The House of Commons Treasury Committee has published its Report into IT failures in the financial services sector, following an almost year-long inquiry that began in November 2018. The inquiry was launched in response to a number of high-profile IT failures at banks and other financial institutions that reportedly affected large numbers of customers. The Treasury Committee examined the causes and consequences of IT failures in the financial services sector and what was being done by industry and the FCA, PRA and Bank of England (the "Regulators") to promote operational resilience, in light of the rise of digital banking services.

The Report sets out a number of recommendations for the Regulators, the Government and firms. It will also be of interest to any individuals that fall under the Senior Managers Regime, Fintechs and outsourced technology providers operating in the financial services sector (in particular, providers of cloud services).

The Report's recommendations include the following:

1. **Greater regulatory focus on operational resilience**

As customers increasingly access their financial services through digital channels, the resilience and availability of digital channels is being brought into sharper focus. Whilst the Committee welcomes the moves by the Regulators towards closer supervision of operational risks and resilience, it considered that further regulatory intervention is needed to improve the operational resilience of the financial services sector. The Report says that the Regulators must give as much prominence to regulating operational risk and resilience as they currently give to regulating prudential and conduct risks. Since the Report was published, the Regulators have published a shared policy summary and co-ordinated consultation papers on new requirements to strengthen operational resilience in the financial services sector. The consultation opened on 5 December 2019 and is due to close on 3 April 2020.

2. **Regulatory supervision of operational resilience**

The Report notes that the Regulators' role in operational resilience is still developing and refers to the Regulators' joint Discussion Paper, 'Building the UK financial sector's operational resilience' (which was published in July 2018 for the purpose of obtaining feedback on the Regulators' thinking regarding operational resilience in order to their respective supervisory approaches). In the Report the Committee recommends that the Regulators should publish further guidance for firms on how their different operational resilience requirements interact and how the Regulators expect firms to implement them. The Committee urges the Regulators to prioritise the publication of their final policy and guidance, given the importance of operational resilience and the fast-moving nature of the risks. As noted above, the Regulators opened a consultation on 5 December 2019 on new requirements to strengthen operational resilience.

3. **Greater industry focus on managing and preventing IT incidents**

The inquiry identified that operational incidents in the financial services sector are increasing in frequency. Where incidents that affect customers do occur, the Committee found that the impacts can be significant: customer inconvenience and distress are the main impact but "second order" impacts – such as cyber fraud triggered by an IT incident – may also occur. In addition, IT incidents can reach beyond customer harm and impact the viability and/or financial stability of a firm. The Report states that financial services providers must treat their ability to manage and prevent incidents with a level of seriousness appropriate to the significant impact that can result from such incidents.

4. **Publicly reporting IT incidents**

The Regulators believe that there is overall under-reporting of IT incidents in sectors outside retail banking. The Report calls on the Regulators to undertake an assessment of the consistency and accuracy of IT incident reporting and clarify standards, guidance and definitions for the industry regarding what should be recorded and reported (and, if necessary, expand the current reporting requirements). The Report notes that higher quality incident reporting will serve to improve the ability of both the Regulators and industry to identify the biggest risks to the operational resilience of the sector. In addition, the Committee has stated that the Regulators should consider requiring clearer and more prominent public reporting to empower customers to make informed decisions.
regarding which provider they use and to increase firms' focus on operational resilience. Where firms already publish information about incidents, the Report says that this should be greater prominence in materials given to current and prospective customers.

5. Increased individual accountability – Senior Managers Regime

The Report stresses that individual as well as firm-wide accountability for IT failures is essential to prevent mistakes being repeated and to focus senior management on IT risk and incident management. The Report notes that the Committee was not aware of any successful enforcement case against an individual under the Senior Manager Regime following an IT failure. The Report expresses the Committee's concern that this indicates an ineffective regime. The Committee urges the Regulators to consider whether there are any barriers to effective operation of the regime. The Report warns that if future incidents occur with no individual sanctions, the Committee and Parliament may need to consider whether the Regulators' powers are fit for purpose. To help improve the prominence of operational resilience, and the level of attention being devoted to IT failures, the Committee recommends that remuneration structures throughout firms should reflect the importance of operational resilience. In addition, the Committee recommends that, because of the impact that IT outages at Financial Market Infrastructure firms ("FIMs") can have on customers, the Government brings senior management at FIMs within the Senior Managers Regime.

6. Upgrading legacy IT systems to reduce risks

The Committee does not consider that firms are doing enough to mitigate the operational risks of their own legacy technology systems, such as moving to new technology. The Committee was concerned about cost-cutting in the level of investment in technology, following the financial crisis. The Report states that this is not an acceptable position "given the profits generated by the financial services sector". The Report concludes that firms must not use cost or difficulty as excuses not to upgrade legacy systems. Whilst the Committee acknowledges that the Regulators' have proposed an approach for improving firms' management of legacy systems, it recommends that Regulators should intervene, if improvements in this regard are not forthcoming, to ensure that customers are not exposed to risks due to legacy IT systems. The Committee recommends that Regulators use their powers to appoint independent skilled persons to achieve this.

7. Poor IT change management and the importance of testing

The Report highlights the risks posed by implementing new technology and gives examples of where high-profile IT incidents have resulted from poor change management. The Committee is concerned that time and cost pressures cause firms to cut corners when implementing change and in particular refers to shortened testing programmes. It urges firms to identify and address any issues in their change management procedures, including having sufficient skills and experience to manage change. The Reports states that firms should not gamble with their service availability when implementing change programmes. The Committee is seeking a greater role from the Regulators in this regard, including proactive intervention to protect customers.

8. Managing risks of outsourcing and third-party failure

The Report states that failures of third parties cannot be used as an excuse when IT incidents occur. It recommends that Regulators amend their rules and guidance if regulated firms are not managing their service providers to a good standard.

9. Managing concentration risk and regulating cloud service providers

The Report states that the Committee found many cases where financial services sector firms are using the same third-party providers, which can create concentration risk. It identifies the increasing use of cloud services as an example. Whilst the Report highlights both the benefits of using cloud services (cost savings, faster deployment cycles, greater cyber resilience, physical robustness and stability) and also the risks (data sensitivity, cross-border infrastructure, market concentration, ease of exiting, real choice of contractual terms), the Committee's conclusion is that the use of cloud service providers is already a concentration risk and that a major operational incident at one of the large providers could have significant consequences on the financial services sector. The Committee also concludes that there is an overwhelming case to regulate cloud service providers and recommends that the Government urgently considers how best to do this.

10. Managing risks of new technologies; AI

Whilst the Committee acknowledges that the use of new technology and innovation in the financial services sector presents opportunities and can facilitate improved operational resilience, new technologies can also pose risks (the Report refers to bias in AI, lack of transparency in ‘black box’ AI systems, and data security as examples). The Committee recommends that the Regulators assess whether firms are rolling out new technologies before they have proven their resilience. It also calls on firms and the Regulators to monitor the potential of new technologies
like AI and machine learning to be discriminatory and it urges the Regulators to set clear guidance for the sector.

11. **Managing risks from Fintechs**

The Report flags potential risks around Fintechs that do not operate under banking licences but are regulated within the open banking regime and which can access data. The Report states that financial services firms that share data with Fintechs must ensure that the data is secure before customers are allowed to use the service. In particular, the Committee calls on the Government to consider a review of the payments landscape as a matter of urgency.

12. **Better customer communications and complaints handling**

The Report highlights the role that poor communications can play in exacerbating the impact of an IT incident and states that customers have a right to clear, timely and accurate communications. The Committee considers that regulatory permission should be obtained if a firm is considering withholding information about an IT incident from its customers. If customer communications are ineffective, the Committee considers that the Regulators should step in, for example, to provide a central source of trusted information. The Report also states that firms must act swiftly and fairly in responding to complaints and awarding compensation, if customers have experienced harm or financial loss as a result of an IT incident.

**Next steps**

Whilst a large number of the Committee's recommendations are addressed to the Regulators rather than to firms directly, the Report provides firms with a good indication of the likely direction of regulatory and supervisory focus. Firms should ensure that they are taking steps now to address some of the key conclusions and recommendations of this Report. Outsourced service providers, such as cloud service providers, should also take note of the Report's conclusions and recommendations as these are likely to have an impact on the way that they operate and deliver services in the future. It is also worth keeping the EU regulatory landscape in mind as the EBA and EIOPA consult and publish guidance on ICT and cyber and proposals for introducing a recovery and resolution regime for insurers to bring them in line with banks.

Following publication of the Report, the Regulators have opened a consultation, *Building operational resilience: impact tolerances for important business services*. The proposals include requiring firms to set impact tolerances for important business services (i.e. thresholds for maximum tolerable disruption to help achieve consumer protection and market integrity), to test their ability to remain within those tolerances and to develop communications strategies for when important business services are disrupted.

**KEY CONTACTS**

<table>
<thead>
<tr>
<th>Daniel Gallagher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Associate, London</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ian Stevens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner, London</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Angela Greenough</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner, London</td>
</tr>
</tbody>
</table>