PRA CP29/19 Operational Resilience: Impact tolerances for important business services

BSA consultation response

Restricted
1 October 2020

Building Societies Association

Introduction

The Building Societies Association (BSA) represents all 43 UK building societies, as well as six credit unions. Building societies have total assets of nearly £430 billion and, together with their subsidiaries, hold residential mortgages over £335 billion, 23% of the total outstanding in the UK.

They hold over £295 billion of retail deposits, accounting for 18% of all such deposits in the UK. Building societies account for 39% of all cash ISA balances. They employ approximately 42,500 full and part-time staff and operate through approximately 1,470 branches.

The BSA welcomes the opportunity to respond to the PRA's consultation paper 29/19 Operational Resilience: Impact tolerances for important business services.

We support proposals set out in the consultation paper to strengthen operational resilience, but we ask for further clarification and guidance on some specific areas.

Our response

All financial service firms, including building societies, have had their operational resilience policies and procedures severely tested during the last 7 months of Covid-19 restrictions. The importance of operational resilience has never been clearer. The BSA and its members therefore support measures to strengthen operational resilience and welcome the opportunity to respond to the PRA's proposals.

We note that CP29/19 is one of a suite of consultation papers issued jointly by the PRA and FCA in December 2019 and that it should be read and responded to with a view to the other proposals. The BSA has responded to FCA CP19/32 and PRA CP30/19, and our response to CP29/19 should be read with the other responses in mind.

As both PRA CP29/19 and FCA CP19/32 cover the same topic, namely building operational resilience and impact tolerances for important business services, our response to both consultation papers is substantially the same. We have set out our consolidated comments under topic headings matching the topics and proposals in both consultation papers. You will note that this response includes comments on the FCA proposals. We believe it is important that both the PRA and FCA are aware of firms' concerns regarding both regulators' proposals, so as to better co-ordinate their response to consultation feedback.

In the main, the BSA supports the proposals in both the PRA and FCA consultations, but we want greater clarity on specific requirements, particularly with regard to practical implementation. Many of the requests for clarification set out in this response were first raised by our members at our *Operational Resilience and Outsourcing Policy* seminar on 25 February 2020. We were pleased to have presentations from all the major financial regulators, including the PRA, at the event and members appreciated the opportunity to talk directly with the regulators about the proposals and their expectations. We hope that there continues to be constructive dialogue between our sector and the regulators on this important topic.

Important Business Services

Whilst we agree with the FCA view that a detailed taxonomy of business services would be impractical and would quickly become out of date, we believe there needs to be greater clarity on what constitutes an important business service than the fairly broad guidance that has been proposed. In particular, there needs to be more guidance on the level of granularity needed when identifying important business services. The FCA indicate services should be assessed against the impact of the loss of service on different customer segments, such as vulnerable and non-vulnerable customers and the PRA has its own views. There is potential for conflict between the two regulators over what constitutes an important business service. For example, loss of counter service is not necessarily important to the soundness of a society (the PRA's concern), but it may have a significant impact on vulnerable customers (one of the FCA's concerns). Will firms have to assess each service on three separate criteria; i.e. The PRA's measures and the FCA's focus on vulnerable and non-vulnerable customers? This may quickly become impractical, as firms will need to determine what criteria should take priority in each case.

In terms of granularity there are differences in PRA CP29/19 that need to clarified; for example, 2.3 and 2.4 of the consultation paper. We need to have clarification around whether all elements of an important business service are in scope and need to mapped out, assessed and tested or just those that 2.4 would indicate are "the most critical parts of the service".

We have concerns regarding how far firms need to go when assessing important business services against impact tolerances – for example the consultation states "Firms should be able to remain within impact tolerances for important business services, irrespective of whether or not they use third parties in the delivery of these services". However, building societies rely on many third parties, particularly for payment services, and practically it will be very difficult for societies to assess those third parties if there is an imbalance in the relationship between the

parties. For example, the sending of outgoing faster payments for internet banking payments, or chaps for mortgage payments rely on large clearing banks, over whom societies have very little control and are unlikely to provide any details on their contingency arrangements. The practical difficulties regarding third party services are address in more detail in our response to PRA CP30/19.

Impact Tolerances

Members would appreciate greater clarity on how to define and set impact tolerances. There is some confusion as to precisely what these are based on. The regulations describe them as "the upper limit where a breach is to be avoided", however this does not appear to always be the case throughout the consultation papers which reference this as "before actual harm occurs".

We also need clarity regarding "harm" and the apparent need to always refer to "time" in these measures, where in reality time may not always be the key measure of harm. Instead, the service, activity or the volume might be a more relevant measure.

Linking to the concerns set out earlier regarding multiple criteria for determining important business services and the regulators' differing priorities, we are concerned that firms may have to use multiple impact tolerances for each service. For example, an important business service to vulnerable customers may have different impact tolerances to those customers who live locally and could access a branch, who again may have different tolerances to those that live out of area and not near a branch. Which should the firm prioritise? There is potential for complexity and confusion and so greater guidance would be welcome.

When determining impact tolerances it appears the regulators want firms to base their calculations on the worst case scenario, for example impact on the highest volume. The worst case scenario, while plausible, may be the most unlikely scenario. We are concerned that focus on worst case scenarios detracts from more likely scenarios, where volumes might be lower, but the likelihood of harm occurring is higher because the likelihood of the event happening is higher. It seems counter-intuitive to focus time, investment and resources on unlikely scenarios then likely scenarios.

Lastly, when defining impact tolerances as the "maximum level of disruption", we need clarification regarding the PRA reference of "acceptable" and FCA use of "tolerable", as they are potentially different and may lead to inconsistency and confusion.

Managing follow-on fraud

An important issue linked to impact tolerances, but not directly addressed in either the PRA or FCA consultation papers is follow-on fraud. Follow-on fraud is where organised crime seeks to exploit customer uncertainty in the wake of an operational resilience incident. Sadly, it has become a fact of life that all firms now need to manage. Common fraud types used to exploit the aftermath of an operational resilience incident include:

- Spoof communications apparently from the firm informing that payment systems have been compromised and asking for bank account details so that they can be re-instated;
- Spoof communications apparently from the firm asking customers to pre-register for compensation by providing their bank details;
- Communications from bogus legal or complaints management firms offering their services for an advance fee; and
- Bogus "Information updates" apparently from regulators, government or private sector experts including a link that will distribute malware when activated.

In addition to customer detriment, follow-on fraud that is not promptly addressed creates significant reputational risk for the firm at a point where it will already be in the media spotlight. This would be particularly so for financial services firms whose reputations are built on consumer trust in their ability to protect them from fraud.

With this in mind, we recommend that management of follow-on fraud should be a required part of all firms' operational resilience planning and that an impact tolerance for follow on fraud should be included as standard in firms' impact tolerance assessments.

Mapping

Members would appreciate a greater steer on the regulators' expectations regarding the level of detail and granularity required for mapping. There is a risk that without further guidance, firms may over think the process, make it more complex than it needs to be and perhaps over-map which would be an unnecessary drain on time and resources. Is it necessary to map everything or could a simpler process be used for internal non-critical processes for example?

It would also be useful to know the regulators' expectations with regard to what mapping software would be appropriate to use and how far firms should map third party service providers, including any 4th or 5th services providers the third parties use. We would appreciate further clarification on these points.

Scenario Testing

Members have concerns around how far they need to test "severe but plausible scenarios" and what exactly these are. We believe there needs to be consistency across the sector on scenario testing and the best way to achieve this would be through further guidance from the regulators.

We are conscious that testing could become very complex and resource hungry, as it would appear firms should test each important business service and each impact tolerance at least annually and on any major change. But this could lead to lots of testing and would be in addition to other business continuity and Cyber resilience testing that is already undertaken

We would like clarification on whether testing is always non-production, using simulators, desktop or BC systems, or are regulators now expecting live production systems/network/infrastructure to be tested?

Should firms test for worst case scenarios, which are unlikely or concentrate on testing for more likely/probable scenarios but which may cause less harm? Or should they test for both, in which case how best should they prioritise these tests given the expected drain on time and resources?

Self-Assessment

We agree with the proposals regarding the use of self-assessment.

While recognising that self-assessment should not be considered a simple box ticking exercise we think it would be useful none-the-less to have a template checklist. A standardised approach based on some form of proscribed template would ensure consistency across the sector and assist regulators to compare and benchmark returns.

Reporting

The PRA consultation paper (1.17) states that new regulatory reporting for operational resilience will be developed during 2020. We have not seen any details on this yet and would appreciate clarity on what regulators will require and timescales.

Governance

As stated in 4.1 of the PRA consultation paper, Boards/Senior Management will be expected to "take action to improve operational resilience where a firm is not able to remain within a set

tolerance for an important business service in a severe but plausible scenario"; however this may not always be possible. For example, it is not clear what action a firm could take if a third party major clearing bank failed, particularly if the imbalance in relationship between the firm and the clearing bank meant that the bank was not willing to share information on its contingency planning.

It should also be noted that the Board does not necessarily set the strategy (and thus does not define the operational resilience standards), but instead challenges the strategy set by the business and has the skills/knowledge to do so.

Accountability

The PRA consultation paper (1.10) mentions that it would "monitor the works firms undertake to achieve these standards" and where firms fall short the PRA will be able to hold firms to account if they fail to make necessary improvements. However, what is not clear is how this links into the 3 year period, and what is meant by necessary improvements. In other words, would a firm have to have completed making all improvements or in some cases would it be sufficient to demonstrate they are making progress (as some changes may take significant time)?

We would also appreciate a steer on what exactly "these standards" are precisely, as they are not exact or prescriptive.

Outsourcing and third party service provision

Both PRA CP29/19 and FCA CP19/32 refer to outsourcing and third party service provision and in particular Chapter 8 of CP19/32 sets out an extensive reminder of existing UK and European requirements and guidance on this topic. However, we note the FCA is not proposing any changes to its Handbook rules and guidance as part of its consultation and that the PRA are consulting separately on outsourcing and third party service provision. We will not therefore comment on outsourcing and third party service provision in this response, beyond pointing out that we have also responded to PRA CP30/19.

Date of implementation

Given the welcome 6 month delay to the deadline for this and the other consultations due to COVID-19 restrictions, we require confirmation that the implementation date for much of the requirements remains the second half of 2021. We would hope that any implementation date takes into account the delays to the consultation process and potential knock on delay to the regulators' subsequent feedback and further proposals.

It is also important to co-ordinate implementation timescales for operational resilience requirements with third party outsourcing requirements. It would not be proportionate or effective if an earlier date of implementation for outsourcing requirements means that firms have to revisit work they have already done to take account of later operational resilience requirements.

Conclusion

The BSA and its members support the regulators' proposals to strengthen operational resilience. However, as demonstrated in this response, there are many areas that require further clarification and guidance. The BSA is keen to work with the regulators to address our members' concerns and we hope there will be opportunities for further consultation and direct liaison between the regulators and the sector. Members very much appreciated the opportunity to ask the regulators questions at our event on 25 February 2020 and we are keen to facilitate similar events once the regulators publish the outcomes from their suite of consultations. We also have an Operational Resilience Panel which would be happy to talk to the regulators in more detail about some of the issues raised in this response and our response on outsourcing and third party service providers.

By Andrew Hopkins
Policy Manager
andrew.hopkins@bsa.org.uk
02075205913

York House
23 Kingsway
London WC2B 6UJ

020 7520 5900
@BSABuildingSocs
www.bsa.org.uk

BSA EU Transparency Register No: 924933110421-64

www.bsa.org.uk

The Building Societies Association (BSA) is the voice of the UK's building societies and also represents a number of credit unions.

We fulfil two key roles. We provide our members with information to help them run their businesses. We also represent their interests to audiences including the Financial Conduct Authority, Prudential Regulation Authority and other regulators, the Government and Parliament, the Bank of England, the media and other opinion formers, and the general public.

Our members have total assets of over £420 billion, and account for 23% of the UK mortgage market and 19% of the UK savings market.