BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Rt. Hon. Andrew Tyrie MP
Chairman of the Treasury Committee
House of Commons
Committee Office
14 Tothill Street
London
SW1H 9NB

Andrew Bailey
Deputy Governor, Prudential Regulation
CEO, Prudential Regulation Authority
T 020 7601 4293
andrew.bailey@bankofengland.co.uk

28 October 2015

Dear Andrew,

IT SYSTEMS FAILURES AT RBSG

Thank you for your letter of 28th September following-up on earlier correspondence regarding the IT systems failure at the Royal Bank of Scotland Group (RBSG).

The PRA Board recognises that technology failure represents both a key risk to individual institutions and a potential threat to the overall stability of the financial system. Accordingly, we expect the identification and mitigation of technology risk to form an important part of the sector's broader risk management and operational resilience activities.

What were [the] terms of reference [of the joint review]?

Following the RBSG outage in June 2012, the Financial Services Authority initiated a review which sought to evaluate the extent to which the largest UK retail banks both understand and actively manage their technology risk ("Dear Chairman I" or "DCEI"). The PRA and FCA subsequently decided to undertake a follow-up review during 2014/15 ("DCEII") in order to:

- Identify actions taken by participating firms to improve critical infrastructure and technology resilience since the first review in 2012;
- Evaluate progress achieved by each participating firm since the 2012 review and draw cross-firm comparisons;
- Examine the adequacy of arrangements intended to minimise customer detriment arising from technology failures; and
- Undertake a more detailed evaluation of the various themes in scope for the DCE II exercise, and the measures taken by firms to ensure the continued resilience of retail economic functions.

Relative to the first review in 2012, DCE II was a more detailed and granular assessment of critical infrastructure and technology resilience and was designed to provide supervisors with a better insight into the management of technology risk by their respective firms.

Which banks were included, and on what criteria?

Participants comprised the seven largest UK deposit-takers.

Without identifying any particular bank or vulnerability, can you provide a sense of the nature of the weaknesses identified? In particular, did the review cause the PRA to revise its assessment of the risks of IT failure causing systemic disruption to critical economic functions, including payments systems?

PRA supervisors provided written feedback to each of the participating firms in early October. This feedback (and any resulting remediation) will be followed-up by individual teams as part of our regular supervisory cycle.

We are now drafting cross-firm feedback based on a comparative analysis of the information submitted as part of DCEII. The cross-firm feedback will draw out common themes and, whilst not yet complete, these are likely to emphasise the importance of remedying any weaknesses in:

- Board engagement in operational resilience;
- Understanding how end-to-end processes deliver critical services to the economy ;
- Awareness of the operating environment and ways in which systems can fail;
- Designing technology, processes, systems etc. for operational resilience;
- Taking ownership of third party operational resilience; and
- Providing training for staff on the role and importance of operational resilience.

The findings that have emerged from DCEII have not caused the PRA to revise its current assessment of the likelihood of specific technology failures in individual firms leading to systemic disruption. However, DCE II has enabled us to make progress on mitigation through the actions firms are now completing.

How many actions did the PRA require as a result of the review?

Whilst a number of common themes have been identified, DCEII revealed different strengths and weaknesses across participating firms. Accordingly, the number and nature of actions required will vary considerably across different entities. In some cases, individual firms will be asked to produce stand-alone action plans, whilst others have been asked to ensure that any additional actions generated by DCEII are addressed through existing remediation programmes.

Is the PRA satisfied that individuals responsible for the integrity and resilience of IT systems in each major bank are clearly identifiable under the Senior Managers Regime?

In addition to the Chief Risk Officer, participating firms were asked to identify the senior executive accountable for operational and technology resilience. All participants provided the relevant details as part of their response to DCEII identifying Chief Operating Officers or Chief Information Officers as accountable for operational resilience, including IT resilience. This responsibility is captured within the Senior Managers Regime under the FCA designated Senior Management Function 18 for significant responsibilities.

Yours sincerely,

Andrew Bailey