HOUSE OF COMMONS

Treasury Committee

Oral evidence: IT failures in the financial services sector, HC 1766

Tuesday 9 July 2019

Ordered by the House of Commons to be published on 9 July 2019.

Watch the meeting

Members present: Nicky Morgan (Chair); Rushanara Ali; Colin Clark; Mr Simon Clarke; Alison McGovern; Wes Streeting; Alison Thewliss.

Questions 1 – 84

Witnesses

I: Simon Chard, Financial Services Partner, PwC; Sarah Isted, Financial Services Risk and Regulation, PwC; Marcus Scott, Chief Operating Officer, TheCityUK.

Written evidence from witnesses:

– PwC

Examination of Witnesses

Witnesses: Simon Chard, Sarah Isted and Marcus Scott.

Q1 **Chair:** Good morning and thank you very much indeed to our witnesses for being here for the session this morning. It is a slightly unusual format, because we have turned it into more of a round table, which is a format we have used for other inquiries. I think you are very kindly going to share your expertise with us this morning. It is partly about asking questions, but also about understanding the work you have done, to help us to set the scene for our future inquiry sessions on operational and IT resilience in the financial services sector.

I am going to ask you to introduce yourselves. This is being recorded; it is all on the record and everything else. For colleagues who are here, perhaps we can be a bit more free-flowing than our normal sessions. Colleagues should feel free to ask supplementaries and make sure we have a discussion and dialogue, as well as trying to extract as much information from our witnesses as we can. Mr Scott, perhaps we can start with your introduction.

Marcus Scott: I am Marcus Scott and I am the chief operating officer at TheCityUK. I am responsible for the work we do on fintechs, cyber, AI and operational resilience. We are a cross-industry membership body for financial and related professional services, and we represent about 150 major firms across the entire industry, which operate both across the UK and internationally. About two-thirds of the 2.3 million-odd people who work in the industry are based outside the M25. It is also the UK's largest exporting sector, so it is a vital part of the UK economy.

Sarah Isted: I am Sarah Isted. I am a partner at PwC, and I lead our financial services, risk and regulatory practice, and specialise in governance and culture

Simon Chard: Hello, I am Simon Chard, also a partner at PwC. I specialise in operational resilience.

Q2 **Chair:** I am going to start with a very broad question, which is to talk about the report you have produced. Who did you speak to? How did you decide what should be included in the report? I am not sure who is best placed to go first, to say where the driver of the report came from and its genesis.

Marcus Scott: Would it be helpful if I put a bit of context around the report and what it is?

Chair: Please do; that would be great.

Marcus Scott: This is a relatively new area and a new term in the terminology of the industry. With any area of human endeavour there is the risk that some things are going to go wrong, so this report seeks to

set the scene for operational resilience, which is a discipline that brings together several areas around technology and processes. Operational resilience is essentially concerned with whether a firm reacts appropriately when a risk crystallises. That is at the heart of it. It especially recognises that the solutions we have developed for recovery and resolution—in other words, normally the injection of capital—will not always be able to resolve that particular scenario, if it is a technology issue.

What has recently emerged is the embedding of capabilities, processes, behaviours and systems that allow a firm to carry out its mission in the face of incidents, regardless of where their source is. It means that the siloed approach that was previously taken to data security, IT systems, business continuity, cyber, etc, is being replaced with this term "operational resilience", which looks at them as a whole.

We and the industry recognise—and, from what the regulators have said, they also recognise—that operational failures are unavoidable. The important thing is, when incidents happen, to make sure we minimise the impact and, if at all possible, minimise any disruption to customers. It is very much about that focus on customers. This report follows the engagement that we had with regulators last year and the discussion paper that came out from the FCA and the PRA, our response to them and our engagement with them. Simon can talk about the detail of who we spoke to and the people we interviewed.

Simon Chard: We spoke to 30 to 40 people across the industry. We tended to speak to chief operating officers and board members, at that level, so not necessarily the practitioners, but more senior folk across financial services, so in banks, insurers and asset managers, and also the financial market infrastructure, such as payment providers. We sought to break the topic down into areas. We felt that, while the discussion paper started the discussion across the industry, it would be helpful for us to highlight the key areas and considerations in what is a new topic, on which there is not a great deal of material.

That is why we structured the report as we have, in relation to some of the threats out there facing the industry, the governance, which is a big aspect of this, and some reflections on what we saw happening on connectivity. A large part of this is not for any one individual firm; it is about how that firm acts and operates within the system of financial services. We have laid out a set of recommendations flowing from that. It was designed to listen to people around the City, the banks and others, and then provide this summary for people to work with. We also pulled together and produced a framework. Again, because the discussion paper started the discussion, we expect the consultation paper to add to that, but to give people a framework to start thinking about the topic.

Q3 **Chair:** Did you talk to people for whom things had gone wrong?

Simon Chard: We did, but we also talked to people for whom things had not gone wrong. We covered both.

Q4 **Chair:** You tried to identify companies that already had systems in place, but also those that had learned from experiences.

Simon Chard: Yes.

Q5 **Chair:** In your experience and expertise, what would it mean if the UK were to be seen as a world leader in operational resilience? We will come back to what operational resilience means. You have both said it is a new term, and clearly people will mean different things by it. It is important to have a definition of it, as you have talked about. What would it mean for the UK for people around the world to think the UK is leading the way in this sector?

Marcus Scott: That is a key point and there are two aspects to it. First, most companies that are members of TheCityUK are international, and will either be headquartered here, or have European headquarters or a base here. Most companies already serving millions of customers will be operating across multiple jurisdictions, so international co-operation becomes even more important. At the moment, the UK is at the forefront of that. We are in a position where the regulators in the UK realise that this is likely to be the third big pillar of regulation, alongside conduct and prudential regulation. They are therefore seeking to develop tools that the industry can use and the regulations that are important to them. That is really important. Co-operation at things like IOSCO, the Basel Committee and the Financial Stability Board is essential, and will come over time. It is only just being discussed at the moment, at fairly early stages.

Sarah Isted: One of the themes we raised, as Simon pointed out, was governance. Where entities are internationally dispersed, but have a relatively small entity here in the UK, sometimes that entity has less influence within the global group. If our regulators are leading the way on different topics that will help them have greater influence in the group on those topics. That is an aspect to pull out as well.

Q6 **Chair:** You came up with some key recommendations. I am a great believer in culture and cultural change, and I was pleased to see that culture was part of the key recommendations. There are six key findings. Are they equally ranked? Are there any that you think are the top ones? If organisations worked towards implementing all of them, would it mean a more robust system?

Simon Chard: We would pull out those that relate to governance, because the whole discipline is about being able to prove your resilience or otherwise. If you are able to make statements about how resilient you are through your governance, many of the other items will follow. Regulation is an important driver and is important on this topic, to encourage and supervise, and innovation is also important. While there are a number of threats here, there is an opportunity for financial

services to continue innovating, to identify new solutions for customers and to respond to fintech and other matters. We would probably focus more on governance, as your ability to prove that you are operationally resilient.

Q7 **Chair:** That is slightly counterintuitive. I do not disagree with the governance point at all, but people might think that you actually need to invest millions of pounds in new software, skills, IT platforms and everything else. I think the point you are making is that it starts with the governance of the relevant organisations.

Simon Chard: Decision-making covers all those aspects, does it not? Decisions firms take over where and how to invest will mostly impact operational resilience. It is because operational resilience is an outcome rather than an activity. If you are able to prove the outcome, your ability to report that through some sort of governance is the ultimate test.

Q8 **Chair:** Moving on to the definition of operational resilience, it is very interesting to phrase it, or think of it, as an outcome. Marcus, you mentioned it was a new topic; you talked about technology and processes. You have an "operational resilience key domains" diagram in the document, but what is operational resilience? For the purposes of our inquiry, which bits should we be pressing, and pressing regulators and industry participants on?

Marcus Scott: Shall I cover the broad terms? This is one of the reasons that Simon and Sarah have talked so much about governance: it is about embedding those capabilities, processes, behaviours and systems. Often, those meet at the board level and the board is responsible for all of them. In the past, a number of these areas—such as IT security, business continuity or cyber—have been in different silos. This is about looking at them all together. Rather than looking at functional activities within a company, it is about looking at the end-to-end journey. If you are delivering a particular product, what are the different things that impact on it? That is it in general terms. Simon, I do not know whether you want to go into more detail about the specifics.

Simon Chard: The other way to think about it is in terms of the impact on customers. That is important, because it is why we are focusing on operational resilience.

Chair: Absolutely, because we have seen a few things where the impact has been very damaging.

Simon Chard: The outcome for customers is most important. For example, the framework looks at a set of underlying capabilities that you would expect firms to have, but is more about how you look at bringing them together. You think about things from an end-to-end perspective, with customers clearly at the front end. Then it is the firm developing a clear understanding about interoperability and the relationship between premises, people and technology, and quite complex component parts.

Then it is understanding, if something is impacted along that end-to-end service, the impact on the customer and what group of customers, at what time, are using what services of the bank, if it is a bank. We think it is important to keep the customer focus, rather than it becoming something else to look at the internal operations of a firm.

Q9 **Chair:** Sarah, this might be a question more for you on regulatory developments. We are going to come back to look at regulation and supervision later. The point you made was interesting, which was that, if our UK regulators are leading the way, it helps to push global firms. Broadly, where do you think our regulators are, particularly the FCA and the PRA? Are they the most relevant?

Sarah Isted: Yes. They see this as a key area of focus. The discussion paper they put out was the start of this discussion, as Simon said. The consultation paper that will follow will hopefully take that forward. They would recognise that this is very much the start. They would recognise that they have some good people within their teams who understand the topic, but that they need more people. The skills across the industry need to be improved in this area. It is a new area and a new, complex topic, so we need to make sure there are enough people focused on it. As we say in the report, that might mean bringing in people from outside financial services to bring a different perspective and particularly to bring the customer view to it.

Chair: We are going to talk about some incidents now.

Q10 **Alison McGovern:** What do you all think is the biggest risk?

Marcus Scott: If you look at the FCA's report from last November about the incidents, the biggest single issue there was change management. That probably represents one of the biggest. We laid out five areas, talking about speed of technology innovation, managing change, cyber threats, climate change and fraudsters. Those two, about the speed of innovation and managing change, are probably the two biggest. We have seen across all industries, whether travel, music, transport or any sector of the economy, new technologies coming in and driving down the cost of doing business. That is allowing new entrants to come into financial and professional services, as they should, and means that existing firms that are already serving millions of customers have to invest. With that investment in new technology comes an element of risk. If you put in new systems and change the way you operate, you need to make changes, which inherently brings risk with it.

Q11 **Alison McGovern:** I will come back to legacy systems in a second. Would you say that new technology and innovation is a bigger risk than cyber-attack? Simon, you look poised.

Simon Chard: If I had to choose between the two, cyber is the bigger threat. The other option, which is around new technology, is much more about an opportunity and is something that should be encouraged. Firms continue to be innovative for good reason: for customers. The cyber

threat, as we see it, is growing and increasing. It is often the combination of threats that causes challenges. Often, two or three different things come together, as you would have seen in previous incidents, to create a scenario or situation that people have not seen before.

Q12 **Alison McGovern:** What proportion of incidents that would be observable by a customer are created by cyber-attacks, versus firms' own failures?

Simon Chard: The FCA publishes that data and that ranking. That is the best place to see that. Recently, the top three have moved between cyber and change. They are cyber, change and third parties, and there is an FCA paper on that ranking.

Q13 **Alison McGovern:** This is going to sound like a naive question, but who is attacking the financial services sector?

Chair: Do we know?

Simon Chard: There is a lot of information publicly available on the various sources of cyber-attacks, from different nation states and groups. I am not a cyber expert myself, but there is a fair amount of information that analyses the source of the attacks. I think it is a wide range

Q14 **Alison McGovern:** We have had a number of inquiries and session that have dealt with the consequences of change from legacy systems. In dealing with legacy systems, for example from past mergers, is that a substantial chunk of the problems that customers experience?

Simon Chard: Again, our experience is somewhat limited but, based on our experience, I would not single it out beyond new and emerging technologies. We do not have the data on whether a change is in relation to a legacy system or a new cloud-based system, for example. We say in the report that it is not appropriate to link legacy with fragility completely, because some legacy systems are reliable and supported. One of the risks that firms need to manage, as many of them are, is that the legacy systems are supported by individuals who have been working on them for a number of years, many of whom are approaching retirement. People need to deal with that aspect of the risk.

Q15 **Alison McGovern:** What are firms' systems like for training and that sort of thing? Presumably, if you work at an old bank, you have to be able to use its technology.

Simon Chard: One of the most encouraging stories we heard recently—again, this is an anecdote, but it is helpful—was of firms bringing together new technologists and existing older technologists, who have worked on legacy systems and different types of coding, so that they share and learn. There are some interesting stories about how some of the more recent technology graduates and people coming into the firm at a young age can learn from those working with the legacy systems. The point is correct that technology skills continue to be very important. As

we say in the report, one of the keys to dealing with this and making firms more operationally resilient is to improve and increase the level of technology skills.

Q16 **Chair:** In your report, you say that 80% of firms "struggle to hire and retain people with the required skills for innovation". That must be one of the risk factors.

Marcus Scott: One of the biggest challenges now is that our industry is competing with the rest of the economy for, more or less, the same skillset. This is only anecdotal, but one of our members, which was a bank, lost a team of web developers to Just Eat, the takeaway company. Now, we are seeing the same skills across almost all sectors. At this point, before we have the volume of skills that can address the needs of our industry and other industries across the UK economy, we are seeing that we have to compete actively for those skills, which are very marketable and therefore move around. That has become the biggest challenge: those things were previously siloed within one industry. If you knew how to do one thing in a particular industry, you specialised in that. They are now much more general, as those technologies are across almost all businesses in the economy.

Q17 **Alison McGovern:** Is that a new thing, though? Banks have also been retailers on the high street for a number of years. They would be competing for customer service professionals, along with high street retailers and others. Is that really a change?

Marcus Scott: It is a change on the technology side. For example, take this AnyWeb technology. Designing and maintaining a website for customers is pretty much the same, no matter what service you are delivering. In the past, working in a bank branch, for example, would be very different from working at a branch of another business.

Q18 **Alison McGovern:** Just to challenge you, there is a lot of evidence that, pre-crash, retail-style working was brought to the banking industry and some of the marketing techniques that were used to sell financial services products influenced the culture. Given the legacy systems issue, if we are seeing a despecialisation of the profession because of technology, to what extent is that itself a risk?

Marcus Scott: I see what you mean. Because the industry is well regulated, for very good reason, a lot of those positions have to be specialist positions. I was referring more to the underlying technology that enables those organisations to operate, in other words things such as machine learning, data science and web development. It is those things that are more common. Skills in customer service and the regulations that revolve around it are still quite specialist to the industry.

Q19 **Alison McGovern:** They are now anyway. There were not in the period up to 2008.

Simon Chard: We are observing an increasing pace of change in technology. Cloud computing is a good example, where, over recent years, we have seen firms moving to private or public cloud, and embracing different types of cloud technology. We have seen that happen in a short space of time, and it is fundamental to the way in which the business is run.

Q20 **Alison Thewliss:** Could you tell us a bit more about the key opportunities that you feel technology innovation creates for the financial sector? You talked about being part of global leadership, but would you like to say more about the opportunities and how firms can use innovation to improve customer experience, as well as operational resilience?

Simon Chard: There is a great opportunity. Part of it comes from the ability of a firm to embrace new technology. If you are better organised in the disciplines we have talked about and if you have a better view of how the firm operates in relation to your customers, it is easier for you to embrace a new technology—open banking is an example—or develop a new product or service, because you have the clarity of how this operates across the firm. We also see benefits in the way that people are able to run their business and be more customer-focused. They are running the business and thinking about services for customers, perhaps, and are less focused on the organisational structure of a functional business. We see some opportunities there. Finally, as you do this work, you can identify how to be more efficient, because you are looking through the organisation rather than up and down the silos.

Q21 **Alison Thewliss:** I was quite interested when you were talking about machine learning, setting systems up and almost letting them go. How do you ensure that those systems are maintained and how do you pick up failures within them, once they are up and running? Who maintains and keeps a check on them?

Simon Chard: From our experience of controlling those operations, if that is the way to describe it, as we have worked through that in specific situations, it becomes quite similar to the set of controls you would put around an operation that is executed by humans. Breaking that down into thinking through, for example, how the piece of technology has been coded, understanding that and then viewing it in operation, as we work through that, how it is controlled is quite similar. Linking it back more to operational resilience, we would say, "Prepare for that to fail in some way; then understand what you would do instead and what you would substitute". If you have something built with AI versus something run by humans, or you have a hybrid of the two, you could spend a lot of time worrying about whether it will fail, but it is probably better to spend time thinking about what you do when it fails and what the alternative is.

Sarah Isted: I would add something about the culture of an organisation. As well as looking at the controls and how things are managed, make sure you have the right culture and a good culture to

help drive forward that innovation. There are three aspects we would pull out. The first is a culture of curiosity, so asking the right questions and seeking the right answers from across the organisation, when adopting or thinking about adopting new technology. The second is a culture of openness and transparency, so that everyone in an organisation feels able to raise issues and concerns, and that they will be listened to. The third is a culture of humility, to understand the risks and learn from mistakes, whether yours or throughout the industry. If you have those three aspects to your culture, that will help you in this,

Q22 **Alison Thewliss:** The report claims, "Disruption at a scale that threatens the viability of one or more major financial services firm has moved from unlikely to comprehensible, and now to inevitable". Can you give us some examples of the types of disruption that might threaten the viability of financial services firms?

Simon Chard: We have all seen recent events in which firms have been disrupted for an extended period. We have also seen events outside of financial services when firms have been brought to a halt and have had to go back, relearn and re-establish the very data sitting behind them. That hypothesis is built on understanding that there is an inherent complexity within financial service firms. There are 59,000 firms in the UK, and they vary in scale, but some necessarily have hundreds of critical systems, so there is a level of complexity. There is the cyber threat we talked about previously. There is a need to continue to make change. As we said earlier, change management is one area that unfortunately creates incidents within organisations. It is those things coming together.

Q23 **Alison Thewliss:** To what extent are there technical standards across those 59,000 firms? Are things being done in the same way or in very different ways? What kinds of threats or risks does that present?

Simon Chard: There is a set of regulatory principles from the rulebooks that firms need, not to set their technical standards, but to meet through the work they do. For each of those disciplines, if you look at the framework in the report and those capabilities, you will see technical standards in risk management, cyber or physical security. All of those things together give an appropriate framework.

Marcus Scott: There have been some quite helpful things, as we discussed in the interviews. The senior managers regime and the establishment of SMF24, which means that somebody is specifically responsible for operations and technology, have been helpful in escalating that to board level. This goes back to Sarah's point about governance: it is making sure that there is a clearer line of accountability.

Q24 **Alison Thewliss:** We have talked briefly about issues with past mergers and acquisitions, and the difficulties they may cause for systems. Are firms taking account of those risks adequately in their due diligence, when mergers happen?

Simon Chard: One of the recommendations in the report is to pay closer attention to that. It is a factor. You will see quite often in firms that the way systems are set up reflects previous organisations and incarnations. One of the recommendations we make is to pay more attention to that area.

Marcus Scott: In the past, if an acquisition had been made 15 or 20 years ago, that probably would not have been on the agenda. Now, there is much more of an understanding of that, when it is happening in real time. There is a process to look at cyber risks and the internal organisation of those companies to get a better appreciation of how resilient they are.

Q25 **Chair:** You are right to say that, in mergers and acquisitions, when you are busy putting people together, you are not really interested in asking questions about IT. Going back to the skills point, it is a huge challenge, is it not? You need skills in the regulators to set the standards or regulations, or at least to supervise that they are being followed. You need skills in the industry more broadly, as you say, and people are now highly competitive. I assume that the people who worked in IT at Deutsche Bank are not going to have too many problems finding other roles, which is fortunate for them. The need to give advice to people within the financial services sector, in terms of operational resilience or how two systems can be put together, means a lot of demand for skilled people. The sector is presumably struggling to have those people at the moment, or people are coming from overseas. People are in high demand.

Marcus Scott: Yes, very much so. In the same way as, in the 18th, 19th and 20th centuries, disciplines such as law, accounting and engineering were established, this is increasingly starting to happen. There is now a Chartered Institute of Information Security Professionals, which there was not previously. That has only just happened. Those things are important, because they start to establish certain disciplines, which means that more and more people are signposted to go in them. If those pathways into particular careers do not exist, people will not know to go into them.

Chair: And more qualifications as well

Marcus Scott: Yes.

Mr Clarke: Sarah, you mentioned that you need to ask the right questions to get the right answers.

Chair: That applies to us as well.

Q26 **Mr Clarke:** That means you need to know the threats you face. Simon, you referred a moment ago to the cloud and emerging challenges for resilience, with new forms of technology and threats emerging off the back of them. What would you classify as the principal emerging threats

in the landscape?

Simon Chard: We have talked through them before. There are threats in relation to cyber and data. We have not talked about third parties. That introduces risk to organisations.

Q27 **Mr Clarke:** Third parties on whom they rely?

Simon Chard: Exactly, yes.

Q28 **Mr Clarke:** In what space do those firms operate?

Simon Chard: In various spaces. In looking at a service end to end, a mortgage or current account service, you will find that various third parties are responsible for different activities along that chain, including big and sometimes smaller technology providers, or things might have been outsourced. It is about having that understanding. The FCA and others monitor the increase and decrease of these risks.

Q29 **Mr Clarke:** It is having those third parties integrated into your own systems, I suppose, and understanding how they operate with your data. That is really the challenge, not just outsourcing both the task and the responsibility for operational resilience.

Sarah Isted: That is a key point from the governance perspective. Where you have outsourced something to a third party, you have to recognise that you are still, ultimately, accountable for it and make sure that you have the right controls and governance over that third party. As Simon said, as we get increasing numbers of third parties involved, those governance issues rise for organisations, but it is something they are focused on.

Q30 **Mr Clarke:** We talk a lot about the rise of open banking and the increasingly intangible nature of data in a digitised world. Are threats emerging in relation to that?

Marcus Scott: I think some will emerge, with new players coming into the market that perhaps have not been regulated. That brings in the issue of where to put the regulatory perimeter, so that everyone is operating under the same set of rules. There has been a tendency to look at new technologies and say that we do not want to stifle them, which is right. At the same time, they need to be regulated in a way that makes sure they are operating under the same set of rules.

Q31 **Mr Clarke:** Are they regulated in that way at present?

Marcus Scott: Some are and some are not. If you are dealing directly with customers, you tend to come immediately under the purview of the FCA. If you are providing technology, you may not.

Q32 **Mr Clarke:** The back office areas are much less closely scrutinised.

Marcus Scott: Yes, and we talk in the report about where that regulatory perimeter is set and whether it is time to review that for

certain areas. I am sure that will be part of what the FCA and the PRA are doing in this area.

Q33 **Mr Clarke:** Is there evidence that the FCA and the PRA are alert to this? The fact they should be does not necessarily mean they are. We see them all the time; they have a vast remit and this may well not be their area of greatest expertise. They are trained precisely on conduct issues, and the lesson of any industry is that it always fights the last battle. Of course, the last battle was around resilience in a different sense, of sustainability in the face of financial shocks. This is a completely different challenge.

Marcus Scott: The fact that the PRA and the FCA are leading the pack of international regulators on this is a good sign that they are aware of this and are concerned to be leading on it. There was a recent report by the Bank of England on the future of finance, which talked about this area, the dependence on technology and where that perimeter should sit. That debate is ongoing; I do not think it has been finalised or settled, but it is a current debate going on, both within the industry and among the regulators.

Q34 **Mr Clarke:** I saw in the report a reference to the US firm Sheltered Harbor, which is in essence the ability to back up crucial data offline. Is that open to UK firms or is there a UK equivalent?

Marcus Scott: No, I do not think there is a UK equivalent currently. This is something the PRA and the FCA have talked to us a lot about. On a sliding scale between market and regulatory solutions, at one extreme, the regulatory solution is for the central banks to put in more capital and liquidity, and a team to supervise the business. At the other end, you might have two banks that offer to white-label each other's services, in the case of an emergency, with the ability to host each other's customers for a period. The current debate is about where these solutions should sit on that slider between the market and regulatory solutions.

Q35 **Chair:** What does "white-label" mean?

Marcus Scott: In other words, they would provide the service to somebody else's customers. They would put on the label from whoever they were providing it for, rather than their own brand.

Q36 **Mr Clarke:** We saw last year with TSB the almost complete collapse of its operational systems. In those circumstances, would it have been viable to white-label? In principle it should be but, when you hit the eye of the storm—and TSB was in almost complete chaos at that time—is it conceivable or feasible to move customers' accounts into the care of another bank, given the level of disruption?

Marcus Scott: I do not know enough about TSB to comment specifically on that.

Mr Clarke: My worry is that it sounds great on paper, but does not work

in practice.

Marcus Scott: With all these things, it is about the forward planning and the investment that has been made beforehand, which might make that scenario feasible. I do not know whether we have seen any other examples of that kind of white-labelling of services, but, from my understanding, this is in the fairly early stages of development.

Simon Chard: The thrust of our recommendations is around planning ahead for such scenarios. We do not yet know exactly what that solution might be. It might be a Sheltered Harbor version for the UK; it might not. It might be a shared utility. Those solutions do not exist today, and a large part of this drive is to explore and establish them. To your point, it is not for the last battle, but just to understand what those scenarios will be in the future.

Q37 **Mr Clarke:** Exactly, because, in many ways, the predators will always adapt more quickly than the prey. That is the thing. This is their entire focus, whereas, for the bank, it is something to try to mitigate. Do we know what quantum the banks are investing in this field, at the moment? Are substantial amounts of money being invested in this level of preparedness?

Simon Chard: In terms of the data we do have, we track investment through a survey we do with CBI. In the last couple of versions of that survey, which is quarter by quarter, we have seen firms investing more in technology, which is one aspect, but not every aspect. There is a lack of data points to establish just how much firms are investing in operational resilience at this point, but there are some indicators.

Q38 **Mr Clarke:** Obviously we are set to leave the European Union at the end of October. Are there issues arising out of that departure that need to be addressed in the specific context of operational resilience?

Marcus Scott: Brexit is a strong example of the industry responding, in operational resilience terms, to a challenge that it has been posed. That was partly triggered by the "dear chairman" letters that were sent out from the PRA a couple of years ago. Over the last three years, firms have moved resource or improved functionality on a range of services, including regulatory licences, which will allow them to serve customers. They have adapted for a range of situations, regardless of what might happen from a political point of view. That is a good example of how firms have to adapt, because there is a range of scenarios, they do not know exactly which will happen, but they need to be ready for when it does.

Mr Clarke: One of the themes we hear constantly from the Governor, when he appears in front of us, is that the financial sector is probably the most prepared of any in the economy.

Chair: Capital will not always solve this.

Q39 **Mr Clarke:** This goes to that exact point. That views it from the context of a 2008 mentality of capital buffers and the rest of it, whereas this is a quite different field of practical, operational resilience.

Marcus Scott: Yes, and that was the focus of the "dear chairman" letters. A focus of a lot of the activity we have seen from our member firms is that practical operational ability to deal with all the scenarios presented to them.

Q40 **Chair:** I want to look at governance. This is open to all. We have talked about front-line skills; what about skills in the boardroom, in terms of having the information reported in, and understanding the consequences and risks? Where is the sector with that?

Sarah Isted: There are three relevant aspects of governance that we have pulled out in the report. The first is about having the right levels of accountability. Marcus mentioned the senior managers regime and having a new senior manager function that covers this area. That has helped to drive a focus on this.

Q41 **Chair:** Can whoever is best placed—we will come back to Marcus in a minute—say a bit more about that? That would be helpful.

Sarah Isted: The senior managers regime was brought in for the banks in 2016, as you will be aware. Later, the PRA brought in an additional senior manager function that covers operations and technology.

Chair: This is SMF24.

Sarah Isted: That is right. Interestingly, as you will again be aware, most senior manager functions are intended to be assigned to one individual. This is a difference, in that it is recognised that that remit is so broad that it could be shared between two individuals. Most firms that we are aware of, certainly the larger firms, are choosing to split it, which shows the breadth of the issue. We have seen that having those individuals and that focus as part of the senior managers regime has brought the issue even further up the priority list of boards and executive committees. They would recognise that that has been helpful. The accountability piece is really important.

There is then an issue around governance structures. We have already talked today about how, when you look at operational resilience, it is important to look end to end for a business service or product. In some organisations at the moment, governance structures are quite siloed. One of the recommendations in the report is to look at how you enhance and potentially change your governance structures to be more end-to-end focused. You can look at the whole lifecycle of a product or business service and think about the end outcome for customers. That is something organisations are looking at.

The third area is MI, management information. We make the recommendation that it needs to follow your governance structure, so

organisations should be looking at how to create end-to-end management information, again rather than siloed. Many organisations already have that end to end for product and service performance. They look at a product in its entirety, but some functions, like risk or finance, tend to be in silos. They will currently receive information on risks as a whole, but we recommended that you should look at your MI across an end-to-end process. That needs some work in relation to some functions. If you have the right accountability, governance structures and MI, it will help the board and executive committees ask the right questions and take the right actions.

Q42 **Chair:** Those are very practical recommendations. Marcus, perhaps this is something we should be exploring in the course of our inquiry: what are TheCityUK member firms doing to implement those recommendations? You mentioned silos earlier on. Are they still siloed rather than looking at end to end?

Marcus Scott: There is a good graphic in the report somewhere that talks about the levels of maturity, and we definitely see there are different levels of maturity for different businesses. We made the same point in a report we did on cyber governance a year or so ago. There is a different level of maturity depending on the company and often that depends on the nature of the company. For example, retail banks are often at the very forefront of cyber-attacks and fraud.

Q43 **Chair:** Yes, so they have an incentive to get ahead of this.

Marcus Scott: Absolutely, and that is now becoming more of a standard. As always happens, what was best practice for the very leading firms eventually becomes best practice for everybody as everyone starts to adopt those techniques. There is a scale of maturity and, as this becomes more commonplace, we will see more companies develop more sophisticated responses to it.

Q44 **Chair:** Is best practice sufficient or should we be asking, when we have regulators in front of us, "Are you planning to adopt this, to put this somewhere?" I do not quite know where it would sit. Is it better to sit in the Corporate Governance Code as opposed to FCA or PRA regulation?

Marcus Scott: You are absolutely right. A number of interviewees we talked to said that, from their perspective, this kind of resilience is a commercial imperative. They see having this kind of resilience as being something that they would present to their customers and clients as very positive. As to where that sits, there are elements of it that can probably sit in the Corporate Governance Code, because they deal directly with boards and with the senior management, but other elements of it will filter down, over time, into the regulatory teams.

Much of the framework that Simon and Sarah have put together in the report is what we would hope that many member firms will use as the measure for their board. We noticed that, when we laid out a framework in the cyber work we did about a year ago, we had a number of members

coming back and saying, "We are now using that". There are various different frameworks. In cyber, there is a range of different frameworks that you can use, but it is making sure that people are using some kind of a framework to access themselves and get some external validation of that as well.

Q45 **Alison Thewliss:** I want to ask about skills, understanding and expertise. How can you be sure that senior managers, through those levels of governance, all the way up to the board, have an understanding of what coders are doing on a daily basis? How do you ensure that the coders, who are working away on a daily basis on tasks, have an understanding of what is required of them by those senior managers?

Simon Chard: This is a new discipline, but there are other places to look. For example, there was a "dear chairman" exercise in 2014, so it is new and the focus is building, but there is learning from previous incidents and from the work done. Two "dear chairman" exercises were undertaken by the regulators to examine those very points about how you link an underlying failure, which might be very nuanced and specific, to the overall levels of governance. For us, it comes back to the same answer: if you have an understanding not just of the services but of the technology that underpins those services and what that interrelation is, by extension you can then understand where a coder is coding, where it is particularly important and how that links in the chain back to a critical service versus some coding activity that is important but not entirely critical. We see that as a way in which you can understand the link between them and focus on what is important.

Sarah Isted: Under the senior managers regime, as you may know, the senior manager has a responsibility to make sure they are taking what is called "reasonable steps" to ensure that the areas of their responsibility are operating appropriately. On the definition of "reasonable steps", there is no detailed checklist of everything they should be doing, but the regulators are intending that they have the right governance, the right people in place, the right controls and processes, so they can look over all their areas of responsibility and be comfortable that things are operating appropriately. That is what the senior manager 24—the person responsible for ops and technology—will also have to do. Given it is a newer area, as we have talked about, making sure you have the right people with the right skills both to do the work and to review and oversee it will be critical. It comes back to the discussion we have already had about making sure you have the right skills in your teams and in the industry as a whole.

Q46 **Alison Thewliss:** Are there any areas of risk if that is an outsourced IT team rather than an in-house IT team and how are those controls kept?

Sarah Isted: Yes. We talked earlier about outsourcing. This is the key thing, for me: if you are a senior manager and part of your areas of responsibility are outsourced to a third party or even to another part of your group—particularly in a global group, you might outsource

something to an overseas team—you need to make sure you are comfortable with the work they are doing. You need to make sure you are comfortable with the scope of what they are doing and the outcomes of what they are doing, in the same way as you would be if it was a team directly sat outside your office. Even if you have outsourced it, you cannot remove the accountability for that outsourced work.

Q47 **Alison Thewliss:** Is there any specific training for coders working in those teams on those kinds of responsibilities?

Simon Chard: As we mentioned earlier, there will be technical standards that they will code to depending on the technology and the language. Again, this is more around understanding, when there is a failure in that coding, what the impact of that will be and how you deal with that problem. It is a good example of a scenario perhaps that you might create, which would be to say, "There has been some rogue code", but how do you understand the rogue code by this team, in this location? What impact does that have on your customers? It is that piece. There is focus on making sure people do good coding and have the right technical standards to work to. We are talking about balancing that with an understanding that failure is inevitable, what the impact of that failure is and how you get around it.

Marcus Scott: It comes back somewhat to that management situation, because it is about understanding where things are in the process and where you have potential danger areas or potential red areas. Then the governance area kicks in, because that is then the thing that gets focused on. A lot of it comes down to how you are managing those systems and assessing them as they go forward.

Q48 **Rushanara Ali:** Good morning. I am going to try not to paint too much of a doomsday scenario. As most of the questions have already been covered there is a bit of a risk of repetition, so do not feel you have to repeat anything you have already said. I wanted to pick up on the point about skills. Do you have an assessment of how many people we would have to bring in from overseas with expertise because we do not have them here, at the moment, while the work is being done to build the field and make sure there are institutions that can train people with the relevant skill sets needed for this new frontier of understanding technology, given how fast it is developing and how fast the financial services and other sectors are adopting new technologies, sometimes not realising the underlying benefits and risks?

Marcus Scott: I do not have specific numbers for you, but our industry has always been very reliant on talent from overseas. Often, and increasingly nowadays, that comes in the form of project teams coming over for short periods of time and doing some work on a specific thing.

Q49 **Rushanara Ali:** That is not difficult. With any visa restrictions and so on, that is pretty smooth and straightforward, is it?

Marcus Scott: We did a piece of work about 18 months ago, which laid out some recommendations that we felt would improve the system. Probably the key factor is the flexibility of the system to allow people to come in for short periods and at relatively short notice.

Q50 **Rushanara Ali:** So that is possible and not difficult. What about longer periods, if banks and other financial institutions need them in for longer? Are there any new restrictions or is it pretty smooth sailing to be able to come?

Marcus Scott: There are always improvements that we can make to the system, definitely. There are some fairly well-documented examples where it has taken a long time to get somebody in or where the regulator has said, "We would like you to have this number of senior managers in this particular company" and the Home Office has perhaps not given them that number of visas to come in. There are always improvements and tweaks that can be made to the system.

The bigger point is probably about the volume of skills. There, it is not necessarily taking people and providing them with seven or eight years' training; it is not like becoming a doctor. A lot of this is dependent on taking the 2.3 million people we already have working in the sector, giving them skills and improving their skills. One thing that has come out more strongly than anything else is that a lot of this material is available, but you need to point people in the right direction, actively encourage them to do so, and provide them with the time and resources to do it. I see a lot of our member firms now realising that and coming round and putting various different systems in place to support it.

Q51 **Rushanara Ali:** Sticking with the human capital that we have and looking at past analogies, without fighting the last battle, we can take the example of early derivatives scandals, such as Barings. I know the senior managers regime will help, but senior people did not realise what this guy was up to. There are lots of other scandals like that: financial crisis, subprime mortgages and so on. The people further up the chain and alongside did not pick these things up. Technology is moving so fast, with machine learning and AI, that at the consumer level we do not know, or have transparency on, which bits are which, which is human intelligence and which is AI. To what extent do you think people working in these sectors, across the board—you mentioned over 2 million—are resilient in their knowledge to spot emerging risks? We have all talked about concentrations of risks and new challenges. Are we resilient in terms of the wider population working in these sectors?

Marcus Scott: There is always going to be that scale of maturity. There will be some firms that are at the very forefront of it and some firms that are less advanced in what they are doing. Again, this comes down to the whole governance issue. The senior managers regime has changed the environment significantly.

Q52 **Rushanara Ali:** Is it adequate? Is it enough? Of course, that came out of

the financial crisis, not out of a technological crisis, in terms of banking being undermined by technology failures on a large scale. Is it fit for purpose or is there anything else that we need to be anticipating that needs to be sharpened up with that regime?

Simon Chard: There are a number of things and we have made 17 recommendations in the report to address that. There is an acknowledgement, to Marcus' point, that there are people who need to perhaps focus on a different area or to think differently. It is as much about thinking differently and innovatively in the areas that Sarah picked up.

Q53 **Rushanara Ali:** Obviously, connectivity has grown. Are there specific risks that you want to highlight as a result of connectivity in the financial services that you have not already referred to?

Simon Chard: I do not think they are additional to those that we have discussed, to be honest.

Q54 **Rushanara Ali:** Simon, you mentioned cloud service provision earlier and, in the report, there are references to overreliance on a few large providers. Can you say more about how much risk is associated with the overreliance on a few?

Simon Chard: There are a number of different risks. The first one is how you transition to the cloud, how you manage what you do and do not put in the cloud, and when and how you do that. That is one key factor that people need to focus on.

There are a small number of firms, but one of the important features is that they themselves have in-built resilience, in terms of operating in lots of different countries, with different types of footprints in different technologies. There is some concentration there but, to be honest, we have experienced levels of concentration in the financial services industry in the past with providers of older types of technology. It is a risk that needs to be managed, but it is not entirely dissimilar to managing that concentration.

Then, to some of the things we talked about earlier, it is about how you manage that supplier and how you understand that. To the point we made before, it is about how you understand whether it is a piece of internal data in the cloud versus customer data, and how that would be impacted if there was a problem with that.

Q55 **Rushanara Ali:** On the issue of substitutability, we saw how things landed with TSB when it is making changes to a new platform and so on. I guess it is a good example of where, whatever substitutability strategy they had, it did not work. What are your thoughts on that? In the report, you refer to not being able to do it en masse and there are different levels at which you should do that. What areas can you point to where companies need to have a more comprehensive process for substitutability versus a more proportionate response? Is it a judgment

call again at the board level, governance level and so on?

Simon Chard: It is around developing innovative scenarios to plan ahead based on the situations that we have seen in the past. The key difference and the key capability that firms will need to develop is more imaginative, more severe yet plausible scenarios, and thinking ahead about how they would substitute for different types of customers, for different services, at different points in time. That is the key behavioural change, perhaps, that we would expect firms to move towards in order to plan for that.

Q56 **Rushanara Ali:** Finally, I have a couple of interrelated points. There is quite a bit of joined-up thinking and working; do you think there should be more? On what the future regulatory framework should look like, I know others have touched on it, but in your report you talk about the third parties that are not part of the regulatory framework of the FCA. What kind of approach should be taken to regulation, given the interconnectivity? One of the issues we have found is the way that, when things go wrong—I am not putting it particularly kindly but, frankly, it is what it is—there is an awful lot of passing the buck. Some of it is not about individuals; it is about the system being set up for different parts of the sector. The public find it very frustrating when things go wrong, because they have to go to different pieces. With technology, it is even more interconnected, so what should updated regulation look like, given your points? Should it be an entirely new way of regulating given the other parties involved?

Simon Chard: From an interconnectivity perspective, firms will and have already started to think about how to plan ahead and understand how they will work with each other in the event of a failure or a problem. In our report, we encourage them, and identify ways in which this can be encouraged by both firms and regulators, to foresee those events, think them through and work together.

From a regulatory perspective, there is a phrase used at the moment, "air traffic control of regulation", which is making the existing regulation work to deal with these threats and opportunities rather than new regulation.

Q57 **Rushanara Ali:** Yes, so which bits need to be improved and worked on to make it work like that?

Marcus Scott: There are sometimes flurries of unco-ordinated demands from different regulators with tight deadlines, which add risks and cost. You were talking about the issue of bringing people to the UK; we can control how we do that to make things work for us. In a sense, we control this, so it is a question of how that is done in the best way possible. The most important thing is to avoid that patching up of old systems at the expense of long-term investment that is going to take us into the future. If there was one thing we could perhaps do differently, rather than

wanting to patch up old systems, it is to look at what the right investment is for the long-term future.

Sarah Isted: On the scenario planning, one of the points in the discussion paper is about organisations looking at impact tolerances for disruption of services, so they can work through what they would be comfortable and not comfortable with in terms of how long a system might be down, for example, from a customer perspective. We comment a bit on that in the report. The scenario planning is key to that. The end result might be a set of impact tolerances, but the process an organisation has gone through to get to them is key, in terms of understanding the different scenarios, suitable alternatives when something goes wrong, etc. That is an important aspect to consider as part of the regulatory agenda as well.

Q58 **Colin Clark:** Your report explains that industry participants are at different levels of development regarding resilience strategy and implementation. To give it context, can I concentrate on one area, open banking, which Simon has already mentioned? Where is resilience strategy and implementation with regard to open banking? My concern is that, when we have heard evidence before about open banking, it seems to be fluid; that is the point. You mentioned third parties earlier, and I am trying to work out how you prepare for something fluid that you cannot predict. Simon already mentioned fighting old wars; so did Rushanara. I am trying to put it in context. How do you prepare resilience strategy and implementation of something that is fluid, where you do not know what it is going to be?

Marcus Scott: I see what you mean. It goes back to what we were talking about earlier on: we need to make sure everyone is operating under the same rules. In other words, if a bank that is operating under a certain set of regulations gives data to a third party under open banking, that needs to be treated in the same way, with the same resilience, the same rules, etc, as it was treated when it was in the bank.

Q59 **Colin Clark:** From my understanding of open banking, it is going to be relatively fluid. People will be coming up with different apps. Bank accounts are going to be sticky or slippery; I cannot remember how they said it. When you say that, are all banks going to be regulated to the same standard in open banking?

Marcus Scott: I think they already are, but it is more about the third parties that are coming in and perhaps wanting to use that data. We need to remember that that is customer data, so it needs to be treated in the same way, whether it is sitting in a bank or whether it is sitting in a fintech or other technology company that does something different with it. That is probably the key thing. It goes back to what we were talking about earlier, assessing where that regulatory perimeter sits to make sure we are treating things in a similar way. It does not really matter where the data is sitting; it has to be treated with the same set of rules no matter where it is located.

Q60 **Colin Clark:** Can I put the same question to you? Is there a trade-off of customer convenience and financial security? Is that not the nature of open banking? Is that not the problem of regulation? How do you know? Customers want greater and greater convenience, but nobody really points out to them the financial risk they are taking, because it is way beyond mere mortals, including me.

Simon Chard: It comes back to the point of understanding where data, for example, is being held, and the clarity over who has responsibility for the data and the standards in relation to that.

Q61 **Colin Clark:** In your own report, you say, "Embracing greater integration without resolving complexity makes resilience more difficult to achieve". That is what I am trying to get at. You have spoken about operational resilience, but in something like open banking, which is going to be fluid, how do you plan for that?

Simon Chard: If you are talking about a current account, for example, you break it down. We would think of it as less about open banking than about what service is being provided to the customer. There will be a situation where that is a very straightforward service provided by a bank to a customer. Then there are more complex situations, as you say, that may be fluid, where different parts of a service may be provided through another bank or another third party. We believe the principles of operational resilience equally apply to that, because you need to understand the nature of the service, who is providing it to whom, at what time, and take accountability and responsibility, back to the point on the senior managers regime. Those principles are the same whether it is you, another bank or another third party undertaking it.

Q62 **Colin Clark:** So there should not be a risk of trading off customer convenience for financial security.

Simon Chard: I think that is right.

Q63 **Colin Clark:** Take faster payments, where money moves immediately whereas before it took 24 or 48 hours. That has created great convenience, but it is part of the cause of £380 million of financial fraud last year. If armed robbers stole £380 million, there would be armed guards outside all our banks. I am just trying to work it through. I have heard what you have been saying about operational resilience, and it sounds like much of it is about very well-organised, terribly honest companies. Sarah, you used the term "humility", which I thought was interesting in banking; I have far too many friends in banking, obviously. I still cannot quite get to the nub of how we stop offering customer convenience that poses a risk to financial security.

Marcus Scott: If the customer convenience is being offered by a well-regulated firm, everyone can be very happy that that is—

Q64 **Colin Clark:** Is there more of a risk as we go to third parties?

Marcus Scott: There could be, but the regulator is very well aware of that. A big focus of the work they have been doing with the sandbox and Project Innovate for a number of years now, particularly in the sandbox, is making sure that there is no customer harm and that, as these companies go through this process, it is well understood how the customer needs to be protected. That is a fundamental part of what firms go through. If firms are consumer-facing, that is well understood and very well regulated. We are possibly talking more about those areas where it is not customer-focused and there is new technology coming in. We need to make sure that that new technology is resilient. It is not subject to perhaps the same regulations because it is not consumer-facing, but it should be subject to the same operational resilience standards.

Q65 **Colin Clark:** Your report explains that there is a business imperative to address operational resilience issues, which you have discussed. Why has it not driven sufficient investment to date and is that a risk?

Marcus Scott: This drive to renew technology and bring it up to date has been a huge focus of the banks and most of the other asset managers, insurance companies and all sorts of companies. They are all making big investments in these future technologies. That has been going on, but at the same time they have been in the situation where they have had to either maintain or continue to service some of the legacy systems. The sooner we can move away from patching up old systems to long-term investment in the new systems, the better off we will all be. One of the reasons that new entrants are coming into the industry is that they do not start off with those legacy systems, and can come in and offer things at a lower cost. That is exactly as it should be; we want to encourage that. Many of our member firms want to be in a position where they can also update their technology, to provide a lower cost offering.

Q66 **Colin Clark:** On that point, PwC gave written evidence saying, "Most major financial institutions have attempted to cut costs significantly and this, in our experience, has resulted in reduced expenditure on technology upgrades and other important infrastructure improvements". Is there a risk of underinvestment?

Simon Chard: There is a risk of underinvestment. To the point you made earlier, we are starting to see, in the recent data we have, that firms are starting to invest more, particularly in technology.

Q67 **Colin Clark:** This is what I am really trying to find out: using a car analogy, does open banking have seatbelts and airbags? I do not think we have built the car; we cannot quite work out if it has wheels or it flies at the moment.

Marcus Scott: I do not know enough about the open banking system to give you a comprehensive argument, but I know that, when the open banking regulations and structure were developed, this idea of consumer protection was at the forefront, very obviously, because it would have to

be. I do not know enough about it to give you exactly where that sits, but I would find it very hard to imagine that that had not been a central part of the whole process.

Q68 **Colin Clark:** It is just because it is so much more fluid. I am sure you would agree it is much easier to regulate something that is rigid, with frameworks, corners and edges. I can see that, but when something is fluid I struggle to understand how you regulate it.

Marcus Scott: The principle we think should be adhered to is that, no matter where the data is, no matter which provider has it, you always have to treat it in the same way. It is customer data and it needs to be protected.

Chair: I expect you have triggered a whole avalanche of written evidence that is going to come in from the open banking industry now, which is not a bad thing in itself.

Q69 **Wes Streeting:** I want to pick up on this point of regulation. The report explains that industry participants are at different levels of development regarding resilience strategy and implementation. Could you elaborate a bit further on the patterns of variation, in terms of types of firms, to what extent that variation exists and why that variation exists?

Simon Chard: One feature that we bring out, in terms of the patterns, is that, unfortunately, those firms that are more focused on operational resilience have experienced a significant failure in the past. There is another pattern: we talked about the "dear chairman" exercises in 2014 and 2015; those exercises were focused on the big seven retail deposit-taking banks in the UK exclusively. That forms a pattern where some of those firms were quite directly encouraged to focus on these activities within banking.

There are those two patterns, and the third one is probably related to the first. The reason we are encouraging more scenario planning and forward thinking is that, when firms that have not suffered a great deal in the past are hit with something, particularly something unexpected and externally generated, it becomes very difficult for them to deal with.

Q70 **Wes Streeting:** Yes, and that goes on to my next question. Are we not in a position now where we are waiting for firms to make mistakes before they start thinking about resilience? Should we be doing more now to prevent firms being in that position? On a directly related note, your report states, "Proportionality is essential, given the proposals which apply to all firms, whatever the size". How are you judging proportionality?

Simon Chard: Our view is that the themes of the discussion paper and the drive to operational resilience are reasonably proportionate by design. If you are a very complicated firm with lots of different services that you apply to lots of different customer groups, you will need to do more work to understand the criticality of those services and the technology and

people that support them. If you are a simpler, smaller firm that perhaps has two or three services, simpler technology and a simpler set of people and third parties, you have less work to do. From that perspective, we feel that there is that level of proportionality in the approach.

Q71 **Wes Streeting:** The regulator's discussion paper recommends that firms establish impact tolerances for disruption to their services. I am interested, from your discussion with firms, in the industry's view on how they might practically implement that recommendation. Are we at a point where we think we need a technological resilience strategy or test similar to the broader stress testing we put banks under?

Simon Chard: Yes, we anticipate stress testing to move from purely financial to operational activities. That has been indicated in various papers and regulatory announcements. We do expect that.

Q72 **Wes Streeting:** You are expecting it and your members, Marcus, are probably also anticipating it for the same reason, looking at the papers, but how will it be viewed by the industry bodies?

Marcus Scott: We have a very clear steer from the regulator that this is going to become the third major pillar of regulation. Therefore, it is always going to have some kind of regulation and teeth that go with that. Whatever testing environment that comes out of that, we understand that that is going to have make sure that firms are in a sufficient position. We have seen that with various different things, like CBEST for cyber and the stress testing on different companies, and it seems like a normal part and parcel. The question is going to be where you set that, and I am sure that will emerge over time, as to what the stress tolerances and stress limits are going to be. We are not there yet. I do not think anyone particularly knows that. I do not think that has already been determined, but it will be the outcome of this work that the regulator is doing on it at the moment.

Q73 **Wes Streeting:** What about the fitness of the regulatory requirement/responsibility burden, depending on your perspective? Is the volume of regulation in the right place? Is it precise? Does it need further clarity? How might the regulatory burden help or hinder firms' operational resilience?

Marcus Scott: Where it focuses on patching up legacy systems, it is not helpful. Where it focuses on long-term resilience by investing in new systems, it is much more helpful. It comes back to this air traffic control concept that the Chancellor and the Bank of England have talked about recently, of making sure there is a co-ordinated approach in the same way that operational resilience is a co-ordinated approach across a company, focusing on the customer. Making sure that there is a co-ordinated approach that means regulations are not piling up on top of each other, with deadlines coming in and creating additional risk, is important as well. Both of those things are welcome.

Q74 **Wes Streeting:** Is that your view?

Simon Chard: Yes.

Q75 **Wes Streeting:** Good. The regulator has put out a joint discussion paper, but I wondered if, more generally, you think there is a need for greater co-operation between UK regulators in their approach to operational resilience. Obviously, the fact that they are talking about these issues together is a positive sign, but beyond a broad policy debate, on a practical level, is there sufficient co-operation between regulators in this space?

Simon Chard: In this space, yes. With the regulators coming together to produce the discussion paper, holding roundtables with firms, et cetera, and joint representation from different regulators, in this space, there is a level of co-ordination. That will be proven or otherwise when the consultation paper lands later this year.

Q76 **Wes Streeting:** A number of times in your answer, you emphasised "in this space". Are there other spaces where there ought to be greater co-operation between the regulators?

Marcus Scott: What we have seen is between the PRA, the FCA and the Bank of England. When we talk about "this space", that is essentially what we are talking about. Many of our member firms have up to nine regulators, including the Information Commissioner's Office, the Payments Regulator, et cetera, and that is quite complex. It becomes more complex the more additional regulators you have. In terms of the regulation we are seeing in this space, between those three bodies it is working brilliantly. Where there are multiple regulators all trying to achieve different things, for perfectly good reasons, it becomes more difficult and that is where the system of air traffic control would be very useful.

Q77 **Wes Streeting:** Broadening out this conversation to other regulators that might have an interest, even if it is a passing interest, would lead to a better experience for firms trying to navigate their way through the regulatory environment.

Marcus Scott: Yes. I am sure that additional operational resilience is going to achieve some of the outcomes that other regulators have.

Q78 **Wes Streeting:** One of the other things your report recommends is that regulators should consider recruiting more senior advisers and staff with operational experience. How did you reach that conclusion?

Simon Chard: In relation to the other pillars of regulation we talked about, we see this as quite a broad discipline in itself. We have talked about cyber, third parties, data, and the framework outlines 10 of those to start with. We are experiencing, in discussion with firms, that they would appreciate being able to have a discussion on those topics and more resource within the regulator to discuss those topics with them. It is based upon that.

Q79 **Wes Streeting:** Your report recommends that the regulators create a map of the financial sector. Can you explain what you mean by this and how you think it would help improve the monitoring and management of interconnectivity and concentration risk?

Simon Chard: Yes. We talked earlier about 59,000 firms in the UK financial services sector, but of course many of those are very small and a great deal are very large. In our view, coming back to scenarios and to interconnectivity, a better understanding at a high level, not at a very detailed level, of the key flows and interrelation between firms can only improve the way in which firms work together in scenarios. There is work there for the regulators and, as you say, there is a recommendation in the report. It is also going to be a by-product of firms thinking more outwardly to who they work with, which would help give the colour to that map as well.

Q80 **Wes Streeting:** Would you share that view, Marcus, or has PwC come up with a very creative pitch for more work on behalf of the regulators?

Marcus Scott: It is important, what those interconnectivities are, and it comes back to the regulatory perimeter we talked about earlier on. Because things are evolving so rapidly, with new technologies emerging and then being deployed by companies, the providers of the different functions within an organisation are often evolving fairly quickly, so I would agree that it is probably an ongoing and dynamic thing. Obviously, it is a good thing that there is additional work for PwC, but it is very much an ongoing and dynamic thing that we need to look at, because there are those dependencies we need to understand and we cannot do it without understanding them.

Q81 **Wes Streeting:** Okay, that passes the test in that case. There are two final things I wanted to pick up on. One is perhaps directed more to PwC this time, because I do not find financial services always demanding more powers for their regulators. Do regulators have the powers they need where risks are outside their current remit? Do we need to look at the ambit and scope of regulatory powers in this space? Broadening out the question to all of you, how do we compare with other countries and where might we learn from other countries in terms of good practice?

Simon Chard: To take the first part, we need to understand more about the interconnectivity first and then understand where the perimeter of regulation is in relation to different types of firms. If you look back, firms have occasionally been brought in to the regulatory perimeter over time. Our view is that you need to do that understanding where the map is, where the participants are and where the risk is. We certainly feel that it may be a consequence of that that the regulatory perimeter is moved or other firms are brought into that.

We have covered the scope. If that is the scope, I suppose we have covered the regulatory question, which is that they have the tools and the mechanisms to monitor and drive operational resilience.

In terms of other countries, we know that there is, for example, a working group of different regulators on this topic. One example where the UK regulators can learn is about the different threats that operate in different geographic territories and jurisdictions. That is a good example of where there can be that learning.

Marcus Scott: I completely agree with Simon. There are always things that we can learn from other regulators. We have been very lucky in this country that our regulators seem to have been at the forefront, with things like the sandbox, Project Innovate and now this with operational resilience. But it is going to be about building coalitions at things like IOSCO, Basel and the Financial Stability Board, which will make it useful to companies that are operating internationally.

Q82 **Wes Streeting:** I promise this is a final question. I am just curious, because this is a big theme of the report on operational resilience, but it applies more broadly to financial regulation. We have a world-leading industry here in the UK, which is also a world leader in shaping the direction and discussion of global regulation and trying to establish a common understanding on issues like standards, culture and the rest of it. You are doing that at a time when the political tide is for nation states to claw back power and emphasise sovereignty. Have you seen examples yet of that kind of nativism creeping into regulatory conversations or do you think that, for now, partly helped by the fact that it is quite hard for lots of people to understand exactly what you do and what it all means, financial services regulation is elevated above that political fray? Is it a concern to you that you might get pulled in, with unintended, unhelpful and harmful consequences either to our industry or particularly to the consumers who rely on your success?

Marcus Scott: We have not seen that. We have seen, so far, really good international co-operation at both the college of regulators and the various different bodies that I have talked about. It is true that international forums like IOSCO were not as strong when there were big blocs like the EU operating as one unit. From the UK's perspective, we are going to need to get better at building relationships with those international forums if we want to work out the best way of doing this and co-operate with other people. But we have not seen that nativism, as you described it, creep into the discussion so far. I cannot predict whether it will, but I certainly hope it does not.

Q83 **Chair:** That is very helpful. I have two final questions. On the stress testing that Wes was just talking about, and the development of that, the way capital stress testing works is to give the banks various scenarios and see whether their balance sheets can cope with them. Given what you have said this morning about the importance of third-party organisations, do our regulators need to find a way to stress test not just financial institutions in London, recognising that some are part of global institutions, but potentially some third-party providers, like the cloud services, for example? It might be nothing to do with a financial

institution, but a cloud service provider goes down and that proves to be devastating. Is it sufficient just to test the institution and ask, "What would you do if your cloud provider went down?"

Simon Chard: You could approach it in either way. We would anticipate, coming back to the accountability piece—this tends to be the way that the regulatory regime works—that you would do it through the responsibilities that the bank has and through their senior managers.

Q84 **Chair:** Yes. More broadly, thank you very much indeed for your evidence this morning; it has been very helpful. Is there anything else from your report that we have not picked up? Any other areas on which you think we should be asking questions of our next sets of witnesses, who are going to be grilled, as you are, but probably in those seats rather than around the table?

Marcus Scott: From my perspective, no. We have covered everything in the report. Thank you for giving us the opportunity to come and discuss it with you. We would be happy to provide any further information that you need.

Sarah Isted: It is the same for us. Thank you very much for the opportunity.

Chair: Thank you very much indeed for your time this morning. It is much appreciated and we will look forward to future sessions. Thank you.