition, communications form a core part of regular rehearsal and testing. (14, 53, 54)

The Authorities agree with the Committee that firms must act swiftly and fairly in responding to complaints and awarding redress in the event of an IT incident. The FCA has clear complaint handling rules for firms that require them to resolve complaints fairly, consistently and promptly.[17] The FCA rules also make clear that if a final response cannot be provided within set timescales, for reasons beyond the control of the firm, the firm must explain clearly the reason for the delay to the customer and keep them informed of progress. (55)

FCA rules require firms to appoint an individual who has responsibility for oversight of the firm's compliance with complaints handling and redress. In addition, where a firm has received a large number of complaints which detail the same issues, it has a responsibility to put in place appropriate management controls and take reasonable steps to ensure that, in handling the complaints, it identifies and remedies any recurring problems. This should include the scope and severity of the consumer detriment that might have arisen and considerations of whether it is fair and reasonable for the firm proactively to undertake a redress or remediation exercise. (55)

In the event of an IT incident the FCA monitors how a firm is dealing with customer complaints and how they are communicating with customers. The intervention and the actions the FCA take around a serious IT incident, including enforcement action, are considered on a case by case basis. (55)

In addition to the rules set out above, the FCA are supportive of UK Finance's work with industry to develop compensation and redress principles for instances when customers suffer harm as a result of operational disruption.

Third parties and new technology

Third parties

The Committee raised a number of recommendations and comments on how Authorities should map dependencies on third parties (33), ensure the industry manage and mitigate third party dependencies (31) and consider how to mitigate concentration risk with systemic providers. (34, 35, 36)

The Committee also referred to the planned payments review by Government to ensure that regulation keeps pace with innovation. The Bank and FCA are fully engaged in HM Treasury's (HMT's) payments review (previously referred to as the National Payments Strategy) in order to maintain UK leadership, and unite innovators, businesses, policymakers and infrastructure providers, in the context of the review. The Bank of England's Financial Policy Committee (FPC) has agreed a set of principles to guide its assessment of how regulation should adjust to innovation in payments activities. These include the principle that regulation should ensure 'end-to-end' operational and financial resilience across payment chains that are critical to the smooth functioning of the economy. (41)

17 FCA DISP Rules

Individual firm level

Since the Committee's report, which asked the Authorities to review existing rules and guidance on third party management, the Authorities have published the Operational Resilience CPs and the PRA CP on 'Outsourcing and Third Party Risk management' ('Outsourcing CP). Together, these aim to improve regulatory certainty by clarifying how firms should identify and manage outsourcing and third party risks. (31)

These CPs build on the current established regulatory framework governing firms' and FMIs' outsourcing arrangements. A key overarching principle of this framework is that firms and FMIs cannot outsource their accountability and are responsible for identifying and managing the risks (in particular operational risks) associated with the use of third parties that they rely on to deliver their business services. This is underscored in the Operational Resilience CPs, which state that a firm's or FMI's operational resilience should not be undermined when it relies on a third party, wholly or in part, for the delivery of an important business service. (31)

While the modernised policy framework set out in the Outsourcing CP is proposed to apply to all forms of outsourcing and, in some areas, other relationships between dual regulated banks and insurers and third parties, certain sections set out proposals to address specific issues relating to these firms' increasing reliance on cloud service providers.

This CP publication delivers on one of the Bank's priorities in its response to the 'Future of Finance Report' to "publish a supervisory statement in 2019, describing the PRA's modernised policy framework on outsourcing arrangements, including a focus on cloud technology and setting out conditions that can help give firms assurance on its use". For instance, there is a chapter on data security that sets out the PRA's expectations on how firms should protect confidential or sensitive data they place on the cloud. There is another chapter dedicated to business continuity planning and exit strategies, which seeks to mitigate some of the risks associated with the concentration in the provision of cloud services, such as vendor lock-in and a lack of substitutability. The chapter underlines the importance of firms having documented and tested business continuity plans and exit strategies so that they can respond effectively to potential failures or outages at material service providers. The FCA also published guidance in 2016 on how firms should manage their Cloud outsourcing arrangements and has included a chapter on Outsourcing in the FCA consultation paper. (35, 36)

The Outsourcing CP also considers the possibility, mentioned by the Committee, of firms carrying out joint inspections of service providers, including cloud service providers (referred to as 'pooled audits') as a means of getting assurance on the effectiveness of their control environment, disseminating best practices and reducing the costs and disruption of individual inspections. (36)

With regard to FMIs, it is not uncommon for the payment scheme companies that manage a number of the recognised payment systems to outsource day-to-day functions and the development of hardware and software facilities to one or more technical infrastructure providers. The PFMIs cover such outsourcing risks, and the Bank reviews the integrity of such outsourcing arrangements. In addition, the Bank has started to supervise directly a

specified service provider to recognised payment systems. Furthermore, the relevant EU regulations applicable to CCPs and CSDs already require the relevant FMIs to remain fully responsible for meeting all requirements for outsourced services and activities. (31)

System-wide level

At a system-wide level, the Authorities are aware that systemic concentration in the provision of certain third party services, such as Cloud, could have implications on financial stability. As part of its statutory remit, the FPC monitors this risk and can make recommendations should it take the view that there are systemic risks to the UK financial system that should be addressed.

The FPC has an established process to assess risk beyond the banking sector. It receives regular briefings from the Bank, the PRA and the FCA on potential risks to financial stability presented by different sectors and activities, and on resilience of market-based finance. It also holds annually a dedicated discussion on these risks and regulation beyond the core banking sector. On that basis, the FPC decides whether to commence or continue close monitoring of certain activities or sectors—particularly where evolving or growing rapidly (such as Exchange Traded Funds, 'fast markets', financial technology or the provision of cloud services to the financial sector), or to launch an in- depth assessment (such as into non-bank leverage or risks from open-ended investment funds). The FPC draws on this analysis to inform its judgement on the appropriate boundaries around, and within, the regulatory perimeter. (34) (40)

The Committee asked how the Authorities could identify common critical third parties and interdependencies (including supply chains) in the absence of a 'sector map'. (33)

The Authorities have been working to understand better the interdependencies in the finance sector. Data collection is a key challenge and at the moment we have some targeted pieces of data/work that will support that understanding. This work is set out in the following paragraphs. (33)

The Operational Resilience CPs propose that firms and FMIs map their important business services and this information will be available to the Authorities. This means firms and FMIs need to develop a deeper understanding of their supply chains and the operational resilience of their critical third party providers and how they relate to important business services. As the Authorities engage with the data and conduct supervisory peer reviews, we will be better placed to identify concentration risks and to consider action where necessary. (33)

Moreover, in line with the recently published 'EBA Guidelines on Outsourcing Arrangements', the Outsourcing CP proposes to ask PRA-regulated firms to maintain an up-to-date register of all their outsourcing arrangements from 31 December 2021. Banks already have to maintain a register of their Cloud arrangements. (33)

New technology developments

The Committee asked whether the Authorities have the skills to deal with new technology (37); how they were assessing firms' reliance on new technologies; and recommended that the Authorities issue guidance in this area, particularly in relation to the risk of discriminatory artificial intelligence (AI). (38).

The Authorities confirm that requirements placed on firms are technology-neutral (ie firms need to meet regulatory requirements regardless of what technology they use). The Authorities believe that new technology can enable firms to enhance their operational resilience, but can also bring risks. The Authorities want to ensure that firms can harness that benefit (and others) without compromising resilience, and have a number of coordinated initiatives to better understand, monitor and promote the safe adoption of new technologies. (37)

In October 2019, the Bank and the FCA published a joint report on AI & machine learning. The report was based on the survey responses of over 100 firms, which provided insight into how advanced the industry is in using this technology and what controls firms had in place. Following the report the BoE and the FCA have announced plans to establish a public-private group to gather insight from the sector. In particular, the panel will consider whether principles, guidance or other regulatory support could help safe adoption of these technologies. This will help the Authorities to explore potential policy areas relating to machine learning in the future. The Authorities have spoken publicly of their continued work in this area and shared their thoughts on the evolving use of technology, including ethical issues such as fairness and the potential for discrimination.[18] (38)

As an example of an area where the Authorities have already set expectations on technology, the PRA published a supervisory statement in 2018 setting out expectations of a firm's risk management and governance on algorithmic trading. This covered a number of areas including the role of the firm's Board and links to the senior managers regime, what risk controls should be in place, and how testing should be carried out prior to deployment.

It is for firms to first assess the benefits and risks relating to their use of new technologies and reach informed decisions. The Authorities assess how firms manage relevant risks and may further update their requirements and expectations if appropriate. (38)

Co-operation between the Authorities and industry

Regulator co-ordination

The Committee recommended that Authorities should take a coordinated approach to the requirements they place on firms, to avoid inadvertently increasing the risk of incidents as a result of change. (20)

The Authorities have developed strong collaboration with regards to operational resilience, including during policy development and incident management. The joint Discussion Paper on and subsequent CPs on Operational Resilience are an example of the former,

18 Please see: https://www.bankofengland.co.uk/speech/2019/james-proudman-speech-at-fca-conference-on-governance-in-banking-london and https://www.fca.org.uk/news/speeches/how-can-we-ensure-big-data-does-not-make- us-prisoners-technology

the ARF is an example of the latter. In particular, the consultative approach to developing policy enables firms and FMIs to highlight where they think there may be unintended consequences of regulatory initiatives. (20)

In July 2019, HMT launched a Call for Evidence on how regulatory co-ordination might be improved. Furthermore, the Bank committed in its response to the 'Future of Finance' report that it will "play a full role in any forum commissioned by the Government, bringing together all relevant Authorities and Government departments to consider any scheduling bottlenecks arising from new projects". In order to advance this, the Bank, PRA and FCA have prepared 'Air Traffic Control' proposals and intend to enact them when HMT is ready to move forward. (21)

Industry collaboration

The Committee asked the Authorities to set out plans to build on existing industry collaboration, adding that the Authorities should intervene if co-ordination is not happening (47, 48)

CMORG is well established as a platform for co-ordinating and promoting work across the finance industry and has a comprehensive workplan. This is developed in partnership between the Authorities and industry, and focuses on areas that benefit from cross-industry collaboration, incorporating particular areas identified from the sector's exercising work. This work aims to enhance the sector's operational resilience by developing new capabilities and by testing existing capabilities and processes.

The recommendations from CMORG's SIMEX exercise (undertaken in 2018) highlighted the following areas, which are currently been taken forward, and includes issues related to data recovery and co-ordination highlighted by the Committee. Projects range from short-term operational interventions to longer-term strategic adjustments. (47, 48)

a. Opportunities to improve the way firms coordinate—a review of the finance sector response framework will be undertaken to ensure that the sector can communicate and co-ordinate at an operational level during an operational crisis. In addition the Finance Sector Cyber Collaboration Centre (FSCCC) will also be integrated into the response framework to ensure the technical coordination capability the FSCCC provides is incorporated into the broader response landscape.

b. Disparity in risk tolerance for suspending services—future work will focus on the production of industry guidelines and good practice for managing potential controlled suspension of services and system integrity risks.

c. Restoring data and recovering service—work will be completed to scope the technical and data requirements for providing services via alternative channels in the event of data corruption or loss. This will be followed by a strategy paper and playbook to support coordination of this contingency during a live incident. (48)

d. Communication practices—to improve consistency and clarity of often complex technical messaging during an operational crisis, future work will focus on best practice for good incident communications practices and consistent definition and use of terminology.

CMORG members include the largest banks and FMIs. As CMORG is co-chaired by UK Finance, outputs from CMORG are shared with its members, who include 250 large and small firms. For smaller firms, the FCA has brought together over 175 firms in sector-specific Cyber Coordination Groups to share information and ideas from their cyber experiences since 2017. The FCA's Cyber Insights document, published in March 2019, collated examples of innovative cyber practices shared by firms and sets out those the FCA considers to be beneficial for a wider audience, particularly small and medium-sized enterprises.[19] (47)

The Committee highlighted cyber as a priority for co-ordination. The CMORG framework encourages interaction on cyber with industry best practice and co-operation. A good example of this is the FSCCC. This focal point for the industry on cyber collaboration was identified as an improvement for the financial services sector during exercising. CMORG in its collective action role then worked with industry and its trade body to build this new capability and improve the resilience of the sector. This is a new initiative and creates a one stop shop for industry on cyber, covering incident management, interaction with Authorities and government, information-sharing and development of best practice. The FSCCC's mission is proactively to identify, analyse, assess and coordinate activities to mitigate systemic risk and strengthen the resilience of the UK financial sector. It will do this through enhanced collaborative activities and focused operations across financial services industry partners and UK and international authorities. (32)

19 https://www.fca.org.uk/publication/research/cyber-security-industry-insights.pdf

Appendix 2: Government Response

IT failures in the financial services sector

Ensuring the operational resilience of the financial services sector and the protection of consumers is a key priority for the Government. Outages can impact individual consumers and pose a risk to financial stability which the government takes very seriously. I would therefore like to thank the Treasury Select Committee for its inquiry and report into IT failures in the financial services sector and welcome the Committee's recommendations for improving operational resilience in the financial services sector.

Responsibility for the UK financial services sector's networks is primarily for the firms themselves, however, government has a crucial role in improving the resilience of the sector to operat ional risk and to respond to signif icant disruption.

We work closely with industry, the Financial Authorities (the Bank.of England, the Prudential Regulation Authority, and the Financial Conduct Authority), intelligence agencies, and law enforcement to achieve this.

We have given the Financial Authorities the powers they need to make changes to regulatory rules to bolster the sector's operational resilience and to act in the event of failures. As you will already be aware, the Financial Authorities recently published a set of consultation papers setting out proposed regulatory changes for improving operational resilience.

The financial service sector also benefits from a dedicated team within the UK's National Cyber Security Centre who work closely with industry to protect firms and provide support during incidents.

The Government has carefully considered the Committee's findings, and I am responding as the minister responsible to each of the recommendations you have put to the government.

Creating and enforcing accountability

Your report notes the importance of holding individuals to account when IT failures happen and recommends the Government expands the Senior Managers Regime to Financial Market Infrastructure supervised by the Bank of Englan.d (Paragraph 66)

The Senior Managers & Certification Regime (SMCR) is aimed at changing behaviours and culture within firms by ensuring individual accountability for misconduct, with enforcement powers acting as a deterrent. The Senior Managers Regime (SMR) itself places a duty on all senior managers to take reasonable steps to prevent misconduct in their areas of responsibility, and holds them accountable for any misconduct that occurs under their watch.

The SMCR currently applies to all firms regulated under the Financial Services and Markets Act (FSMA). It was first implemented for all banks, building societies, credit unions and Prudential Regulation Authority designated firms in 2016. The regime was then extended to cover insurance firms in December 2018, and the majority of Financial Conduct Authority solo regulated firms in December 2019.

We are now considering the case for the creation of new SMRs for firms regulated outside of FSMA that is consistent with that created for FSMA firms. This includes Financial Market Infrastructures. The Government will update on progress in due course.

Regulatory burden and coordination

You welcomed the former Chancellor's announcement in the 2019 Mansion House speech of a review into the future regulatory framework for the financial services sector, and called for the Treasury to implement a continuing coordinating forum to assess the cumulative burden of regulatory change and to facilitate a permanent "air traffic control" in the financial services sector. (Paragraph 75)

The Government ran a Call for Evidence on regulatory coordination between July and October 2019. Views were sought on how HM Treasury and regulators with jurisdiction over the financial services sector work together to coordinate regulatory interventions for financial services firms. HM Treasury is in the process of developing a response to the Call for Evidence, which will be published in due course.

Cloud Service Providers

Your report highlights the potential benefits and risks of cloud service provision in the financial services sector, and recommends that the Government should consider how best to regulate cloud service providers. (Paragraph 136)

The Prudential Regulation Authority in December 2019 released a consultation paper on 'Outsourcing and third party risk management' which proposes changes to the regulatory framework to ensure that a firm' s operational resilience is not undermined by the provision of any third party services. This paper sets out the Prudential Regulation Authority's expectations of firms on issues such as the protection of confidential or sensitive data that is placed on the cloud and business continuity planning and exit strategies for services outsourced to the cloud.

Risks to financial stability from the provision of cloud services is also being considered by the Financial Stability Board (FSB), which in its 2019 report on 'Third-party dependencies in cloud services' concluded that there are no immediate financial stability risks stemming from the use of cloud services by Financial Institutions; as well as the Financial Policy Committee (FPC), which in its meeting on 13 December 2019 agreed to continue to monitor the risks from the provision of cloud services in 2020.

HM Treasury keeps the regulatory framework under review and will continue to take into consideration findings from the FPC and other expert organisations to inform policy and ensure a resilient financial services sector.

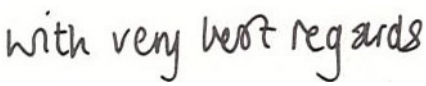
Regulation of new technology firms

In the 2019 Mansion House speech the former Chancellor announced a Treasury led review of the payments landscape. Over recent years there have been significant developments in the UK's payments landscape with innovations in the way that people and businesses make payments. The proliferation of new technologies has resulted in new service providers entering the UK's payments landscape and transforming payment

services available. As such, and as already highlighted in this letter, it is vital that we keep our regulatory approach under review. This will ensure the UK remains a world-leader in payments inn ovations that are safe and reliable.

In your report, you asked the Government to set out the scope and timelines for the review of the payments landscape in the government's response to this report. (Paragraph 153)

HM Treasury have worked closely with regulators and will be publishing a Call for Evidence in the coming months. The review will identify what changes can be made within the current legislative framework, and evidence will feed into HM Treasury's longer-term legislative work. This review will consider the FPC's proposed approach to payments regulation as out lined in the December Financial Stability Report. The review will also consider the wider work being undertaken as part of the Financial Services Future Regulatory Framework Review, and the Treasury-led Cryptoassets Taskforce.



John Glen