TC Webinar Series:
Revised Core Principles for effective banking supervision
Part 4: Operational Resilience and Proportionality

Panelists:

Chuchi G. Fonacier

Deputy Governor, Bangko Sentral ng Pilipinas (Central Bank of the Philippines)

Jessica Chew

Deputy Governor, Bank Negara Malaysia

Moderator:

Bill Coen

Former Secretary General, Basel Committee on Banking Supervision; Board Member and Chair, Finance, Audit and Risk Committee, Toronto Centre

Date:

Sept. 18, 2024

Transcript:

Babak Abbaszadeh:

It is great to be here. I'm Babak Abbaszadeh, CEO of Toronto Centre. For those of you who were with us for a couple of minutes, sorry about the silence. There's a lot of people registered. I know it felt like being inside an elevator, but we needed to make sure everyone gets into the Zoom room. Welcome to our fourth panel on the revised Basel Core Principles, we have one more left after this. Today, we'll focus on operational resilience and proportionality. You may recognize Bill Coen here; I don't know why but whenever Bill appears, our numbers just go through the roof. So, Bill, right now we have 442 or more people registered from 95 countries covering all letters of alphabet from Algeria to Zambia and everything in between, probably around 40 agencies. I think we've got to keep bringing you back to our webinars. Maybe it is the ladies, I don't know, but the point is it's a very successful webinar.

So anyway, since our establishment in 1998, Toronto Centre has trained more than 28,000 financial supervisors from 190 countries and territories to build more stable, resilient, and inclusive financial systems. I'd like to thank Global Affairs Canada, the Swedish SIDA, IMF, and other valued international partners who make our programs possible.

If you step back and look at it, over the past two decades or so, we've witnessed a number of threats to the stability of the financial system. They range from the Global Financial Crisis to unprecedented technological advances that are still continuing, AI, everything else, FinTechs, COVID-19 (who can forget that), to the rising geopolitical risks that were really not on the horizon a few years ago. So, it shouldn't come as a surprise that banks' operational resilience has become a crucial supervisory priority. Banks now face increased risk from system failures, diverse cyber-attacks, terrorism, regional conflicts, and natural disasters. Compounding this is the growing reliance on third parties, which adds complexity to operations and incident analysis.

The Core Principles for effective banking supervision emphasize proportionality, ensuring that rules and practices align with banks' systemic importance and risk profiles while reflecting local conditions and supervisory capacities without compromising standard robustness. I know we're focusing on banking today, but probably everything I'm saying here can apply to other sectors as well, as we live in a very strong, cross-sectoral - universe. But let's bring our focus back to the banking sector. We congratulate the Basel Committee for amending the core principles for effective banking supervision to reflect on operational resilience and proportionality.

> The regulatory work, Basel III, and several other rules, that's behind us. This is real world stuff that we're talking about today.
>
> **Bill Coen**
> Toronto Centre

Today, our distinguished panel will discuss the importance of operational resilience for banks in a rapidly changing world, as well as the role of proportionality in effectively scaling standards for different banking sectors. I'm honored to welcome Chuchi G. Fonacier, the Deputy Governor of the Central Bank of the Philippines, and also Jessica Chew, Deputy Governor of Bank Negara Malaysia, who's appeared in some of our previous programs as well. This conversation will be moderated by Bill Coen, former Secretary General, Basel Committee on Banking Supervision, who's also a very valued member of our board of directors and the Chair of our Finance, Audit and Risk Committee of Toronto Centre. Welcome to our speakers and moderators. You've seen their bios, so I'm not going to take time to read them. Now, it is my pleasure to hand the podium over to Bill. Bill, please proceed. Thank you.

Bill Coen:

Babak, thank you very much, and it really is my honor to moderate this panel. So, thanks to you Babak, and the Toronto Centre, and congratulations to the Toronto Centre. This webinar is, in my view, a perfect representation of what the supervisory community should be looking at. We spent more than a decade recasting the rule book, Basel III, and there's so much media attention, so much political attention, and so much industry attention on the new rule book, and not enough, in my view, of what the regulatory community, the supervisory community really should be doing, and that's putting the rules in place, careful, prudent oversight of their institutions, using their judgment. Babak, the things that you mentioned, cyber resilience, operational resilience, the digitalization of the world, pandemic effects; this is real world stuff. The regulatory work, Basel III, and several other rules, that's behind us. This is real world stuff that we're talking about today. So, congratulations to Babak, Demet, and the Toronto Centre for

establishing this series of webinars on the Basel Core Principles for effective banking supervision. This is hardcore supervision, and this is really what we should be thinking about and talking about.

It's also a privilege for me to moderate a session with two women I've worked with, and I've known for many years. Ladies, thank you very much for your time today and participating in this panel. Jessica, if I can start with you, I'd like to start off with operational resilience. Just to get a flavor of your region, Malaysia, tell us what's the top current and emerging threats to bank operational resilience in Malaysia?

Jessica Chew:

Thank you, Bill. I hope you can hear me fine. It's a real privilege for me to be on the panel today with Chuchi, and obviously with your moderating. It seems even as I'm starting my remarks, it seems that it isn't that long ago that we were in a COVID-19 crisis, and I think if anything, that was perhaps the test of operational resilience of this decade and probably beyond as well. So, for Malaysia, we run an annual survey of emerging operational risks, and for the last seven consecutive years, technology and cyber risks have topped that list for most of our banks, in fact all of them.

> In Malaysia, we run an annual survey of emerging operational risks, and for the last seven consecutive years, technology and cyber risks have topped that list.
>
> **Jessica Chew**
> Bank Negara Malaysia

I just wanted to make a couple of points about this observation. I think obviously the rapid adoption of technology and reliance on third parties across business functions and processes, and this goes beyond just customer onboarding, which was typical in the past, but also now the provisioning of critical services. Now this has intensified risks significantly as a result of four factors. One, the pervasiveness of technology adoption. We've not seen this level of diffusion of technology across all business functions in financial institutions to date. Secondly, the criticality of activities involved. Thirdly, the more complex interactions and interdependencies that have arisen from the rapid adoption of technology that we're seeing. And finally, the thing that's also different is the proliferation of cybercrime business models such as cybercrime as a service and ransomware as a service. That's making the challenge of defending against cyber and operational risks that much more difficult.

So, the implications for us have been firstly, obviously high exposure to single points of failure. That's been a very relevant consideration for us. Secondly, the impact from cyber and technology incidents now occurs and materializes much faster because of straight through processing and things like that and is also much more widespread. And finally, incident response and recovery is more challenging for financial institutions because it requires really close coordination and stronger risk assessment capabilities. For example, there is now a need to really understand interdependencies, to anticipate second order impacts of disruptions, and to be able to react swiftly to likely responses of threat actors, customers, and business counterparts.

Risks associated with outsourcing and third-party service providers are also increasing. This is compounded by the reality that non-substitutability of IT systems and cloud services within the maximum tolerable down times for critical business functions. That's been difficult, and the reality is even if we do say in theory that we expect banks to have continuity plans, many of these systems and services are not really substitutable within the maximum tolerable down times that banks have set for themselves.

There's also the core issue of very complex legacy systems within financial institutions, and we've observed a reluctance by banks to accelerate the modernization of their systems in favor of other priorities.

Jessica Chew
Bank Negara Malaysia

Risks are compounded by the concentration of dominant third-party service providers at the system-wide level. So, in Malaysia we've developed contagion maps to identify system level concentrations, and we simulate failures of systemic third-party service providers to test incident response plans, and that's surfaced very valuable insights. For example, in incident response and recovery plans, in a test of cash operations that we conducted recently, there were only four major service providers and because all of the recovery plans had banks switching to an alternate, the alternate service provider just didn't have the capacity to ramp up to support the number of institutions that were turning to them. So, these insights became something that banks had not factored into their incident response and recovery plans.

There is also a lack of visibility in the subcontracting and supply chain risk. This is very often underestimated and subject to insufficient oversight. The cost of actions to mitigate outsourcing and third-party risk, we believe is going to increase substantially, because of our expectations, because of what banks are discovering they need to do to close gaps, and I think going forward this could potentially alter the calculus for outsourcing decisions by banks, and I think that's something that we cannot rule out as well.

Finally, Bill, my last point, I think is an observation that we continue to see technology outages recur. We know the root causes, they are commonly latent system vulnerabilities, presence of unmitigated single points of failures, inadequate management of obsolescence risks, technology architectures that are not managed properly, and gaps as I mentioned in incident response and recovery plans. The challenge is that the core issues to achieve a higher level of maturity required to deliver longer term fixes to deal with these recurring outages, these challenges remain.

Number one, talent and competency gaps are something that we're still really struggling with, and that's not to say there isn't good talent within financial institutions; there is very good talent within financial institutions, but what we're finding is many lack the skills and experience needed to effectively manage a fast moving, complex risk environment, and that's something that we've observed in simulations. There's also the core issue of very complex legacy systems within financial institutions, and we've observed a reluctance by banks to accelerate the modernization of their systems in favor of other priorities. So, incentives are also not well aligned, so the issue

remains unresolved. Finally, there is an expectation gap that has become something that we've discovered is really also challenging operational resilience responses. Online banking now means that there is a provision of ubiquitous 24/7 online banking services. The public expects those services to be available all the time, but technological operating models aren't built to the kind of standards that we're more accustomed to for large value payment systems, for example. I think that that expectation gap continues to challenge the response to operational risks that we're seeing in our banks. So, let me pause there and we can make more observations later.

Bill Coen:

Fantastic. Thank you, Jessica. The Basel Committee organized an international conference of banking supervisors a few months ago, around the same time as it published the revised Basel Core Principles. This whole topic, one of the things that you just mentioned, outsourcing reliance on third party, sometimes fourth party service providers, talents and skills, or retaining talent and attracting the kind of talent and skills that we need, legacy system, and incident response and recovery, these are all topics that are important issues in Malaysia. I know for a fact these are global issues, and every jurisdiction that I'm familiar with is struggling with all the issues you just mentioned. So, thanks for putting them on the table. I asked what are the current and emerging threats, and you gave me a long list, but I think it's a great start because it's something that if it's not on everyone's mind, everyone participating in this webinar, these are the topics that should be on your mind. Thank you very much Jessica.

> The Philippines is consistently ranked as one of the most vulnerable countries to climate change. The recurring exposure of Philippine banks to calamities has enabled these banks to beef up their disaster preparedness and business continuity planning.
>
> **Chuchi G. Fonacier**
> Central Bank of the Philippines

Chuchi, let me turn to you. In the Philippines, what kind of disruption in banking services have you experienced in the past year and how was the bank's response to the disruptions?

Chuchi G. Fonacier:

Thank you, Bill. I hope I'm getting there clear in your area. Before I respond to that, I'd like to thank of course the Toronto Centre for inviting the Bangko Sentral ng Pilipinas (BSP) to be taking part in this panel. Happy to share, and of course I'm honored with the experience of being with Bill on the panel moderating, and of course with Jessica.

Now going back to the question, there are actually two common triggers of business disruptions in the Philippines. The first is pertaining to extreme weather events, and the second is technology-related business disruptions. The Philippines is consistently ranked as one of the most vulnerable countries to climate change. The recurring exposure of Philippine banks to calamities has enabled these banks to beef up their disaster preparedness and business continuity planning. This means that there is less adjustment needed on the part of Philippine banks to attain operational resilience.

Let me share the experience of small banks whose operations were affected by Typhoon Rai, and that's the deadliest typhoon that hit the country, in 2021. We observed that small rural banks were able to restore operations in the immediate aftermath of Typhoon Rai, compared to branches of universal and commercial banks in the affected areas. Now, how were these banks able to do this? Ahead of the typhoon's landfall, rural banks stockpiled critical supplies, including gasoline for their generator sets and basic food supplies. So, digital online platforms also played a key role in the immediate restoration of their banking services. For instance, the core banking system and network solutions of some rural banks are cloud-based, and these banks maintained an internet - subscription to two of the main Philippine telecommunication companies. So, going back to the question, what did we learn from this experience? First is that the bank's business continuity and disaster recovery plans should include trigger points that will call for immediate coordination with other key stakeholders such as local government units, the Department of Energy, the Department of Information and Communications Technology, and also other various industry associations.

On the cybersecurity front, significant threats include malware, account takeover or identity theft, application programming interface (API) exploits, and also distributed denial of service (DDoS) attacks. These attacks cause major disruptions which lead to financial losses and damage reputations.

Chuchi G. Fonacier
Central Bank of the Philippines

Also, an industry-wide multi-stakeholder BCP and BRP will enable the key actors to undertake regular localized regional disaster resilience drills to better prepare for calamities. Meanwhile, since the BSP-supervised financial institutions, or we call it the BSFIs for short, are now into digitization or at least have simple systems used in their operations, the reports received by the BSP are mostly technology-related disruptions. For instance, in 2023, 80% of disruptions in the financial system stem from technology-related outages, while the remaining 20% were from cybersecurity-related threats. Frequent instances of technology-related outages include capacity concerns leading to application slowdown, preventive system maintenance, and also network connectivity problems. The unavailability of integration issues in third-party systems also caused disruptions in bank operations.

Now, on the cybersecurity front, significant threats include malware, account takeover or identity theft, application programming interface (API) exploits, and also distributed denial of service (DDoS) attacks. These attacks cause major disruptions which lead to financial losses and damage reputations.

For instance, the CrowdStrike blue screen of death issue in July 2024, which affected Microsoft users worldwide, also caused disruptions in the operations of about 16 BSP-supervised financial institutions. Some of their critical functions were not accessible from one hour to about nine hours while service interruptions, largely partial unavailability of certain services, lasted up to 24 hours or more.

So, the experience highlighted the importance of communication in times of disruption. So, the bigger banks quickly released advisories and information on other banking channels that were available to provide services which appeased the public. But the BSP also issued a statement that it's closely monitoring the incident that affected banks and that are already addressing the issue. Now, the BSP also reminded our supervised financial institutions to adhere to existing regulatory requirements on the adoption of comprehensive cyber defense and resiliency strategies. On their part, the banks and other financial institutions are rolling out security awareness and education campaigns, implementing multifactor authentication for high-risk systems and transactions, that's to minimize cyber fraud, and also conducting tests on the business continuity and cyber incident response plans to ensure these plans function as intended. So, the conduct of investigation and root cause analysis are also in place to ensure that incidents, including those causing business disruptions, will not occur. I think I'll stop there for now, Bill.

> Supervisors, of course, play a critical role in promoting operational resilience in the financial industry. So, we have developed in-house training modules covering areas relevant to operational resilience.
>
> **Chuchi G. Fonacier**
> Central Bank of the Philippines

Bill Coen:

Thanks, Chuchi, really interesting. A couple of things you mentioned a few times: the importance of collaboration among the various stakeholders. It's not just between the central bank and supervised authorized institutions, it's everyone involved including customers, and other stakeholders like the third-party service providers. It is a collaborative effort that involves a lot of people, and that's why the last thing you were talking about, communications and just creating awareness. So, that's really important. It sounds like the BSP has a very strong program there.

Chuchi, if we can stay with you for a moment, I'd like to come back to something that Jessica had mentioned, and that has to do with training, recruitment, and talent management. All the banks I speak with, that's a common thread: the ability to attract and retain staff. Things that both of you, Jessica and Chuchi, you've discussed today with us, the digitalized world, and things of course will continue in that vein. In the Philippines, how do you ensure that your staff, the supervisory staff, have the right capabilities in operational resilience? There's such competition for that kind of talent, those kinds of skills. How do you do it?

Chuchi G. Fonacier:

Yeah, thank you, Bill. So, we really recognize that our supervisors, of course, play a critical role in promoting operational resilience in the financial industry. So, we have developed in-house training modules covering areas relevant to operational resilience, and we also tap the support of a development partner for technical assistance.

Now, pertaining to our in-house development, training program, we have what we call the Professional Excellence Program for Supervisors, or we call this PEPS for short, which is as I

mentioned, an in-house structured training program for supervisors. So, the PEPS offers everything from entry-level all the way to expert-level courses. So, it's a “ladderized” training program covering key areas relevant to supervision, including those related to operational resilience.

We have also what we call the Technology Risk Supervision course, which is a part of this PEPS that we have. So, this comprehensive program is tailored to address the evolving risks emanating from financial institutions' increasing reliance on technology. So, key areas covered include cybersecurity, IT governance, risk management, and technology recovery and resilience, among others.

As I also mentioned, we also benefited from the technical assistance (TA) from the IMF in equipping our supervisors with the right capabilities on operational resilience. The IMF TA was delivered in two phases. Phase one supported the development of operational resilience regulations, and this phase focused on first, identifying regulatory gaps, then second, understanding the linkages of operational risk management, business continuity management, and information technology risk management with operational resilience. Third, developing the guidelines on operational resilience for Philippine banks. Now for phase two, we were supported with the integration of operational resilience as a factor in our existing supervisory assessment framework. This phase covered capacity building for supervisors, wherein the IMF conducted trainings that emphasized that the BSP may leverage existing engagements and touchpoints in the supervisory cycle to include operational resilience.

We also created a technical working group (TWG) that was tasked to develop training materials for both internal and external stakeholders based on the learnings from the TA. This TWG will also develop internal guidelines to facilitate the implementation of the regulations on operational resilience. So, the guidelines will include good practices or benchmarks that may be used as reference in the conduct of supervision. I think I'll stop there for now, Bill.

Bill Coen:

Thanks, Chuchi. So, this is a well-thought-out, carefully considered program with a couple of different phases. I should also add a shameless plug for the Toronto Centre. When you talk about technical assistance and capacity building, the Toronto Centre has a terrific program in that regard.

I'm glad you mentioned the IMF because it's just another reason why the Basel Core Principles are important. There is a specific standalone core principle, number 25, on operational risk and operational resilience. Of course, the IMF and the World Bank and their Financial Sector Assessment Program will evaluate a country's adherence to the Basel Core Principles. Another reason, as if it wasn't already important enough to address the issues that both Chuchi, you and Jessica have been discussing today, you want to be seen as in full compliance with the Basel Core Principles.

Jessica, on this topic of operational resilience, and from a supervisory perspective, where the rubber hits the road as people say, how exactly is it being done in Bank Negara? How do you make sure it's embedded in the supervisory approach, checking the operational resilience?

Jessica Chew:

Thank you, Bill. So, in Malaysia, we have, for some time now, adopted a risk-based supervisory framework, and there are significant activities of financial institutions that are identified and they're subject to supervisory reviews. Part of that framework provides for an operational management review of every significant activity. This would cover our assessment of how the financial institution is managing strategic, financial, governance, execution, and even integrity risks – the money laundering and terrorist financing risks as well.

It's a two-track process. There is the first track, which looks at significant activities and evaluates how those activities are managed by operational line managers, and then there is an overlay of that, where assessments are conducted of the quality of the overall enterprise-wide risk management control functions. This would cover, across all activities, the effectiveness of board and senior management oversight, risk management functions, the compliance functions, and the audit functions. So, it's very much embedded into both the first track and the second track of the supervisory assessment process. But we've realized that given the evolution, the nature, and complexity of technology and cyber risk, we have a dedicated unit that is called the IT Supervision Unit. We established this, with a headcount now that's about 43, who are dedicated supervisors that undertake deep dives into supervisory reviews of technology and cyber risk management of banks and insurance companies. I think this has a number of benefits. One obviously, we are able to devote a specific focus to this area of operational risk.

Secondly, and more importantly, I think for us it was the need to consolidate our knowledge and expertise in this space and to really be able to be more effective in building capabilities within what we consider to be quite a specialized area. We also do event driven supervisory reviews. We may conduct this, for example, in connection with applications that we get from financial institutions on cloud adoption, or if they wish to outsource material business functions that might trigger a supervisory review to understand how they have identified and plan to manage these risks. All of these assessments are obviously done and assessed against standards that we set for the management of operational risk, and they're very much aligned with what the Basel Committee on Banking Supervision BCBS has issued in their principles for operational resilience and the revised principles for the sound management of operational risk. But in our case, it spans five different policy documents. So, we've got a policy document on operational risk, a separate one on business continuity management (BCM), a separate one on stress testing, and then there is a dedicated supervisory standard on risk management of information technology risk, and another one on outsourcing. So, we continue to update these documents, and I think that's been one of the challenges, just keeping the regulatory requirements fresh and current as the world changes as rapidly as it does.

So, what we end up doing is from time to time, and it does happen pretty frequently, we issue additional supplementary guidance to deal with specific issues. For example, we've just issued guidance on cloud risk management. We issued one in June this year, saying that we wanted banks to undertake technology stress tests based on common scenarios, so that we could surface some horizontal issues. So that went out in June this year, and we are currently in the process of refreshing our risk management and information technology policy document, to strengthen expectations for financial institutions, but to raise the level of resilience against large-scale system outages. This includes requirements for them to strengthen contingency

arrangements, to make sure that they're able to avert multiple service outages, and also, we're raising standards in terms of how we expect FIs to manage third-party risk on a continuing basis and not just at the point when they are appointed.

We also undertake thematic reviews and stress testing, and these efforts to help provide additional insights on operational vulnerabilities at the system level, which I alluded to earlier. It also supports our efforts to raise standards, actually, across all FIs. So, when we undertake thematic reviews and they focus on a particular area, the outcomes of those reviews are shared with the industry, and we also use that as an effective way to just raise standards across the board. Sometimes, we do these reviews in response to specific emerging risks that we identify, for example, around disaster recovery arrangements. When we saw an uptick in technology related outages, we did a thematic review on branch operations. We also did one when we saw an uptick in the reporting of non-compliances or fraud incidents at the branch level. Other times we do them as part of our planned cycle of reviews to observe implementation of risk management standards by financial institutions.

> We're raising standards in terms of how we expect FIs to manage third-party risk on a continuing basis and not just at the point when they are appointed.
>
> **Jessica Chew**
> Bank Negara Malaysia

More recently, as I mentioned, we've required FIs to undertake stress tests based on defined common scenarios. So, one of them, for example, is a simulation of a destructive cyber-attack at a third-party service provider. We're finding that these common scenarios help to improve the rigor of the crisis and stress test simulations that they do around operational risk. More importantly, it has helped been valuable to surface common vulnerabilities across financial institutions. Of course, I think like many others, we do cyber drills and simulation exercises as well that involve financial institutions. So, these are industry-wide exercises.

I'll just close this with a point about the important role supervisors play in galvanizing coordinated action. So, you mentioned collaboration earlier, Bill, and I think in our case that's been really crucial. We've really had to step forward to coordinate efforts around, for example, the sharing of cyber threat intelligence. I think without the supervisors stepping in, it would be impossible to get financial institutions to collaborate. Increasingly that has been something that we've been very active in. We've got a national scam response center where we collaborate with other law enforcement agencies and we facilitate regular forums where we bring chief risk officers, chief information and security officers, cyber working groups, and the heads of operational risk together. It's been very helpful to align expectations and also review emerging threats and issues. I'll pause there, Bill.

Bill Coen:

Thank you, Jessica. Such an important point, the role of the supervisory authority in working with the industry, sharing information, and really taking a lead role. I also liked your point about the horizontal reviews. I've seen more and more jurisdictions doing this: make some kind of an assessment on cyber resilience or some other form of operational resilience, and share the

results to say, "Here are some of the best practices. Here are some of the common deficiencies, common weaknesses that we've seen." From a bank's perspective, it is so important. Both of you have talked about the many, many challenges, and supervision is a tough job: and its scope is just expanding more and more, and we're expecting more and more of banks.

The traditional risks like credit risk, market risk, and operational risk, of course, are now so much larger because of a digitalized world. Everyone has limited resources: human resources and financial resources, so this leads me to the question of proportionality. Proportionality is mentioned prominently in the Basel Core Principles. It underpins everything.

The traditional risks like credit risk, market risk, and operational risk, of course, are now so much larger because of a digitalized world.

Bill Coen
Toronto Centre

As senior officials of your central banks, I'd like to get your perspectives on this question of proportionality. Chuchi, if I could start with you. Which areas of the Basel Framework have you found challenging in implementing in a proportionate way?

Chuchi G. Fonacier:

Thank you, Bill. Actually, in order to effectively apply the principle of proportionality, regulators must have a deep understanding of the business model and the risks inherent in the operations of banks. So, these are important inputs to the design of the regulatory framework governing the Basel Core Principles and its scope of application. So, the Philippines is home to diverse types of banks, large and complex, banks such as universal and commercial banks and digital banks that operate alongside small banks. So, large banks dominate the industry in terms of resources and customer reach, meanwhile small, rural and the cooperative banks, if taken as a collective unit, maintain an extensive regional footprint. These small banks are systemic in the areas where they operate because they play a key role in driving economic growth in their respective communities.

Within each banking category, there may also be banks whose operations may differ from their peers in the group. And so, to address this challenge, the BSP has adopted principle-based regulations that allow the exercise of supervisory judgment. For instance, in applying the Basel corporate governance and risk management standards, banks are classified as simple or complex. By default, universal and commercial banks and digital banks are classified as complex, while the rural, or a cooperative bank, is considered a simple bank. But the BSP, however, is not precluded from reclassifying a simple bank as complex if our supervisory assessment of the bank's asset size, the branch network, complexity of its products and services, the business model, or the risk appetite indicates that there is merit or to reclassifying such bank.

Another area that we find challenging is the identification of the minimum standards that will be adopted for simple banks. In the case of the BSP, we endeavor to incorporate in our regulations the minimum standards expected of simple banks, and that's to provide these banks with a guide in enhancing their corporate governance and risk management systems. For instance, in the area of corporate governance, complex banks are required to constitute at a minimum three

board-level committees, which include the audit committee, the corporate governance committee, and the risk oversight committee. So, universal and commercial banks that are part of a conglomerate are also required to create a related party transactions committee. Meanwhile, simple banks are only required to constitute the audit committee, unless their operations necessitate the creation of other board level committees. So, this is on the condition that the board shall discuss corporate governance and risk management matters, and that the views of the independent director shall be duly considered and minuted.

Now, in terms of liquidity risk management, complex banks with active treasury operations are expected to adopt more dynamic approaches in a range of techniques that factor in the future changes in their activities and balance sheet. Simple banks are allowed to use a static approach to liquidity risk measurement, and this may consist of a simple cash flow projection in a spreadsheet where the bank's sources and uses of cash over different time horizons may be analyzed. We have also recently issued guidelines on the preparation of recovery plans for banks with simple operations. Now, in order for the BSP to be able to do this, we need to know the range of approaches that are adopted by large and small banks in managing a specific risk and identify the approach that would be best suited for these banks.

In terms of liquidity risk management, complex banks with active treasury operations are expected to adopt more dynamic approaches in a range of techniques that factor in the future changes in their activities and balance sheet.

Chuchi G. Fonacier
Central Bank of the Philippines

Lastly, another area which we find challenging is the application of proportionality in supervision. So, since the BSP's regulations on corporate governance and risk management are largely principles-based, supervisors must exercise good judgment in undertaking supervisory assessments. Now, to ensure consistent implementation and application of the standards, we have issued internal guidance, conducted trainings, and established avenues for supervisors to discuss their supervisory findings, observations, and corresponding enforcement actions at the technical as well as management level. So, I'll pause here for now, Bill. Thank you.

Bill Coen:

Thank you, Chuchi. It sounds like a very reasonable approach. I particularly like what you said about requiring recovery and resolution plans for less complex banks. Everyone thinks when they hear about recovery and resolution they think, "Well, that's just for a global systemically important bank (SIB) or domestic SIB." But as we've seen, disruption in certain parts of an economy or certain parts of the banking system can easily cascade and have contagion effects. I've experienced this firsthand; I started my career in the 1980s in the US and we had what was called the savings and loan crisis. A class of really small banks, for the most part, none of which were domestically systemically important, certainly not GSIBs, but in the aggregate their weaknesses led to some major economic problems in the US. So, thanks for that.

Jessica, I'd like to get your and Bank Negara's views on this issue of proportionality, both from a regulatory and a supervisory perspective, and then we'll open it to the audience. I see a few questions, but first, Jessica, what are your views and Bank of Negara's views on proportionality?

Proportionality has to be informed by robust assessments of risk, and I think here the tendency has been to focus mainly on size and complexity, but as recent banking turmoil episodes have shown, we do need to deepen our understanding of how risks are transmitted, and I think that calls for a more comprehensive and careful consideration of how we look at risk.

Jessica Chew
Bank Negara Malaysi

Jessica Chew:

Thanks, Bill. So, we're guided by several considerations and guiding principles as we consider how we operationalize a proportionate approach. One is obviously the goal being to try and optimize costs and benefits of regulation by scaling our regulatory and supervisory expectations appropriately based on risk. We have several outcomes that we keep clearly in mind. One, obviously overriding everything, is the interest of preserving financial system stability, avoiding at the same time the effects of stifling growth and innovation. Managing risks of financial exclusion is also an important consideration for us. At the same time, we want to make sure that we're promoting a level playing field for competition. Proportionality has to be informed by robust assessments of risk, and I think here the tendency has been to focus mainly on size and complexity, but as recent banking turmoil episodes have shown, we do need to deepen our understanding of how risks are transmitted, and I think that calls for a more comprehensive and careful consideration of how we look at risk.

Capacity considerations have also been an important factor for us. So, we have gone through periods where we've allowed for the gradual elevation of standards as capacity is built up, and this allows us, for example, to move from predominantly rules-based regulations to more principle-based, as capacity both at our end as well as the financial institution's end matures. For us, one of the key issues that we've had to continually come back to has been defining the supervisory risk appetite. So, it's one thing to say we want to implement a proportionate approach, and if that's not well aligned with the internal supervisory appetite, then I think it does create a wedge between the supervisory responses and expectations both of the public and of the leadership within the authority itself. So, that's something that we keep having to come back to make sure that how we are operationalizing a proportionate approach is aligned with our own supervisory risk appetite as an organization.

We want to also make sure that we're providing a reasonable level of predictability to firms. Maybe on this, one of the points that I think is worth making is that our approach to proportionate regulation and supervision has been very much centered around our ability to also implement robust supervisory processes that guide supervisory judgments. So, for Bank Negara, for example, we put a lot of effort into developing baseline good practices, and so that allows supervisors as they're exercising discretion and judgment, there is some consistency and

predictability in how firms expect us to respond to their practices. We have review panels that look at, challenge, and validate supervisory composite risk ratings. In our case, we call them composite risk ratings for financial institutions. We have policy clinics when we issue new standards to make sure that supervisor's interpretation and how they view the application of those standards within a bank is also consistent. At least there's a forum where we're discussing these issues and making sure that we're converging. We make use of implementation guidance and FAQs to also communicate our expectations.

So, these are just some of the key ways that we try and operationalize proportionality in our regulation and supervision framework. We don't segmentize our institutions, unlike in the Philippines. So, the same rules-based requirements apply to all FIs. But over time, as I mentioned, we've moved quite a lot of what were previously rules to more principles-based and overlaying that with the supervisory assessment and discretion and judgment. I'll just pause there because I'm mindful of time and I know we can take questions and continue the conversation.

> When we do stress testing as well as simulations, it is very important to do it together and with the involvement of the third-party service provider. I think that, in our experience, has helped surface some issues to the third parties, which have opened up opportunities to close gaps.
>
> **Jessica Chew**
> Bank Negara Malaysi

Bill Coen:

Yeah, this is really interesting, and really, we could talk about this for a long time. Jessica, I like what you said about, and this is such a core part of financial institution supervision, the need to balance innovation with safety and soundness considerations and the need for predictability, as you called it. Really good points. I also like what you said about having a supervisory risk appetite. We always tell banks, "You need to articulate your risk appetite." But that's true from the supervisor's side as well. So, in the remaining few minutes, we're going to do a rapid fire. We got some really good questions, so I'm going to pose a question. Starting with Jessica, I'll ask each of you to just give a one-minute response to the extent that you can. Sorry for that, but we've got some really good questions. The first one is from Richa Goyal, and Jessica, I'd like to get your response to this. What measures can supervisors take to mitigate the risk arising from reliance on third parties for critical operations?

Jessica Chew:

Thank you. I've just mentioned that we are raising standards for monitoring of third-party rates and making sure that that's monitored on a continuous basis, so it includes requirements like expecting third parties to undertake independent assessment of their cyber maturity levels, and having FIs make sure that they're receiving that and reviewing that on a continuous basis. That's really important. The other one that I would mention perhaps is stress testing. I think when we do stress testing as well as simulations, it is very important to do it together and with the involvement of the third-party service provider. I think that, in our experience, has helped surface some issues to the third parties, which have opened up opportunities to close gaps.

Bill Coen:

Excellent. Thank you, Jessica. Stress testing, continuous monitoring; Chuchi, is there anything you'd like to add to that?

Chuchi G. Fonacier:

Yeah, I think, Bill, also by having clear expectations from our supervised institutions, this would also require that they conduct thorough due diligence on the third-party providers, ensuring that contracts include strong service level agreements. Mandating compliance, of course, with data protection, cybersecurity, and regulatory standards across jurisdictions, as well as of course, performing regular financial and performance evaluation as well of these third parties. Also, another one that's important is cross-jurisdictional cooperation as well. That of course, is where regulators can work together to harmonize standards and can facilitate, as well, mutual recognition agreements, all in the interest of enhancing transparency, and as I mentioned, setting clear expectations.

By having clear expectations from our supervised institutions, this would also require that they conduct thorough due diligence on the third-party providers, ensuring that contracts include strong service level agreements.

Chuchi G. Fonacier
Central Bank of the Philippines

Bill Coen:

Chuchi, that's a really good point. We mentioned collaboration, but that's a dimension that is really important, the cross-border collaboration with other authorities, not just bank supervisors, but consumer protection perhaps, and certainly central banks. Chuchi, how are regulators dealing with systemic concentration risk? Cloud providers could be a prime example. You've got one company perhaps that is the dominant firm in that particular area. What are the respective banks doing to deal with that?

Chuchi G. Fonacier:

Actually, for the part of the regulator, we should really conduct regular monitoring and surveillance as far as the emerging risks are concerned, and we can flag the risks that will eventually, for instance, lead to a concentration risk. So, we should be informed by data that are being submitted to the BSP and also the results of our stress testing exercise. We do surveys as well and we gather inputs from the industry on what we have also discussed. And, of course, that will circle back as well to setting clear expectations, but really, very good surveillance should be in place for these types of developments.

Bill Coen:

Okay, good. Thanks. That question comes to us from Kathryn Aggio, so thanks for that question. Jessica, anything you'd like to add to that?

Jessica Chew:

Yeah, so we are asking banks to have multi-site and multi-region backup arrangements to mitigate risks of concentration to a single provider. Again, in some extreme cases where we have remained not satisfied with how the bank is mitigating and managing these risks, we're actually nudging some of these banks to put in place defined strategies for exiting critical third-party service providers where necessary. This is a huge effort, and we reserve such actions for pretty exceptional cases where a series of interventions where we're not seeing the kind of progress that we need, and they are important institutions in the system. But it does involve a multi-year extensive plan, and it's very costly and it's really actually requiring banks to develop an alternate technology roadmap that will allow them to actually port over these services to another service provider. Again, we are contemplating such actions for at least one institution, but it would be the nuclear option almost.

Bill Coen:

Yeah. I see we are almost at time. There was a very good question from Tia Greenidge. She asks, due to the competitive nature of financial institutions, are they reluctant to share information? I think this goes back to what we were talking about before with the horizontal reviews and the really important lessons that other banks can learn from their competitors, both strengths and weaknesses. I'm going to answer this question only because I think there's a very simple answer, and it's that information is collected on an anonymous basis, and it's reported on an anonymous basis. There's never an attribution to a specific bank or financial institution. An excellent practice in my view that I think everyone should do, but really, it needs to be done anonymously.

Ladies, I'm going to close with a simple request. We have some other really good questions that we were not able to get to. With my colleagues from the Toronto Centre, I'll answer some of these myself personally. I've got some strong views on the questions that we received. If it's okay, I'd like to be able to forward these questions to you, and if you have a response, I would really appreciate your response, and we could share it with those who wrote it. Or for my colleagues at the Toronto Centre, if there's a way to share the responses with the rest of the audience, I think we have a very full audience at this webinar today of more than 400 people in more than 100 countries. I think that would be great. So, there's nothing more for me to do than to give my sincere thanks to Chuchi and to Jessica, Deputy Governors, both of you, Philippines and Malaysia. I thank you for a really rich discussion, your insights, your experience. I felt this went really well, and I sincerely thank you for your time today.

Jessica Chew:

Thank you.

Chuchi G. Fonacier:

Thank you. Yeah, our pleasure. Yes.

Bill Coen:

Thanks for the questions, people who wrote in, and thank you for your time and your participation. I look forward to our next Toronto Centre webinar.