BANK POLICY INSTITUTE

ANNUAL CONFERENCE

DEFINING OPERATIONAL RESILIENCE EXPECTATIONS FOR U.S. BANKS AND SUPERVISORS IN A GLOBAL ECONOMY

Washington, D.C.

November 19-21, 2019

ANDERSON COURT REPORTING
500 Montgomery Street, Suite 400
Alexandria, VA 22314
Phone (703) 519-7180 Fax (703) 519-7190

PARTICIPANTS:

Moderator:

ADAM GILBERT
Partner
Financial Services Advisory Risk and Regulatory
Co-Leader, PwC

Panelists:

JOHN A. BEEBE
Deputy Associate Director, LISCC
Federal Reserve Board of Governors

CHRIS FEENEY
Executive Vice President and President of BITS
Bank Policy Institute

STEPHEN C. HOSTETLER
Managing Director
Enterprise Scenario Planning and Execution &
Global Real Estate Services COO
Bank of America

AMY SHANLE
Global Head of Enterprise Resiliency Strategy &
Regulatory
Bank of New York Mellon

* * * * *

P R O C E E D I N G S

MR. GILBERT: Good afternoon, everyone. We're going to get started. Thank you very much for coming to our panel on Operational Resilience. With Financial Resilience shorn up post the crisis with new regulations around capital liquidity, stress, resolution planning, Operational Resilience of individual firms in the system is a next area of focus and I'm delighted to have a terrific panel here today to help frame the issue for you and explain where this is all headed. So, my name is Adam Gilbert, partner at PwC, Regulatory Leader, and I'm going to start on the far right here, my far right, John Beebe from the Federal Reserve System, Board of Governors of the Federal Reserve, Chris Feeney from Bank Policy Institute, Steve Hostetler from Bank of America, and Amy Shanle from Bank of New York Mellon. Your programs may say James Hardy from State Street. He was not able to make it and Amy kindly agreed to step in and will provide you. Having worked with her over a number of years, you will get tremendous value from her insight. So, thank you, Amy, for joining us.

John, I want to start with you and get the

regulatory perspective to set a foundation on this important topic. So, if you could just start telling us, what's meant by Operation Resilience at least in the eyes of the Federal Reserve. Why is it important and why now? There's a lot of focus on this right now and why has the time come? So, start us off.

MR. BEEBE: Thanks. All right. So, first I want to thank everybody for inviting me to the conference. I think this is going to be a great topic. I can't believe folks went to the FTP topic instead. This is the one to go to. I also heard this morning that for D.C. folks the bar is to have a sense of humor and be reasonable to I'll shoot for that today. You know, and I think you've probably heard (inaudible) speakers before. They give the disclaimer, the views I offer our (inaudible). Not because of the Federal Reserve. Especially around Operational Resilience. We don't have a definition that we put out there. We don't have a policy called Operational Resilience. So, the definition I give you is not the official Fed definition. But I think the way we're thinking about it, it's the ability of the bank to deliver critical

operations through a disruption and you get into some of the familiar concepts that you see in cyber of identifying issues, detecting them, protecting against them, responding, and recovering. I think what we focus most on is the capability to recover when an event occurs so it really is that piece.

The why now is interesting. I can't remember when I first started hearing Operational Resilience. I think it was probably back when the Fed was working on changing its ratings framework and we thought, "Okay. What do we want? We want Financial Resilience and Operational Resilience," and that was probably the first time I heard it, but it's come on strong over the past year or so and I think there are a couple of reasons why. One, we've heard it all through today's conference. I'm sure you heard it yesterday. There's just a lot of technology led business transformation going on in the banking industry. It's brought a lot of attention to operations and how you all do things.

I think two, we've seen a number of events both in the industry and its regulators. We've seen events out there that have brought more attention to,

you know, how do we make sure that our firms are truly Operationally resilient.

Three, I think Brexit has been the catalyzing factor and that's why I think you see the PRA out with a paper. It really put a focus on business processes, where your processes are, and what if the Brexit change doesn't go as planned, what do we do? I think that brings a lot of attention.

And fourth, and probably most importantly, I think this is where I have sort of the most interest. I think it's the interconnectedness that we all recognize in the system. It has brought a lot of attention that there's a lot of common interest here. If one bank has an operational problem and can't get back up running, the rest of you are going to have a problem. So, I think the common interest and the interconnectedness is probably the other thing that has brought it together.

MR. GILBERT: Great. Thanks. We'll come back to that interconnectedness point in a bit. So, what are your objectives in this area and I recognize it may be early days, but what does the Fed want to achieve with respect to the topic of Operational Resilience and using

the examination process policy levers in this area?

MR. BEEBE: So, as a supervisor, I give really simple answers to complex questions. So, I think what we're looking for are resilient firms in a resilient system. That's what we want, you know, and part of how do we know that we have that? It's looking to the firms to demonstrate the capability to recover. What does their framework look like for that? I think, and I'm involved, if you look at my bio, I'm involved with the largest banks, I would say firms in the Federal Reserve. We look a lot to systemically important critical functions. So, what are those functions that the banks do that can impact the entire financial system, the global economy. And then we also look at what are those functions that are important to the safety and soundness of the individual firm. So, I think those are the things that we look to for objectives.

One of the things that's a little different in our approach here then I've seen how we approach things in the past, we're doing a lot to work with other U.S. and global regulators to harmonize what we put out there for standards. I think we're working with the industry

more. I know members of this panel because we've had a lot of outreach efforts with the industry to understand where the industry is going. We're looking for industry solutions, you know, where do we need to step in and solve something? Where can the industry solve it for itself? And I've learned just over the past several months of a lot of developments in that area. And as a supervisor of a large bank, I think, you know, where my heart is on this is really the critical functions. It's making sure that those are available to the U.S. citizens, world citizens, when an event occurs.

MR. GILBERT: And, John, what levers, what positive mechanisms are you going to use in this area? So, for example, for the nerds out there who wait with bated breath for examination handbooks, you might have noticed that November 14 the Business Continuity FFIC Manual was updated for a lot of the issues that we're going to talk about today. So, can you comment on that? What was behind that? How is that going to be leveraged going forward? Are there are going to be other policy mechanisms that you use to advance the agency here?

MR. BEEBE: So, the handbook is not policy.

The handbook is a tool that examiners use to ensure consistency as we go out and do exams. From personal experience, especially for the large banks, some of what's in the handbook applies, some doesn't. And so, it really is a tool so that the way we look at Bank of America has similarities to how we look at U.S. Bancorp and so it's a tool for examiners. It is not regulation. So, I think the tools that we're really looking to use and why we come to forums like this is to use the regulatory framework to help advance the industry. We have to figure out what that regulatory framework looks like. Something that is more enforceable and then with that, as we referred to earlier today, you go regulation, then guidance, and then it filters into the handbook.

The handbook is an interesting thing though. I wasn't involved in the rewriting, but it did pull in a lot of the concepts that we've talked about in the Operational Resilience framework and part of that is because a lot of what's in Operational Resilience, continuity planning, disaster recovery, those types of things, they've been around a lot longer then this word

has been popular. And so, I think you have some of that in there, but it will be a tool. I don't think it's the main tool for getting us to an Operational Resilient framework if that makes sense and others can chime in.

MR. GILBERT: Okay. Meg?

MS. TYRE: That's great to hear.

MR. GILBERT: So, my good friend, Greg Bair, who I'm sure is here, will be delighted to hear that the handbook is not official policy so that will be --.

MR. BEEBE: It really is a handbook for examiners. It helps us as we go out -- I group up a field examiner after a few years of doing community banking and you take the handbook and gives you a set of questions that you can work from. You don't ask them all, there's not a prescribed answer to them all, it helps give you the questions and it's a tool that we give all of our examiners.

MR. GILBERT: Okay. We will, at PwC, reconcile MRA's to the handbook going forward and we'll let you know if that stands.

MR. BEEBE: Now, we can't issue an MRA, but comments like that might get you one.

MR. FEENEY: This is where I have to make peace.

MR. GILBERT: Let's go Chris if we could jump to the -- let's expand this globally --

MR. FEENEY: Yes.

MR. GILBERT: -- because this is not a topic unique to the Federal Reserve of the United States. This is a global issue so can you provide us some perspective on what's happening globally?

MR. FEENEY: Yeah, I'd be happy to and I'm going to do it two ways. I'm going to go a little macro and then we'll go a little bit more to the, you know, granular discussion. So, you know, John's here. We've been working with the Fed and the policy side of the Fed as well for quite some time. It's been about a year since the Bank of England paper came out a little bit more and we've been working with the U.S. regulators so, in addition to the Fed, the OCC and the FDIC on Operational Resilience and there are probably three or four things that have been very consistent.

One is the interest in a collaborative dialogue, which is great. We didn't quite have that

with cyber and it turned out to be, you know, a significant period of time before we finally sort of calibrated and settled in on the best way to examine the cyber security side of the business so it's been very helpful, right, and to be honest, so you guys know, the Fed actually came to us and asked for this kind of conversation, which is great.

The second is we're trying to keep it very risk in principle space and this again a U.S. discussion. You know, things that are important, you know, as John said, the Operational Resilience is really a maturation of cyber resilience, BCP planning, the things that have been in play a long time, but you have to thing of sort of post event. What does it really mean? How do you evolve that resilience of the firm through a different set of exercises or a different way to connect an important to business more actively? So, it's really important that the business understand it, make decisions around it. There's a couple of new concepts and I'll talk about what the Bank of England has put out that will probably get adopted globally. But it's habits of business, you know, participatedness,

make decisions, and run that all the way up through the Board so that the Board understands some of the decisions that are being made. We have also heard multiple times this is a multi-year process. As you heard John say it earlier, you can talk to any of the other regulators, we don't have this figured out, right? So, regulators learn a lot from what the firms are doing and we all do it a little bit differently. So, the other component, and we've heard this reflected back to us, is it's important for firms to pick how they do it. It's unique to your business, it's unique to your footprint, it's unique to the systems you've chosen to install over the period of time. It's frankly unique to your talent as well so those things are important. So, we're really thrilled about sort of the ability to have the discussion. We're all sort of feeling around in the dark a little but right now, but we'll get there.

The Basel Committee is similar, right? They're trying to coordinate the international view of all the regulators who participate in the Basel Committee. In fact, just maybe two hours ago the Chairman of the Basel Committee gave a speech talking

about this at Euro Finance Week and talked about how they're really trying to adopt a forward looking approach to Operational Resilience. So, it's sort of front and center and real time if you want to think of that that way. I think that's really important. The other benefit is right now or at (inaudible) with the Fed is actually the Chair of the Basel Committee that's doing the work on this. So, we are trying to keep it very principled and risk based. Again, so, firms have room to move, right? If you're an operator, you really need the flexibility to respond in a way that's pertinent to your firm.

The Bank of England is a little less principles and risks based, right? They're papers are in the making. They're getting a bit more prescriptive around what they'd like to see. They're putting more quantitative type measures into what resiliency looks like. I think that's going to be a, you know, challenge that we'll have to sort of coalesce around and figure out how to sort that out.

The other component, and this is on the heels of a treasury select committee report, but also some

issues in processing and some harm to the consumer, is the Bank of England is thinking about this maybe a little more weighted to the consumer end and harm then we might be more weighted to the systemic end and the totality of the industry. Both are important. I think we as firms as an industry support both, but you might approach the problem differently depending upon which one of those is most important. So, that's sort of where the dialogue is right now, you know, as of maybe 20 minutes ago when the last speech was given.

MR. GILBERT: Real time updates.

MR. FEENEY: Yeah, there's probably seven other Operational Resilience panels right now at this time.

MR. BEEBE: But this one's best.

MR. FEENEY: Yes, exactly.

MR. GILBERT: Steven and Amy, let's jump into the industry perspective on this and maybe, Amy, you get us started.

MS. SHANLE: Sure.

MR. GILBERT: Can you talk to us about how your firm

is thinking about this. How do you define Operational Resilience or if regulators have different views on it or objectives?

MS. SHANLE: Well, I'm not going to contradict the regulators. Feel free to (inaudible).

MR. FEENEY: You get a free pass.

MS. SHANLE: Yeah, house rules, right?

MR. GILBERT: And how are you organized around that?

MS. SHANLE: Sure. No, happy to do so. So, I mean, I won't add too much from the definition than what's already been said, but I think very simplistically in laymen's terms, it's the old keep calm and carry on. How do you continue to carry and deliver your business services to the market? I think of that in the most simplistic way possible. You know, at Bank of new York Mellon, we took a fresh look a little bit over a year and a half ago and we really came up with a bit of different approach for resiliency around the time that the discussion paper actually came out. We actually created a new first line of defense resiliency office. At the same time, we created a second line of

defense resiliency office. So, as John mentioned, these things like business continuity, disaster recovery, incident and crisis management, they are nothing new. They've been around for ages whatever your sector is. What we decided to do was just bring them under one umbrella and bring in a more wholistic approach to how we manage and monitor these things ultimately to continue to carry on and deliver our businesses to the marketplace. So, it's about a year and change into that structure, but really, at the same time of having sort of this central coordinated office with this federated model, we found that for resiliency to really be embedded in the business as usual practices, you have to embed in the business as usual senior leaders into each of the businesses.

So, at the same time that we created this new office, we actually created various senior individuals in the businesses and they ultimately are accountable for delivering against that resiliency framework that we set at the first line office function.

MR. GILBERT: Is that how it's working at B of A, Steve?

MR. HOSTETLER: Yes, precisely. We copied everything. No, but, in fact, there is a lot of similarity. So, the concept of first line ownership of resiliency, we're 100% on board with that. We think that's a very effective way to drive more engagement in the work. So, the team that we've put resiliency with sits alongside the same teams that drive capital planning and CCAR and recovery and resolution planning and those are all owned by a first line team that quarterbacks those activities across the firm. So, I think that point is definitely consistent.

The second point also kind of tying to capital planning CCAR is extending the work into the stress continuum and, John, really to your point on recover, I think we would represent that the firm has done a lot of work to make sure that we prevent disruptive things from occurring in the systems that we run, the business continuity work that would allow you to plan for some, but think about what happens if your prevention fails, you know, if a very core critical system fails, what can you do to continue to provide services to your customers and clients? Perhaps it's in an alternate strategy for

a period of time, an alternate channel, but that sort of scenario analysis we think is an important component of resiliency, so, in terms of net new thinking, that's an area that were focused on in the near term.

MR. GILBERT: What are some of the key challenges you fact and in particular, do people have a clear understanding, especially the business peoples, and I think, Amy, your organizational design is leading you to a good answer here potentially. They have an understanding that this is moving from continuity and disaster recovery and restoration of service as a technology and operations problem to a business problem and I think that's one of the things that organizations if understand, John, what the Fed is doing, what the Bank of England, the UK authorities are up to, even the Basel Committee, is to change the dialogue around this resilience to be a business risk management issue. Do people understand that?

MS. SHANLE: Yeah, I mean, I'm happy to start and Stephen you can jump in or John or Chris. I think, and Adam you're correct, the way that we structure it and approached it it's fostering that accountability,

it's fostering that drive and ownership at a business level really embedding that into the business.

MR. GILBERT: Mm-hm.

MS. SHANLE: But, you know, we think about it from a three leg of a stool approach so it's not just business, but you have to operations, you have to have technology. You have to have all three of those areas present to determine your critical business services, to ascertain an impact of an incident, to know how you need to respond to a DR event, what have you, I think you need to have that whole three sort of three legs of the stool approach to really have a fulsome perspective to make sure that it's being drive through not just business but ops and tech and that really helps spread the awareness and ultimately, encourage the delivery of the service in that market disruption. Now, Steve, if it's a different for you.

MR. HOSTETLER: We concur. So, having the teams collaborate in that planning phase critical to make sure that you're capturing, you know, you're planning for the right businesses, what are the most relevant ways in which we're serving customer's clients

today, has that changed in the last several years versus when we originally established are plans. So, collaboration on the planning and prioritization component of the work and then in response in the real world or even in an exercise, we think it's also very valuable to get all of the players at the table. Who is going to talk with the customers? How trained is the sales force to work through an alternate mechanism of service clients if you had your network down as an example. So, absolutely, it requires the collaboration and so, bringing the front line maybe be a little closer to that work is the behavior part that is changing, but we think there's a lot of value that comes with that.

MR. GILBERT: Chris, any thoughts on this?

MR. FEENEY: No, just, you know, we have the benefit of having numerous clients and we're doing this work with a couple of the other associations so we're seeing about 100 firms in the dialogue and say it's all consistent. Many have appointed people to actually run Operational Resilience to coordinate across those three groups that Amy mentioned I think is really a factor.

The other things the firms are doing, and

these guys both mentioned it, is really rethinking the scenarios, like, what could happen, right? There's a whole (inaudible) of a plausible discussion going with the regulators and the financial community and it's hard to figure those things out, like, what would you really do in a problem that looks different than the last one you solved for? And that's where the discussion is going and that's where it gets a little grey and it's hard to exercise anyway, but we will do it and we do it as a practice, but the style or the magnitude of the exercise is changing.

So, that's part of the dialogue I think we're having as a group.

MR. BEEBE: Yeah, I think the only thing I would is that, you know, I think the Fed is coming from a place or the regulators where this was really a data center question and so, how do you recover a data center when it goes down and it is -- a lot of that thinking goes back to what happened around September 11 and the rules that went into place there. And I think we found as we did exams over the past say four or five years that there wasn't a lot of advancement and I think

that's part of why Operational Resilience has taken hold. A lot of that was still just very IT data center focused and now there is a change where it's more of a business driven process. And I don't know if it's the regulators pushing that or the banks finding their way or maybe it's Chris doing some good work in BPI. I'm not sure where it came from, but it's a more holistic view. It's a more end-to-end view and it's considering how technology is fully integrated into the businesses now. And so, I think it's the right evolution and it's the right time for it.

MR. HOSTETLER: John, the one, I mean, one catalyst here is customer and client expectations so their expectations are leading us and the industry to make these investments to be respective of, you know, regulatory guidance.

MR. GILBERT: I want to come back to restoration and decision rights, but let's dig a little deeper into some of the technical aspects. So, Steve, Amy, can you define -- people will hear the word critical business service or critical business function, what is that, what are you doing to define that, can you

leverage a resolution plan because that's part of the nomenclature in resolution planning? Give us some foundational concepts here.

MS. SHANLE: Sure. And you hit the word appropriately, foundational. So, as part of what we did with our new office structure and our new governance model, we took a fresh look at how we define our critical business services and that really has served as the foundation for everything we do from an enterprise resiliency perspective. So, to your point, Adam, you know, back with Todd Frank and RRP, we had already some defined terms by the regulators, global regulators. Things like critical operations, core business lines, critical economic functions, critical functions. Forget the adjectives for a second, but what do you actually do that's most important for your customers in the market and the like? So, we had a set of criteria that we developed. Certainly, leveraging those RRP and terminology globally, but then we looked at sort of the intraday impact from market, client, regulatory perspective, applied that criteria to a large universe of our business services, and we came up with a subset.

That was really the foundation for what we did from a process mapping perspective as well and what do I mean by that?

So, process maps have been around and used for a multitude of reasons across and organization regardless of your industry. What we decided to leverage them for is to really decompose these business services in a way that would give a much more granular view and understanding of what it actually took to deliver that business service to the market. So, if you think of it as you have your overall business service and you identify the functions or groups of activity that are used to deliver that business service, instead of tiering those upper business services, we actually tiered those functions that deliver the business service. For each of those functions, we then identified things like assets, IT assets, applications, vendors locations. To really understand in a much more granular way, if there's a break in a vendor or if there's a break in an application, we now have a very clear view of what function, what activity is that actually impacting, which ultimately is impacting what

part of our business delivery service.

So, it's a pretty foundational shift. Certainly, not a light load to do, but certainly, we now have a good strong foundation to understand where an incident occurs how is that really impacting us? And, you know, we've talked about the UK papers a bit, the forthcoming ones and the one from July of last year. When you think a bit more broadly as well across, as Steve mentioned, that stress continuum, you know, we don't want to look at things in isolation. So, we don't want to look at just this RRP term for this regulatory requirement or this instant or this scenario. By doing sort of a process mapping, architecture perspective, and getting that granular view, when we go develop things like scenario analyses for cyber, for vendors, what have you, for business impact analysis, for impact tolerances, right, it's a nice foundation to really be able to spring forward in different ways leveraging, you know, risk appetite statements, traditional operational risk measurements. It gave us a nice foundation to be able to then offshoot with these other disciplines.

MR. GILBERT: Great. Steve, talk to us about

your definition around critical business services and functions and then, also, Amy just used another foundational phrase, impact tolerance. Can you describe what that is as well? So, start with critical business services and take us into impact tolerance.

MR. HOSTETLER: Okay. Just the thought process, you know, one reaction, Adam, for, you know, the business that you're in is that any time you ask a bank to think about re-describing what it does it's kind of a full employment act opportunity.

MR. GILBERT: I'll keep that in mind. Thank you.

MR. HOSTETLER: So, I think you led off can we use RRP, can we use resolution recovery planning services? We think the answer is yes. We also think it's important that the taxonomies we use to run the bank through these various disciplines are integrated and so, even if it's not perfect, we think that's a great starting point and that is what we chose to use to do our initial prioritization. And I think other than that our definition and the work process is pretty similar to what Amy described.

The piece that I would communicate to the group around where we think we're going to get some leverage out of how we work through this is that recognizing each of these services, and I think this is similar to what you're describing, we believe that you break it down into capabilities that it takes to really run and to lever a service to the customer so there's core applications that support that, other enablers. And from a resiliency perspective, we can test each of those capabilities, you know, once, twice, three times, four times, but then get benefit across the full suite of services in which one of those capabilities is used. So, we are trying to look for leverage points where we know we can't test every single permeation of a service in something that goes wrong, but we get enough coverage that we ourselves comfortable that we have the right capabilities to bring ourselves back and that we can deploy this work in a real life scenario. So, we don't want it to be a book report. We want to be able to use it and so, that's one of the ways in which we're breaking down the work irrespective of services.

MR. GILBERT: Great. Before we go to impact

tolerance, Chris, you mentioned 100 firms active. We have two G-SIB's here. Are other firms advanced in their thinking around and discipline around critical business service and function?

MR. FEENEY: Yeah, it's funny. We've all been to the arcade, right, and there's the game where you shoot a water pistol and the horses run, right? We're in different places, right? Just to be honest. People have a different, you know, inventory, people have gone through a capabilities mapping, they've gone through process map, they've cross-referenced them. Others are getting there. So, I think, you know, just reality is a real practical nature to this. The full employment act it true. This is hard work for a technologist. It's extremely detailed. It's extremely dense. It changes every day. You're doing releases, you're making anything from a cyber release every Monday to a something in enhancement release every Thursday. Every time you go back the environment has changed, right. So it's work, it's hard work, but I think everybody is focused on it. They have been through the normal resiliency work they've done whether it be cyber

resilience or your BCP work, but it's a constant.

I think the difference here is when you think about this and the impact, it's a multi-factor equation now. That's what changing. You know, systems down, boom, systems up. It's not that simple. You know, what else goes into that is it a time based equation? Is it a business impact equation? Is it a consumer, a systemic? And that's where I think the thinking is changing, but it will take a while to mature.

MR. HOSTETLER: And I didn't answer your question on impact tolerance.

MR. GILBERT: Yeah, let's talk about that.

MR. HOSTETLER: Yeah.

MR. GILBERT: Because that's a hard concept for people to understand.

MR. HOSTETLER: Yeah. We think it's important to not be aspirational and define impact tolerance too close to what your BAU expectations are of either being always on for your customers or if there is an event, it's milliseconds or minutes or, you know, 15 minutes in your backup. If you do that, then you're not admitting

what could occur if you pushed yourself farther into the stress continuum. So, we think it's important to set it as a threshold where you're going to experience and your customers are going to experience a little bit of, you know, meaningful disruption. Then we also think it's important that once you define that to push yourself beyond it and think about how you would restore from reaching that relatively critical threshold.

So, mentally pushing yourself kind of -- if you want to think of -- and I have not spent a lot of time in tech ops risk, but push yourself into that severely adverse scenario from a CCAR analogy doesn't happen very often. Maybe it never happens, but think about it and exercise how you would handle that type of a situation.

MS. SHANLE: I mean, I think one of the other things that this concept that was introduced by that UK paper, it left a lot of questions verse answers to be candid and I know we've had some chats on other discussions with this, John, that these upcoming papers we actually hope give a bit more clarification on what the regulators really intended by this concept. For

example, they introduced things like maximum allowable downtime. Is that the same as a recovery time objective? You mentioned the FFIEC handbook that just came out.

MR. FEENEY: Right.

MS. SHANLE: I think they used the term maximum tolerable downtime.

MR. BEEBE: Tolerable downtime, right.

MS. SHANLE: So, you've got all of these terms and these concepts, but is there a global lexicon? Do we have global alignment on what these really are intended to solve for and what they mean and then certainly building off of stress continuums, risk appetite statements, again, not looking at this in isolation, but I think to be candid, that paper sort of left a few more questions than specific answers on this topic too.

MR. GILBERT: Yeah, that's a great point. John, do you want to pick up on that and --

MR. BEEBE: No, not at all (laughter).

MS. SHANLE: I laid it up for you, John.

MR. BEEBE: Thanks. Fortunately, I don't know

that my policy colleagues are in the room so I'm going to freewill on this one.

MR. GILBERT: All right. I love it when the (inaudible) free wills.

MR. BEEBE: And I think this is one of the reasons that we don't have policy out there is these are still some things we're thinking about. I have synoecism around putting numbers on non-financial risks and it comes from living through sort of AMA with ops risks and some things we've tried around legal risks and such. I think they can be indicative and helpful, but in terms of being definitive whether or not something is recoverable, I don't know that a number is going to get you all the way there. I think it gets you partway there. As the industry and all of the global supervisors sort of work through this question, the thing that I think I look for on the supervision side is what does that number drive? Does it drive the firm to make the investments to become more resilient and to do the right things around those critical functions? I think that's what I'm looking for it to do. Whether or not the PRA paper gets there or we get there on the

policy side, I'm not sure. I do think, you know, we need to leave some room for innovation around what this ends up being.

MR. FEENEY: And that's consistent with what we're hearing from members, right? I said multi-factor because there's some qualitative aspects to that as well. So, if a raw number, if you will, becomes an indicative number, that's probably okay at least to sort of set some, you know, guidelines, but there's a lot more work to add to that. And that's, you know, frankly, that's part of dissidence, if you will, to the economy between U.S. regulators and the Basel Committee and where the UK regulators are. There a little closer to finding a number, as I mentioned earlier, and we're I think probably closer to having a number of components go into how you think about it and how you invest in it and, you know, change your processes and put the muscle, if you will, behind it.

MR. BEEBE: Yeah, it's hard. I think this is a place where -- I sat through supervisory judgement discussion earlier today and I think this is where if we stay principles based, there is going to be supervisory

judgement that has to be applied as we work through this.

MR. FEENEY: Mm-hm.

MR. BEEBE: If we went to a standard, you know, we have 5% capital, we want a five hour business impact or impact tolerance, then it would be easy for everybody to check the box. It would be the wrong box to check so I think this where I think we as the Fed have tended to look to the principle based guidance and work from there rather than trying to set a standard around this at this point.

Now, notably, post 911 we did set some standards out there. We said these are the most critical things, you know, the recovery time objectives and that did drive change in the industry and I do think putting a number out there does drive change, but it is right for this circumstance? I'm not quite sure.

MR. GILBERT: Okay. Planning around scenarios is going to be an important part of this discipline. Steve, extreme but plausible is a phrase that gets thrown out there. Do John and friends need to define that for people so that there's commonality in the

industry? Is there such a thing as extreme but plausible?

MR. HOSTETLER: Yeah, I absolutely think those words could mean a lot of different things to different people --

MS. SHANLE: I agree.

MR. HOSTETLER: -- so I think it's almost got them. It almost means nothing currently. I think that if we stuck, John, with your approach and it was principles based and you were looking to define what actions are firms taking based on the process, I don't think it really matters to put a lot of meat on the bone around extreme but plausible. If we had defined impact tolerance thresholds, then the scenario become critical and I think you almost need example scenarios, which I'm not sure, you know, if that would really work across firms. So, I think that's my point of view on the regulatory side. From a testing perspective, we think about scenarios as absolutely being something the firms need to, you know, invest in and that we should have an independent team. We're thinking probably like Amy the first line team that's responsible for resilience

running the process likely is also responsible for developing the scenarios and the testing regimen. So, independent of technology or operations of the business is the team that's helping define, okay, is my plan -- what's the scenario that I want to use to evaluate the effectiveness of this plan and, you know, the effectiveness of this business being able to work through that sort of operational disruption.

MS. SHANLE: Yeah, just some additional thoughts too. I mean, certainly, you have to consider your scenario, cyber, vendor, what have you, premise, you know, tech risk. At a certain point though, it's almost scenario agnostic with regards to, what are you going to do about it, right? How are you going to recover? Whether it was a cyber attack might be a little different. That tends to have a longer tail for a multitude of reasons, but at a certain point it's, okay, there's a disruption in my premise, a tech, an app, a vendor, how do I recover from it and how quickly can I recover from it? So, certainly, agree, there's a lot of (inaudible) and work that's need to be done around scenarios, but at the same time, you want to make

sure you're flexible enough to be a bit more scenario agnostic in how you are able to respond.

MR. GILBERT: We got a question from the audience about testing and I wonder if I could ask Chris, Steve, and Amy to comment on how does he definition of critical business function or impact tolerance affect your approach to testing? I would think the affect is pretty profound, but I'd love to get your thoughts on that.

MS. SHANLE: Sure. I can start if you want. You want me to start? All right.

MR. FEENEY: You can start.

MR. HOSTETLER: You're farthest down.

MS. SHANLE: I know. Thanks. For better or for worse. So, I mentioned a little bit about our new business service framework and that being the foundation that really did change how we test. So, from a disaster recovery perspective prior to service foundational shift, we would test the resumption of an application. Tests would be done in siloed to see if the application comes up, it meets it recovery time objection, check the box. That didn't really tell us the bigger picture of

what that application supported and how that actually contributed to the deliver of the service. So, we actually now test from a DR perspective the recovery and the resumption of our business functions, not just those applications. So, by understanding which groups of activities need that recovery time objective in two hours or what have you, we're now changing how we test to really focus on the resumption of a business, not just that resumption of an application.

MR. HOSTETLER: Yeah, we also have thought about the end-to-end amount of time that it takes for us to, I think similar to you, kind of restore the full value chain of what it takes to enable that service. So, these are not tasks that, you know, these are tasks that usually take over 24 hours, but we know exactly how long we think it takes to rebuild the technology infrastructure supporting a service so that's great. The testing would then say, "Okay. You represented that that's your plan. Let's go actually do it over a weekend and see if you can do it on the clock." So, that's one way in which testing is changing to help support Operational Resilience services based approach.

But we're thinking of testing and we're still working multiple ways in which you can test what your work here and it would include exercises, it would include pulling senior management together in a response framework to role play through a very severe outage. So, I think that's what we're thinking. I think your question was you said impact tolerance. How does that impact testing and given that we are taking a little bit more of this principles based approach, it probably doesn't matter as much as maybe as it feels like it should. We set it, we establish plans, and then we test the plans. Chris, anything?

MR. FEENEY: Yeah, I'm fortunate I don't have to test anymore, which is great. I did many weekends and all that stuff, but I think that makes sense. You know, there is a component to this that's a little sidebar, but not much. The industry has been doing testing like this for decades. We have, like, as an industry done 38 tests. We have a whole institution set up to do interconnected tests. It's called the FSARC and they do wholesale payments and other things. So, there has been this other testing and that's been more

consistent with what this view is, which is, you know, how do you process when you have to go around the globe, right? It's an interconnected system for instance. So, that's a little bit different with both Amy and Steve described as how firms -- what we're hearing is how firms are thinking about the testing. It's alternate location, it's moving to manual processing, it's manual processing in an alternate location, and, you know, people probably stressing the duration now a little bit, you know, instead of two hours, what if it's four, what if it's eight, what if it's something else? All right. So, that thought process I think is filtering in to the exercise programs.

MR. GILBERT: John, any perspectives on testing from what you've -- your discussions with industry?

MR. BEEBE: Yeah, I think a couple of other things to add. I think the revolution or evolution here is the end-to-end test as opposed to application level testing. That is one of the big innovations. It think the big challenge that we hear from the industry is what do you do with third parties where that end-to-end

process is connected to a third party. How do you engage them in the test and are they willing to engage in the test and what does your contract look like? I think that's one of the places where we're hearing that there are some challenges and working through it.

MS. SHANLE: That was a big thing to in the FFIC handbook as well and the concept of testing. It's not just good enough to do a tabletop with your vendors or what have you so it will be interesting to see how that additional guidelines, you know, pan out.

MR. GILBERT: Let's stay on third parties for a second because, you know, with the advent of the cloud and there's so much innovation going on out there, third parties are critical to the provision of your financial services to your customers and clients. How are you thinking about third parties and the context of operational resilience and, John, I'm going to want to come back to you on this because the regulators have kind of a list of third party providers who are important to the financial ecosystem and have some interaction with them shall we say and so, I think an emerging question is, you know, does this need to

intensify? How are you guys thinking about third parties in this context and then we'll ask John to comment as well.

MR. HOSTETLER: Yeah, I can kick us off. So, I kind of break third parties into two components. Those that we hire and so, we (inaudible), we hire, we have an onboarding due diligence process, we have expectations, standards, QA. So, we have the ability to, you know, change those terms. I mean, not always within the contract, but over time we can evolve the expectations of third parties and ask them to participate more directly and work that we think is critical for resilience so that's on us and we can drive those changes and we will drive those changes.

The other kinds of third parties are ones that are customers select and so, we don't have as much necessarily control over them and we can't ask them to, you know -- we can't necessarily always control what their processes are, their level of cyber security resilience, things like that so there we probably need more help from people like John to help set expectations.

And the last piece is that third parties, while it creates complication and a little bit unknown in terms of the complexity of testing, it's not only a bad thing. It definitely can be a resilience enhancer in that it may create a substitute channel for us to transact, which is a good thing I think from a resilience perspective. If you have more than one payment system as an example to process transactions that's helpful when something fails. So, it's not a black or white. It only creates complexity. We do think it can enhance a firm's resilience and probably enhances systemic resilience, but they have to be part of the, you know, equation. Amy, your thoughts.

MS. SHANLE: Yeah and no, certainly agree with a lot of what you shared. Also, just two other items that come to mind and you mentioned the substitute ability factor of what that third party provides and knowing where you need to go to if they can't continue to provide that service and certainly, the governance of third parties, right? So, are you doing the proper due diligence in your questionnaires? Are you reviewing their testing and BCP policies and procedures and plans

as well? I think the governance is key to those third parties as well as you start to continue to ascertain their resiliency both testing with them and also, to your point, almost that fourth party concept too.

MR. GILBERT: John, you know, hedge funds aren't technically regulated, but you could argue that through the banking system, the provision of credit, the access to transaction services and so forth, they are in a sense. Is the same thing going to happen here with third party providers in the context of Operational Resilience or might the regulators go further? And I know it's early days, but conceptually, how are you all thinking about third party?

MR. BEEBE: So, I think, you know, in years past, we put third party risk management guidance and some general principles around how to manage the engagement with third parties. I think first cyber and now Operational Resilience has started to change that question or maybe our answers to that question. I think we spend more time through other government agencies thinking more broadly, you know, how do we address this issues, right? This is not just the banking regulatory

agencies. So, our policy folks will meet with treasury and they will bring in telecom and banking, you know, and try to address some of the questions through there. On the purely banking regulator side, we do have our significant service provider program. It tends to cover firms like Jack Henry and others that I've seen here today that service the smaller institutions. It doesn't necessarily get into some of the big cloud providers and others that could come under consideration, you know. I think that it's loge question, it's a loge debate. You know, I think I heard the comptroller say it takes about a year to get regulation through. I don't know. He might be optimistic. I think this is going to be a live discussion and the playing field will change as we're having the discussion and so, honestly, I'm not sure where that lands at this point. There are some basic expectations we have of the firms that deal with the third parties if they're going to choose to outsource something, you know, that's their choice, but they need to manage that relationship.

MR. GILBERT: Chris, any thoughts on that one?

MR. FEENEY: No, I'm good.

MR. GILBERT: Good. I want to talk a little bit about the market. We've talked a lot about harm to customers, but and, Amy, your firm has a unique position in the financial system especially with respect to the clearance of government security. And we've talked with, you know, other financial market utilities. You know, if they're the single point of failure, what are you all supposed to do?

MS. SHANLE: Yeah.

MR. GILBERT: And what are others supposed to do about you in the context of their own scenario planning and analysis for Operational Resilience?

MS. SHANLE: Yeah, I think you bring up a very good point that's peppered over a number of white papers, you know, the handbook and the like. Single point of failure is certainly a continued hot topic --

MR. GILBERT: Right.

MS. SHANLE: -- and the substitute ability factor as well continues to come in, you know, certainly from a -- if you look at the (inaudible) moves, there are some real, you know, key players here that you might not have a substitute. So, I think our thinking around

this is continuing to evolve with this new framework that we're putting into place, but it's really a hot topic across the number of areas as we work with the (inaudible) moves, as we work with our clients in the marketplace. How do we account for these single points of failure and how do we make sure that there's a resiliency process in place to respond to it? So, still evolving a bit in that maturation process.

MR. GILBERT: Steve, any?

MR. HOSTETLER: Yeah, I think just in the concept of where do you focus firm specific and industry wide exercise and prioritization? You know, the high single point of failure type choke points in the financial system in our view our worthy of more industry focus and more industry exercise.

MS. SHANLE: Yep.

MR. GILBERT: Chris, anything you want to --

MR. FEENEY: Well, no, just that the industry is definitely looking at it. I mean, you know, when I think through those tests, some of the ones we've discussed, the last test that treasury hosted that's part of the sector coordinating counselor was on third

party cloud providers for instance. We also did the one before that on communication in a crisis that how does the industry respond when social media is flaring and it's a major issue here, there, or the next place, but that's a whole different panel, which I'd be happy to stay for if anyone would like.

MR. GILBERT: Okay. We got a really good question from the audience about connecting this to risk appetite and communication with Board about the state of play of the resilience of your firm. How do you put this in the context of risk appetite? How do you describe to your senior management and Board and other key stakeholders whether you become more resilient, you're less resilient, you're the same? How do they know progress is being made?

MS. SHANLE: Want me to start? Okay. Cool. So, we have very active dialogue and engagement with our Board and the respective committees. I think what you're really touching upon is metrics. What are the resiliency metrics that tell the story and tell management how resilient are we? I mean, certainly, you can look at a RTO and check the box. You said you

needed it in two hours, it came up in two hours. That's a nice easy story. Regulator like it. It's an easy fix. But if you're looking at it from, you know, and I think, Chris, you mentioned this, too, there's a lot of qualitative factors that have to come into play. So, as we continue to mature in how we measure and demonstrate a resiliency, some of those metrics may be more qualitative in nature. Certainly, building off of risk appetite statements, KRI's, where applicable to our Operational Resiliency, but that is that broader stress continuum that that impact tolerance piece will continue to be critical under that as well, but I think you can't just look at these things from a quantitative perspective. You have to look at it from a more qualitative perspective as well. I don't if that's your thought, Steve, or Chris.

MR. HOSTETLER: Yeah, we are absolutely early in terms of we definitely have not defined KRI's for resilience kind of hard core metrics there. I think initially our view is we walk the process, we show the progress, we actually go through the scope of work for each of our services. Our key learning is from that so

we're very interested in talking about what we're finding, what we're learning, and then the decision-making process we make around how we can mitigate those risks whether those are new tech investments or new business plans, you know, exercises. So, that's sort of walking the talk as where we think we will be spending time in the near term and then if that can become more metric driven and we can quantify across the scope of work, you know, we will do that, but initially it's going to be walking the process.

MR. GILBERT: John, how does that grab you the way that they're thinking about risk appetite?

MR. BEEBE: So, I think it aligns with what I said earlier about having some synoecism around having numeric risk appetite for non-financial risks Operational Resilience. I think, you know, there needs to be some numbers that are indicative and then the qualitative piece with it. I've seen banks -- I sort of stumbled into Operational Resilience because I was a Board effectiveness kind of guy. Don't make me explain the story to you, but I think we've seen banks do different things with different Boards to help them

understand a risk and keep track with how things are changing and for complex things like this, numbers never work in totality. You need more and I think there are a lot of different ways depending on your Board to handle it, but definitely needs to be a qualitative piece.

MR. GILBERT: Chris, anything?

MR. FEENEY: No, I'm good.

MR. GILBERT: Okay. So, we've just a couple of minutes left and I want to ask a couple of kind of lightning round questions. So, first, for Amy and Steve and Chris, should the regulators set clear requirements in the near term or should they wait to see how practice evolve, gather insights, and regulate later if necessary?

MR. FEENEY: Near term quantitative? I think there's some time that we need, industry and regulators, to continue the discussion. I think it's a little early to set them yet, but, you know, maybe a year from now we wake up, we've had the discussion, they've been out in the field looking at the work that's been done. That just feels pragmatic to me, but that's a non-operator's view.

MS. SHANLE: Yeah, I mean, we think we continue to support a principles based approach verse the prescriptive nature, but I would agree with Chris as well.

MR. HOSTETLER: And the opportunity for, you know, collaboration here, learning, sharing best practices both, you know, between regulators and firm, between firms, we feel like that's critical so if we could find means to communicate quickly on that, that would be awesome and, you know, what are the mechanisms that we drive that kind of information sharing.

MS. SHANLE: And global coordination.

MR. FEENEY: Global is important, right, because, you know, it's the language issue and you choose different words and have different definitions and the regulators, at least U.S. and the Basel Committee, are key on having a common lexica. The other thing I wanted to note is going up into the boardroom, you know, the regulators are going to see this swath of different firms and I've heard the CEO say this multiple times, if you see something, say something kind of thing. Like, we want to know, right? This is all about

getting it right. We all agree we need to be resilient, we need to be even more resilient then we are today. So, you got to just keep that in mind. That's good input for firms actually.

MR. GILBERT: John, will it be possible to say principles base for a long time or when somebody, you know, having had a lot of experience in the international regulatory community myself, once somebody puts a stake in the ground and starts to really hone on something and define it clearly, it's hard for others to resist that because it feels like an emerging best practice or standard and principles sometimes get sacrificed to the snowball effect of harder policies. What's your take on that.

MR. BEEBE: So, I think we can stay, and this is projecting into the future so it's probably going to be wrong, but I think we can stay principles based for a while and if the industry continues to move to be more resilient, then you can stay with principles based. I think you need the standard when the industry view is well, you know, if it goes down for six weeks, we don't care and then the regulator steps in because the market

hasn't solved that problem. But if the industry is moving along and the principles are helping move along, then we can stay there.

I would like to add. One of the things that I worried about sort of the first BPI conference I did or meeting I did there was a lot of talk about harmonization and having the same language and sort of the same requirements, it did worry me that were getting a little too focused on what are the boxes we need to check so we get a good exam versus how do we get resilient and I think the only reason Chris or anybody else knows me is because I raised my hand. I said, "Wait, you know, we don't want to make this a box checking exercise. This really is about having systems that you can recover in an event." And so, I think if principles get us there, we can do that. I do think there is a debate internally whether we need standards or not. I just think it's really hard to set a standard in a topic like this.

MR. GILBERT: Well, that's a good place to park this issue for now. Stay tuned, strap in, it will get interesting because this tug of war around

principles versus hard standards is one that evolves quickly sometimes and we'll have to all pay attention and I bet a year from now we'll have a whole lot more to say on this very important topic. So, thank you for your attention, thank you for your questions, enjoy the rest of the conference.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020