Transcript: Operational Resilience and Outsourcing – New Expectations

Nick Dent: Good morning and welcome, my name is Nick Dent. I'm your host today, although I won't be speaking that much, I think we'll leave that to the experts Julie and Lindsey who I'll introduce in a second. But as you as you realise, we're here to talk about operational resilience and outsourcing today. I mean, kind of needless to say maybe it's obviously increasing up the regulatory agenda, we are, of course, really interested in the fact that the regulators the FCA the PRA and the Bank of England are coordinating their approach to this topic.

So that's intriguing and I know we'll mention that and draw on that a little bit during the session as we go through, with a view towards, you know the coming years and the legislation that's yet to come. This is an interesting and timely time to be talking about this topic, and I'm joined today by two highly experienced and knowledgeable individuals into indeed if, if there was an Olympic event if I could make that analogy in knowledge about governance, risk and compliance two speakers today would certainly be on the podium. So we're joined today by Lindsey Domingo. Lindsey is a Senior Director at Xcina Consulting and Lindsey has been advising on governance, risk and compliance related issues in the UK but also in Europe and across Africa as well over 29 years now, and we're also joined by Julie Pardy, Julie is our own Director of Regulation and Market Engagement at WorkSmart.

Julie Pardy: You know a huge welcome to Lindsey, for joining us for this event and sharing his time. We met Lindsey at a previous regulatory event and we're very impressed by his knowledge and experience and felt because this was such a relevant topic that we'd ask him to join us. And on that note, I will hand over to you to kick off this event for us Lindsey.

Lindsey Domingo: Thank you Julie and thank you Nick for the kind introduction and good morning, everyone. Really pleased to be here today. We have quite a large and diverse audience of dual regulated, as well as solo regulated firms of different sizes and sectors, and those who joined at the beginning about heard from Nick that we're really pleased to have over 200 participants today. I also expect that the firms represented might be at probably different levels of maturity with respect to the topics that we're going to have on the agenda today. So what I'm aiming to do is give you a whistle-stop tour of the key expectations for operational resilience, outsourcing and third-party risk management, and then talk about what firms should be doing. Next slide please.

So as background and context and Nick also alluded to this, operational resilience is a key priority for the Supervisory Authorities in terms of putting in place a stronger regulatory framework to promote the resilience of firms as well as Financial Market infrastructures. So, in terms of context, the PRA, FCA and Bank of England issued their discussion paper in 2018 followed by consultations in 2019, and at the end of March, they issued their joint covering document, with their respective policy statements so that means we are having to address both PRA and FCA requirements on the same topic. The PRA also issued their policy statement on outsourcing at the same time.

And, from the regulators' perspective, the objective of operational resilience really is to improve the market as a whole, by focusing on each individual firm with a continuous improvement mindset and operational policies complement various existing requirements. Those include recovery and resolution planning, operational continuity and resolution resolvability assessment framework, as well as business continuity planning. They also complement other EBA guidelines, notably on IT and security risk management and outsourcing arrangements. Again, what we are doing here in the UK is not in a vacuum because it is aligned with parallel developments and convergence at international level. You know, we have the Basel Committee who came up with their guidelines, two days after, after the PRA, the European Commission brought out DORA and the US also have their paper on operational resilience that came out in October last year. So, there is some consensus that operational resilience is not just a regulatory exercise but really a better way to run the firm that can help improve controls and also lead to better outcomes for customers and for the market. Not least, in the light of the pandemic, which has brought operational resilience to the forefront of everyone's thinking it's imperative for firms to take a proactive approach to operational resilience.

Julie Pardy: Thanks for that Lindsey and I'm wondering if now is the right time to get your audience involved, and set the first polling question. Okay, right, so what I'm going to do for everybody on this if you watch your screens. I'm going to launch the first polling question., and really this is just, we want to get you involved we know for feedback that we've had that, you get value out of our events when you get to have a voice, to put some commentary, ask questions and just generally put observations. So this is all about trying to understand **what stage you and your organisation are at with regard to this preparation**. So, I would encourage you, I know not everybody feels that they like to vote at these events but if you do feel able to share where you are. It's just really so we can gauge that you know where, where people are at this stage, and it's also helpful. Obviously for Lindsey's work he will share with you some anecdotal information about, you know, working in this marketplace but it's good to see where you are. From your perspective Lindsey, I'm giving people, you know, a good 90 seconds to vote because some people will want to think about this for a while. Some people may not know exactly the full position in the firm but I'm just wondering, what you would expect to see for your work in the market where do people tend to be at this point in time because I think people gain comfort in knowing where they are in relation to others.

Lindsey Domingo: Yes absolutely, I think. I think there's quite a range in the sense that some of the larger institutions started working on operational resilience programmes, even before the regulatory guidance came out, so already when the first discussion papers, came out some of the larger let's say systemically important institutions already started working on that. Therefore they may be relatively advanced in comparison to some of their peers. In contrast, I think some of the perhaps smaller firms or newer firms may tend to use regulation as a catalyst to begin development, and therefore they may have made less progress on that on that topic. So, we see quite a range depending on the size and maturity of the institution, you're talking to.

Julie Pardy: Absolutely, well shall I end that polling and share results so you can look at the results and see what their peers have said. I suspect if we asked you to, to say which one you've thought everybody would be at, does that reflect where you think generally the market itself is at the moment?

Lindsey Domingo: Yes, I think it does because, as we're going to see, you have to get through these steps one by one, and the first parts are probably quite time-consuming and resource-intensive so it doesn't surprise me altogether.

Julie Pardy:

I think we've got a few individuals as well, that have wanted to give a different answer, which we see on the screen, and I think looking at the comments. Some organisations are saying, No, we're actually, we're at the pre stage, so we're not at point one, we're at the point before that. So, I suspect from your perspective you're saying, you already alluded to the fact that there's an awful lot of time and effort that needs to be involved in this. So, you know it's interesting to look at the timelines that you're going to share with us later on, for when certain things have to be done.

Lindsey Domingo:

Absolutely.

Julie Pardy:

And so, okay, thank you everybody for getting involved in that and hopefully just seeing where everybody else is, is of some value to you I'm going to stop sharing the results now for that particular poll, and I'm going to move on to the next slide for you Lindsey.

Lindsey Domingo:

Okay, let's look at some definitions, just to make sure we are all on the same page. So operational resilience - I've put here the definition which is the one used by the Bank of England, the PRA and the FCA - is the ability of firms financial market infrastructures and the sector as a whole to prevent, respond to recover and learn from operational disruptions. And examples of Operational disruptions can be anything really, from market instability, cyber-attacks, geopolitical events, third-party supply failures, system outages, natural disasters such as pandemics, fire, floods. The regulators' approach really recognises that you cannot have full contingencies for every vulnerability, disruptions will occur. So, it's not about focusing on preventative measures to reduce likelihood here. Rather, the focus is on recovery from a disruption which has already crystallised. Resilience as such is not an entirely new issue, but traditionally it was managed with a narrower focus, for example looking at disaster recovery and business continuity planning, often at a business unit or asset level. And the key difference is that operational resilience is really end-to-end, and it's broader than just technology. In addition to that, it's also outward facing so it's focusing not on the firm's own business objectives but rather on the regulators' objectives. In other words, focusing on what the impact is on the clients, what the impact is on the markets, rather than, what does it mean for us internally. Operational resilience considers how the fundamental capabilities of the firm, in other words people, processes, technology and third parties, would allow that firm to adapt and to recover when things go wrong. A business service is the service which the firm provides and which delivers a specific outcome or service to an identifiable user external to the firm. So we're not looking at internal services here. And also, in terms of granularity, it should be distinguished from business lines which could be more like a collection of services and activities.

Important business services and impact tolerances are really the cornerstones of operational resilience, which is why those take probably the most amount of time. To define important business services, those are basically services provided by a firm, which, if they are disrupted would pose a risk to the firm's safety and soundness, or to the financial stability of the UK market. So that's the PRA's definition. We also have to address the FCA definition, and they're important services which, if they were not available, would potentially cause intolerable harm to consumers of the firms services, or the risk to market integrity. As far as impact tolerances is concerned, this is the maximum tolerable level of disruption to an important business service on the assumption that

there is a disruption to the supporting systems and processes. So, basically how long or how far can you survive without that particular piece being up and running. The definition of consumers here, referring to the FCA definition of important business services are the direct consumers of the firms services, or those who are in other ways, dependent upon that firm's services so that would include both retail and wholesale market participants.

Julie Pardy: so can I ask you Lindsey, just from the work that you've done in the marketplace, around the import business services can you give us maybe a couple of examples of the sort of services that people are identifying as being those important services because, certainly from the conversations we've had, and the potential impact this has on us as a supplier there are very different schools of thought on this?

Lindsey Domingo: Okay, I'll give a couple of this probably basic and simplified examples but just to illustrate. For example, if we're looking at retail bank, they might consider that the dispensation of cash from their ATMs would be an important business service. Because if their customers are not able to withdraw cash that could cause harm to them and beyond a certain point, which needs to be defined for example, if they decide it's four hours, four hours could be then the impact tolerance for that specific important business service. Another example might be, let's say we take a car insurer. The car insurer might consider that the handling of its customers' claims would be an important business service because for example, if customers cannot get their claims in, they might be stuck without a courtesy car, and that could cause harm to those customers. For example, they might decide that two days maybe might be the impact tolerance they would be prepared to accept. So those are two. Obviously depending on the business model you're going to have different ones, but these would be a couple of examples.

Julie Pardy: I think that's really helpful, and I can actually see that already the comments that you're making on the slides as we're going through. We've got questions starting to come in and we've got comments and observations. So, for those people that are asking questions, please bear with us, because we will do that question piece at the end if we feel we're able to answer it at this point. That's really helpful, thank you should I move on to the next slide for you?

Lindsey Domingo: So, in terms of scope as to who is impacted by these operational resilience policies coming from the regulators? The following are in scope: UK banks building societies and PRA designated investment firms - let's call them "banks", including subsidiaries. Then Solvency II firms Society of Lloyd's and managing agents ("insurers"); recognised investment exchanges as regulated directly by the Bank of England. And then on the solo regulated side, we have enhanced scope SMCR firms, as well as payment services and e-money institutions. So those are in scope of the operational resilience regulations. For those who are not in the scope, for example core firms under SMCR, I think that, given recent events and potential future regulatory focus, they would probably benefit from familiarising themselves with the regime. Also those who may not themselves be regulated, but are providing services to a firm which is in scope of the regulations, they may also be impacted because they will need to demonstrate that they have resilient processes to support their client firm. So, irrespective of the above all firms should also continue to meet their existing obligations, e.g. business continuity, outsourcing and information security as well.

Julie Pardy: Can I pick up on a point with reference to those that aren't in scope, and this is really interesting. So, we're saying that those are not in scope, for example, the core firms under SMCR. But this point around familiarisation, do you sort of get a feeling for any move in the market in terms

of those types of firms or are they just really keeping a watching brief on this at the moment as opposed to acting on it?

Lindsey Domingo: Okay I think, what we're seeing is probably a bit of a mix. Most firms not in scope, are at least making themselves aware. And as evidence of that we have we have many of those firms in the audience today. They are not necessarily following the letter of the policy. However, we're finding that many are adopting the principles as good practice, and, and one of the reasons for that is because they all have an overarching requirement to implement appropriate systems and controls to avoid going through customer detriment. So, and the pandemic has reinforced that, therefore, what the operational resilience policies are providing are good practices in terms of how to achieve that. Just because you're not strictly required to do it doesn't mean you cannot by yourselves, and some firms are doing that, so they're also following the evolution because they expect that sooner or later that they might be put in scope as well. And I guess the one, maybe one notable exception, perhaps, is third country branches so if you saw on the slide. I emphasised the fact that subsidiaries were in scope. Strictly speaking, if you follow the letter of the regulation. 'Third Country branches' are not in scope because they are not CRR firms. However, on that one. The regulators have stated that, as part of their supervision, they would expect the third party country branch, to be able to demonstrate how they are meeting the outcomes of the operational resilience policy.

Julie Pardy: It's interesting, isn't it? Thank you ever so much for that. That's hugely helpful but as you were talking, I was thinking about, you know parallels with other regulation and a really simple one, we've observed is the training and competence regime. And, you know, within the training and competence regime only applies to certain organisations that do certain things, but actually what we've noticed is, that at times, there's been a trend for firms that don't need to do it to absolutely mirror it for exactly what you said that you know there's a lot of good common sense, and there's a lot of good practice in some of these regimes that don't apply to firms, and so there can be a move some time for people to pick up and follow that best practice approach. The next slide for you.

Lindsey Domingo: Thank you. Okay, let's have an overview of the main requirements, and I will go quite quickly through those and appreciate that some people may already be aware of those. Okay, so in terms of the framework, operational resilience is what you would call an overarching framework which brings together a number of other existing frameworks within the firm, including risk, security, business continuity management, crisis management, third party risk management. It's end to end, holistic and dynamic.

Important business services, as we've seen from the definition. We're talking about intolerable levels of harm for customers, not just inconvenience to consumers, threatening firms' safety and soundness and risk to UK financial stability. So, this means the bar is actually set quite high. When it comes to identifying important business services firms need to identify all their business services and then shortlist the ones which would have a severe impact based on the definitions we have provided. So, this means that the list of important business services would a relatively short list of external facing services. So, from my experience, at least six to ten important business services seem like a reasonable ballpark figure. Obviously depending on the firm's complexity, products and markets but it's not the intention that it covers everything the firm does. So, if you got 30 important business services, it might be worth looking at that again. And firms are expected to review that list of important business services at least once a year and whenever there's a relevant change to their business or to the market. Impact tolerances are expressed by reference to specific outcomes and metrics, and those should always include a time-based metric.

So, therefore, the maximum tolerable duration and firms can also include other considerations such as the volume of disruption. For instance, the number, or types of consumers affected or the measure of data integrity. Dual regulated firms specifically are expected to set up two impact tolerances for each important business service in line with the statutory objectives of each regulator. So that would mean for each important business service two impact tolerances, basically one for each regulator.

Mapping. The end to end mapping of resources and capabilities for each important business service is really a critical foundation to allow us to then do scenario testing. It's probably the most resource intensive part of the exercise in a large complex organisation. The objective of the mapping is to allow the firm to ascertain whether the supporting resources - the people, processes, technology, facilities and information - are fit for purpose, to allow them to identify new vulnerabilities and to consider what would happen if those resources were to become unavailable. And as part of doing that exercise firms may be able to leverage some of what already exists. For example, scenarios used for stress testing, any process maps they have, any business impact analysis they have done when doing business continuity planning. They may use this as a starting point but they will need to build on those further. So, when it comes to scenario testing this is really about testing the firm's ability to remain within the impact tolerances in severe but plausible disruption scenarios. The focus is on recovery and response arrangements. For example, if your cloud provider, whether you're using AWS or Azure goes down, what happens next? And third parties are part of your end-to-end process, and therefore they need to be prepared to support your operational resilience testing, and that may not always be an easy conversation. It's also I think important to emphasise that it is not necessarily the objective of scenario testing to try and prove that, regardless of the scenario, any important business service can always be maintained within tolerance. But rather the objective is to try and understand, under which scenario is the firm would not be able to recover the important business services, and it is then those scenarios that need to be discussed with our board and senior managers to determine is it acceptable or not in their view, for the firm, to be able to recover those with an impact tolerance. And if it's deemed that it's not acceptable, then they must determine and prioritise investment decisions to allow recovery within tolerance.

Then you need to conduct lessons learnt based on the scenario testing you've done; you need to develop internal and external communication plans. And then there's this key piece, which is the self-assessment. The self-assessment is a comprehensive document. And the whole purpose of it is really to articulate what the firm's resilience journey has been, in other words, the work that has been done over time. To demonstrate the operational resilience, as well as their plans to remediate any vulnerabilities and findings, and what that document needs to contain is the approach taken to service definition and prioritisation resource mapping, how they've gone about developing and testing scenarios, how they define their impact tolerances. It needs to list the important business services and their tolerances, include the mapping of all the results, resources, the scenario testing plans and results. The lessons learnt, any appropriate remediation plans, and also which scenarios, if any, would the firm not be able to recover within impact tolerance. So, it is quite a comprehensive document, and it will take some time to produce and there may be a few iterations. The board is accountable for, and should approve that self-assessment document as well as demonstrating that prioritised investment decisions are being made to address any gaps. The board will need some time to reflect on it and before they sign off so it will probably not be advisable to, you know, to give it to the board, and on the 25th of March next year so I'm not sure that that's going to receive a warm reaction.

Looking at governance. As I mentioned, operational resilience is a priority at the board and executive levels. The board must approve and regularly review the firm's important business services, impact tolerances , and as I mentioned the written self-assessment. It is really important to get the accountability and the mindset right because those are really fundamental, particularly at the level of senior managers, especially the SMF24 who tends to be quite involved and have more overall responsibility in their statement of responsibilities, and also at board level. And in terms of governance and oversight, what we're finding is that many firms are looking to apply a proportionate approach, using the existing risk governance framework and committees where possible. But we've also seen that some are, for example, setting up specific operational resilience committees that would address all things relating to operational resilience, recovery and crisis management, etc.

Julie Pardy: Again, it's a great overview of what the requirements were and I know when we were talking about this earlier, very specifically on this point of board and senior manager, but that sometimes there are so many regulatory papers that come from the PRA and the FCA it's hard to see everything, but there were two that we felt would be very relevant here and again we can put these in the Q&A document. And this is the thing where you may or may not be familiar with, with this from an audience perspective where the FCA will write their Dear CEO letters, and the Dear CEO letters are basically when they've got something on their mind, that you know they're really worried about something, and you may not necessarily have looked at these because they were very specifically focused on platform firms, but I think it's always good to see what they're talking about and very specifically they published a Dear CEO letter last month. And they referenced a Dear CEO letter that they published back I think was February or March last year, and they were talking about some issues that happened with platforms back in November, when there have been some peaks in trading and platforms that had some problems and therefore retail consumers were affected. But I think, have a look at those if you get time because there's a very specific piece about technology and operational resilience, and how important it is to the regulator that not only should firms have got those within their within their documentation overview, but where they should be giving them a regulatory report where something really is happening that that the FCA needs to know about how they've also alluded to the fact that they're not also being told what they should be told. So we'll share that afterwards but I thought it's quite interesting that you know we've got these policy statements that the firms are working with, and it's still enough from the regulators mind that they're actually writing to the CEOs of certain companies saying, Look, we're really worried about this you need to reassure us.

Lindsey Domingo: Yes, and I would have certainly echo that it does reinforce the message that this is a really a priority for the regulators.

Julie Pardy:

On to the next slide for you.

Lindsey Domingo:

Okay, timeline, so the effective date for the operational resilience policies is the 31 March 2022. So what does this mean? So before 31st March 2022, firms must have identified and mapped their important business services, set PRA and FCA impact tolerances for each important business service as appropriate (obviously if they are solo regulated you just need to worry about one of them), carried out their mapping and scenario testing, identified any vulnerabilities in their operational resilience and defined a prioritised plan to address any vulnerabilities, and also set out how they

plan to comply, no later than 31 of March 2025 for being able to manage to stay within impact tolerances. So, the self assessment should also be documented signed off by the board and ready for the regulators.

After 31 of March 2022 firms, will then need to review the important business services at least annually, and whenever there's a material change. And as soon as reasonably practicable after 31st March 2022, on a risk basis, and no later than March 2025 firms must be capable of maintaining all the important business services within their respective places in severe and plausible scenarios. So when I say on a risk basis, probably, the systemically important institutions, for example, I doubt that they will be able to wait until March 2025 they will probably be under greater regulatory scrutiny to have everything addressed sooner rather than later. And of course, depending on what the issue is some firms may or may not get, much time within that that three-year window. Hence all firms must have made any necessary investments and remediation, to allow them to operate consistently within their impact tolerances. And after, after March 2025 maintaining operational resilience becomes a dynamic activity, all firms should then have effective strategies, processes and systems in place to manage operational resilience. Now, I'd like to emphasise that operational resilience is a journey, and it's also an iterative learning process and you've got to give yourself time. There's a lot to be done by March 2022 but not everything, and regulators are saying that clearly as well they expect the mapping and the testing of important business services to evolve, and to become more sophisticated over time. So, what do we need by March 2022? It needs to be sophisticated and granular enough to be able to set out your gap analysis and identify what are the major shortcomings, and what are the areas where you're going to need further work to be able to make sure that you can stay within impact tolerance. So, it doesn't have to be perfect and it cannot be perfect by March 2022. However, regulators expect it to be done thoroughly enough so that you're able to identify what your gaps are and set out your remediation plan, even if it will become more sophisticated over time.

My conclusion as an operational resilience would be that it's quite a daunting task, not to be underestimated. So, give yourselves enough time, and hopefully, you should have some assets in the organisation that you should be able to leverage as a starting point and it's about being pragmatic and proportionate and taking one step at a time.

Nick Dent: Can I just interject there, just one point of clarity I can see in the chat here that there was a there was a bit of a challenge about the testing of the IBS' and the deadline of March 2022 when there seems to be a bit of concern that that deadline isn't necessarily set as being clear, I can see people responding to that already that your view of that, the scenario testing by that deadline.

Lindsey Domingo: There are different ways of doing scenario testing, I mean, based on our experience and what we've seen so it goes paper based desktop exercises through simulation exercises to real life testing right, people are not expected to have done the full sophisticated detailed level. However, you need to have done sort of testing to be able to validate the assertions that you're putting in your self-assessment to say, because the regulators will say, where do you draw your confidence and comfort that you are or not able to stay within those tolerances? Which is then going to define what you need to work on going forward because that plan of what you need to work on has to be part of that assessment. So, if you haven't done any scenario testing whatsoever, and I'm not talking about how you do the testing, as I said, there are some lighter ways of doing the testing and some more sophisticated detailed ways which would involve other market participants as well but you need to have done some sort of measure or degree of testing. In order to support the assertions you're making your self assessment document, and what you've done in testing has to be within the self-assessment document as well.

Julie Pardy: Hopefully that clarifies, because you have a hard time going through all the slides and talking to all the points, I can see in the chat, there's been a variety of discussion points by delegates and so we're getting a breather in a minute so you can catch up in the chat but thank you for that, that's, that's really helpful. And I think when we were talking about this before we were talking about, you know, as suppliers to the financial services industry. It's interesting when this regulation is arising and it's moving, and we wanted to get a view on just really what the delegates, think about **how that impacts and outsourcing and third party risk management**. So, what I'm going to do is launch a poll and get everybody involved, once again, where we're going to ask people to have a think about this. Because actually, my observation to Lindsey was that, sometimes, as we've seen with other pieces of really important regulatory change firms go over and above what is required, which is why I asked the point about core SM&CR firms, and we have definitely seen a big increase in what's being asked of us and that's obviously fine because firms need to reassure themselves that they're the right partner for them in a particular scenario, but actually you can see that there will be unintended consequences. And I think here with this we're just looking to get a view really from the audience that, you know, there's always risks involved in the process and which is why we've got some of these things up here, from your perspective Lindsey. If any of these resonate with you. You can see in that poll there.

Lindsey Domingo: Yes probably a few, actually, I think. I think my view on this would be that you know the cost of risk management and compliance are part of the costs of doing business, and, you know, and you will still need oversight and monitoring even if you were to bring the service in house, and perhaps, as an analogy to consider if the cost of taxi drivers insurance goes up, the fares would probably go up. How many customers will stop using taxis and decide to drive themselves instead? A few probably, perhaps, the majority, and companies, I assume will still use taxis and pass the cost on to their customers. So, I guess whilst recognising probably the adjustment, may not happen overnight. So, for me it's probably, one, two, and three.

Julie Pardy: Okay, that was a really good analogy, I like analogies because they bring everything to life. Not everybody wants to particularly vote on this particular topic and it might be that they haven't got a view. So, exactly as you predicted, with the majority in the first three, and I think it's definitely the delayed procurement cycles. Actually, we can see that in the procurement cycles that we're involved in. That very occasionally we'll have a procurement cycle that might last a couple of months, but more often than not, they've been extended, even now, even before this event, maybe six or nine months even longer. As we go through this period of reassuring firms around our safety, to be a partner for them, and the ISO 27001 obviously, which we have goes a long way, as we talked about before. Does that surprise you, those polling figures there?

Lindsey Domingo: No not at all, considering they're consistent with what I said, I'm not going to dispute them.

Julie Pardy: Yes, exactly, unintended consequences, there's bound to be some. Thank you so much for joining us for that particular vote. So, shall I move on to the next point, where I know that you're going to talk to us about the policy statement on outsourcing and third-party risk management?

Lindsey Domingo As context to the PRA's policy statement on outsourcing and third party risk management. It's not a new regulatory topic, however, the reason it's been brought out is because the existing framework hasn't kept up to date with the pace of change and also with the changing nature of outsourcing and new technologies. So, the PRA's aim on this is that firms should apply adequate governance and controls for all their third party arrangements that could impact the PRA statutory objectives. This policy basically aims to leverage and complement some of the existing

requirements. Notably, the ones on operational resilience that we've already seen. Also, there was the Future of Finance report back in 2019 when the Bank of England made the commitment to facilitate firms' use of the cloud and new technologies to increase operational resilience. So, the way this policy paper hopes to address that is to provide regulatory clarity about certain topics such as data security, access, audit and information rights, business continuity and exit planning.

This policy also implements and expands further on the EBA guidelines on outsourcing arrangements, which itself integrated the previous EBA guidelines on cloud outsourcing, and it also takes into account, a few of the international guidelines and standards which are out there from the EBA, IOPA, Basel, Financial Stability Board, the European Commission and from IOSCO. And at this time the FCA did not propose new outsourcing requirements, but they reminded firms of existing rules and guidance, SYSC 8 , SYSC 13.9 if you are an insurer, and also the FG16/5 guidance on outsourcing to the cloud and other third party IT services as well as the existing EBA guidelines.

Julie Pardy: It's interesting, actually to note that on the finalised guidance I was looking at it again this morning. And obviously, some of their guidance, they will publish and republish, and then they republished again. In, I think it was October November 2019, where they sort of made some updates for the link to European requirements. So I think some of these documents definitely stand the test of time, but the problem is, as I go about implementing sometimes find it quite challenging to find information on the FCA website that we know has been previously published because of the search functionality so what we'll do, again, we'll put that updated finalised guidance in the Q&A document so hopefully, then people have sort of a really helpful group of documents that they can refer to.

Lindsey Domingo: Yes, that's a good idea. So, the scope as to who does this policy apply to: banks building societies and PRA investment designated firms, insurers, and this time I mention UK branches of overseas banks and insurers as well, so third country branches. There are, as we mentioned, existing outsourcing requirements for all FCA regulated firms set out in SYSC, but I would say the PRA outsourcing requirements are more detailed and more prescriptive than what the FCA have in SYSC, and because the FCA guidance is a bit less detailed and specific there's going to be a bit more leeway, however the two are aligned. So, in other words if you comply with the PRA requirements, you're also covering 99% of the FCA requirements, probably the only 1% you're not covering is the requirement to notify things to the FCA which you're not going to find obviously in the PRA paper, but both, both regulators have asked to be notified.

Okay, so in terms of looking at the definitions just so we're on the same page, third parties, that's probably reasonably straightforward and includes anyone, any third party upstream or downstream vendors and suppliers. The definition of outsourcing, and so that's both the FCA and PRA definition, it's an arrangement whereby the provider performs a process, a service, or an activity, which would otherwise be undertaken by the firm itself. Now, the criteria to determine whether something is outsourcing or not also includes whether things are performed on a recurring or ongoing basis, whether it would normally fall within the scope of functions that realistically that firm could be expected to perform and there's also a list of exceptions provided by the PRA. For example, things like one-off purchases of software licences will not be regarded as outsourcing, anything that's anything that's required legally can be performed by a third party for example in the statutory audit would not be regarded as outsourcing, the design and build of an on premise IT platform would not be outsourcing. But between the definition of what is outsourcing and that list of exceptions, there is quite some room for judgement and interpretation, and I have seen and witnessed and been part of debates about whether a particular service falls within outsourcing or not, as classification, and part of that debate or discussion was driven by the desire to avoid higher levels of due diligence, scrutiny

and oversight, so by saying its not outsourcing, therefore you should not have to worry about it too much.

But what I'm going to say is that, probably the more relevant question now is whether it's material or not, not so much whether it is outsourcing or not. So while there is some merit in that distinction, that's really the shift of emphasis we've seen from the PRA from the consultation paper to their final published policy. It's basically this shift from focusing on outsourcing per se to materiality. So, in other words, whilst the definition of outsourcing is unchanged, there's recognition that some non outsourcing, third party arrangements can give rise to a comparable level of risk. Therefore, the expectation is that you're going to have effective risk based controls for material, non outsourcing third party arrangements, which are commensurate to the level of risks involved. Hence, the requirement is to assess materiality for all third party arrangements. And that's one of the key points of difference, as I said, compared to the December 2019 consultation the other points of difference are to do with proportionality in the context notably of intra group outsourcing and access information and audit rights. So, the next important definition is materiality: the PRA says material the FCA says critical or important, so basically the key elements of the definition are : it's a service, which if it fails would have any impact on your firm's safety and soundness, so that includes financial performance, financial resilience, operational resilience. For example, if, if that provider is supporting one of your important business services, you will automatically classify them as material. So, the other key elements of the definition, are that failure of that service would impact you as a firm if, in terms of your ability to continue satisfying your threshold conditions so the conditions, based on which you were authorised, as well as fulfilling your regulatory obligations. So, basically you need these three elements of the definition to be taken into account in assessing whether something is material, or not.

Julie Pardy: So I think for the purpose of time, I won't put up the next polling question now, because I know that a bit more to cover, so I'll just move on to that next slide.

Lindsey Domingo: Okay, looking at an overview of the requirements then. So, in a nutshell, what the policy does, is it increases or gives more specific requirements in terms of knowing your provider, and knowing the status of your provider on an ongoing basis. And so therefore these requirements could also be interest if you're a provider, even if you yourself are not necessarily regulated but are providing services to a solo or dual regulated firm so for example, providers need to be prepared to support on operational resilience testing.

Materiality assessments. Firms need to determine the materiality of every outsourcing and third party arrangement. As materiality can vary throughout the duration of the arrangement, it is not something you only need to do upfront, but you should also reassess it at intervals.

Notifications to the regulators, the main thing that's changed here is in terms of the number of notifications, there are more mandated touchpoints with the regulator than before. So, you need to notify the relevant regulators before you enter or significantly change the material arrangement, and that's not only for outsourcing, but you also need to notify them of your non outsourcing material, third party arrangements, as well as any issues you encounter, down the line in order to access and audit information from your providers. And in general, the FCA principle 11 and the PRA fundamental rule 7 will also apply in this context, in terms of making sure that you notify them on everything they would reasonably expect notice.

So, in terms of due diligence, firms are required to perform appropriate, and proportionate to diligence on all potential service providers and assess the risks of every outsourcing arrangement, irrespective of their materiality. Due diligence and risk assessment to feed into each other, they go hand in hand and they cover a broad range of topics from financial, operational, Information Security, legal, regulatory, geographical, concentration, reputation, capabilities, as well as integration with the firm's own processes. An enhanced level of due diligence is expected for material outsourcing. Risk assessment is not just something you do at the point of onboarding but it's something you have to maintain so you need continuous monitoring and ongoing risk management in terms of understanding the vendor, not just assigning a RAG or tier rating but how frequently you engage with them, what conversations are happening and trying to find those leading indicators, not just lagging indicators like quality of service. Quality of service is great, if it tells you after the event but is not going to help you anticipate if something's about to go very wrong, and technology of course can help. You probably have to revisit how you categorise and assess your vendors, and also the skill sets and resources that you need in-house to be able to do that. You should not underestimate the effort. And that approach has to be tailored to the nature of the service you're getting from the vendor so. Otherwise, the risk is yet, you'll be ticking boxes rather than taking full ownership of the underlying risks.

Business Continuity and Exit Planning so basically you need to develop a business continuity plan an exit strategy for each material vendor and you need to do that before you sign the contract with them. And you need to do the testing of that as well once the arrangement is live.

Contractual agreements: you need to have a good contract so that the provider complies not only with your requirements but also with the regulator's requirements. Regardless of materiality firms need to make sure that outsourcing arrangements don't impede regulators' ability to oversee your activities including outsourced activities. Contracts also need to cover the items the regulator has listed. There are more than 20 items which are explicitly listed and need to be in the contract.

Security and resilience: We've talked about resilience and data security, there are 13 control areas, specifically mentioned by the regulator - things like Incident Management and Identity Asset Management, and the main expectation there is that the service provider's environment, when you're sharing data with them, needs to be at least as effective and secure as your own.

Access, information and audit: you need to do audits to obtain assurance on your third parties.

Governance and record keeping: Even if you outsource, you're still fully responsible for your regulatory obligations, you need to maintain an outsourcing register, and the board needs to implement an outsourcing policy as well as set the control environment and the appetite for third party management and outsourcing. Generally we've found that the outsourcing prescribed responsibility is allocated to the SMF24 function, which is taking a lot on and that covers the overall framework, which doesn't mean that individual responsibility from specific outsourcing arrangements cannot be assigned to other individuals in the firm. So, I think that's what I really wanted to cover on this slide.

Julie Pardy:

That's great, thank you. I know we're hitting the 12 o'clock mark now so you've got a couple of concluding slides and I know Nick has confirmed in the chat that people will get their questions answered, even if we can't, we can roll over by few minutes if people don't have to go to other meetings. But if they do have to do then we can pick those up, but I'll come back to you. Moving on to the timeline piece Lindsey.

Lindsey Domingo:

Yes, absolutely, so very quickly on the timeline. Yes, we must comply by 31 March 2022, and again that means that any outsourcing arrangements you are entering into since March 2021 should meet the expectations by March 2022. And also you have to review and update your legacy outsourcing agreements. So that's something that you're going to have to do and the language is a bit ambiguous, but I think, to, to recap and simplify the message, you need to comply by 31 March 2022 in respect of all your outsourcing and third party arrangements, legacy as well as new ones, so I think we can move on to the final slide.

So, what firms need to do. What we've done is for both frameworks. So, we've listed the ten things we think firms need to be doing before March 2022. So, the first one is assessing your current third-party risk management framework and aligning it with those new requirements in terms of what's your governance in place, your policy, your processes, your outsourcing register, your management information. Secondly, reviewing and repapering your legacy agreements, and considering your current operating model and capabilities, and how you're going to operate, going forward, as you need to meet this increased workload and activity that we are seeing firms having to do.

Third party risk management, assurance and due diligence: there's quite a lot of work involved.

In terms of operational resilience you need to, as we've said before, identify and then map your important business services, set your impact tolerances, do your mapping and scenario testing, identify any vulnerabilities, define your prioritised plan to address those vulnerabilities, prepare your self-assessment. And again assess implications for your current governance and operational risk management framework, having the right policy standard guidelines, reporting and monitoring in place so that you are able to manage operational resilience consistently going forward so that you're then going to have resilience by design as a sustainable way of working across the organisation so just to emphasise what I said earlier.

There's a lot to get done by March 2022 and the refinement and remediation will continue beyond 31 March 2022, but there's already plenty of work that we need to do by March next year. That's it from me.

Julie Pardy:

Okay, we'll let you have a breather now, that was fantastic. We've got so many questions and comments and we still got quite a lot of people with us, so what I'm going to do, I can see when Nick appears, I know when Nick appears and he's going to hold us to account on the time, I've just put a poll there and just reminding people please don't tick the anonymous box if you want us to reach out to you. We've had that on a few webinars, and we haven't been able to reach out to people that we know have had needs. So, we put that up there for you to have a have a look at and I'm just wondering whether we still got quite a lot of people on the webinar. So, I'm just wondering Nick whether you know if there's any critical one or two questions that you think we should answer now, or whether you're thinking that we should do that via the Q&A?

Nick Dent:

There may be a couple that warrant a bit of discussion. There was one that came up in the chat earlier, right you know there was an insurance firm that delegated an awful lot of responsibility for claims handling and underwriting and that kind of thing so they were kind of struggling a little bit on identifying for themselves what the IBS's were. So, I know Lindsey that you ran through that in a slide where we were talking about the definitions but I wondered whether there was any guidance or advice you can give in terms of helping people that are struggling.

Lindsey Domingo:

Yes, absolutely, I think the short answer on that, and that is something we can discuss more at length as well. The short advice and input on that is that those outsourced tools, processes are still your processes so therefore you're going to have to sit down with these third parties to try and understand how they work, because at the end of the day, you're required to map the processes so the mapping, I appreciate a lot of the knowledge of the details is with that third party but you're going to need to have that understanding, because ultimately, you will have to identify what your important business services are, and even if it is with the help of a third party. And secondly you need to understand how it's done because that third party is a critical dependency. In terms of then identifying scenarios, one plausible scenario could be that the party is not available, what do you then do so that has to be part of your plan. So, I would advise sitting down with that third party doing that exercise together.

Nick Dent: And just while we've got a fair few people on the call as well, I know we're running over by an awfully long time, but just one related comment here that was made during the session, which I thought was interesting. And it's kind of related to what we were just talking about and the identification of risks and that kind of thing. Is there any difference. If a firm is reliant on a parent company, services, especially if those intra group organisations are located in different geographies internationally. Is there any extra consideration that needs to be given to that?

Lindsey Domingo:

Yes, and that's one of the areas and this is what the PRA referred to as proportionality so that's one of the areas where the stance has changed slightly from the consultation to the final policy. Because in the consultation, the view was that, as far as we're concerned, those are all third parties and they should treat them like any other outsourced service. What, the regulators have introduced in the policy is this principle. Basically, in terms of proportionality when it's intragroup outsourcing for example, you can take a more proportionate approach in terms of what you would expect from them, for example the due diligence that you're doing, how do you get your comfort and the sort of assurance you're getting over the service provided by that external party which is not so external because it part of the group. But you still need to get comfort and assurance, and there are some challenges because sometimes you may not have the required influence over, what the head office has decided that they provided you in terms of service. Some tricky discussions and really what we need to remember is that there will be a senior manager here who's got the accountability and facing off to the regulator for the, for the services, and they need to get comfortable, but yes there is some flexibility.

Nick Dent:

Thank you very much. Thanks for your attention. Really engaging an interesting topic, I think that probably warrants more conversation so please do if you've got any questions or queries reach out using the contact details that you see on the screen in front of you. Feel free to ask anything, whether it's about products and services that we have on offer, or whether it's more of a regulatory question or just a query. We'd love to hear from you. Thanks very much. We'll draw that to a close.

Have a good day. Take care of yourselves, and we'll see you next time. Thank you.