Sylvie: You're listening to a Toronto Centre podcast. Welcome. The goal of TC podcasts is to spread the knowledge and accumulated experience of global leaders, experts, and world-renowned specialists in financial supervision and regulation. In each episode, we'll delve into some of today's most pressing issues as it relates to financial supervision and regulation, the financial crisis, climate change, financial inclusion, Fintech, and much more. Enjoy this episode.

Babak Abbaszadeh: Hello everyone. I'm Babak Abbaszadeh, CEO of Toronto Centre. I'm delighted to be with you again today. And our distinguished speakers will discuss how we can help to sustain financial stability and inclusion in the digital era. The International Monetary Fund research indicates that without proper supervision, risks to financial stability increase when access to credit is expanded.

This research also indicates that investing in high-quality supervision can pay big dividends as financial inclusion expands. That's where Toronto Centre comes in. Since our inception in 1998, Toronto Centre has trained more than 15,000 supervisors from 190 countries and territories to build more stable, resilient, and inclusive financial systems.

We see financial inclusion and digital finance and the potential for poverty reduction and balancing the gender gap in finance as the key connective tissues of the Sustainable Development Goals. Consider the digital search accelerated by COVID-19. Today, conventional banks account for only 72% of the total market value of the global banking and payment industry. This is down from 96% a decade ago.

Fintech and non-bank payment firms make up the other 28%. So certainly, there's chipping away at that. While digitalization has moved the distance barrier in remote areas, it has also exposed risks. The pandemic has heightened the urgency for supervisors, especially in developing countries, to meet the challenges of underdeveloped digital financial services and infrastructure at a time when there is a proliferation of unregulated multiple financial services providers.

None might be a major risk on their own, but as they aggregate, they could pose systemic risks. Think of an army of ants eating an elephant, not least given the disproportionate impact on the poor, particularly women, who are financially excluded. This intensifies pressures on supervisors to monitor sound lending, work with multiple stakeholders and to be on top of cybercrime and fraud.

Join me in welcoming our two distinguished speakers who are leading their nation's supervisory efforts to tackle these challenges. Irene Espinosa Cantellano is the Deputy Governor of the Central Bank of Mexico. Ben Gully, a good friend of Toronto Centre, is the Assistant Superintendent Regulations of OSFI in Canada. Irene, Ben, welcome.

We will have three rounds of questions, and then I will take questions from the audience. Please use the Q&A tab to submit your questions. And have mercy on your moderator, brief questions. If you have long speeches, I just want to have time to you. Before we start, I would like to thank Global Affairs Canada, the Swedish International Development Cooperation Agency, the IMF, Jersey Overseas and Comic Relief and the USAID for generously supporting our mission.

I would also like to thank Demet Çanakçı, Ashley Thompson and Diana Bird for tirelessly working on our webinar series and a shout out to Diana Bird, who's leaving us. She was my partner in doing all these webinars series since the pandemic started. Diana, we wish you the best and don't forget about us. Irene, the first question is posed to you. Central banks are developing or at least [inaudible 00:04:31] issuing digital currency. Are you planning to move Mexico's payments to digital? How will this help unbanked populations? Thank you.

Irene Espinosa: Thank you. And good morning, everyone. Thanks to Toronto Centre for the invitation, and I'm very glad to share the panel with Ben. I'll start with your question. Of course, as you mentioned, I think before the pandemic, digital financial services were a very relevant priority, but after the pandemic, now it's a necessity. We need to advance on that. And the pandemic has also not only evidenced the inequalities but also potentially also increasing the inequalities because of the social distancing measures.

What are we thinking in the central bank to move to digital payments? We need to have a very long-term vision and what we are planning is... Our vision is to have every Mexican, regardless of its social-economic stand to be able to send and receive payments in a safe manner, in a transparent manner, trustworthy, but also at cost zero or at a very low cost.

So, in this sense, all of the payments run on a payment system and there, the Central Bank has a key role to play, not only as a regulator but also as the developer and the operator of the infrastructure. So, our strategy is to strengthen the public infrastructure, taking advantage of the scale that it can also handle on the network externalities and also to have the incentives for innovation and also for competition.

What have we done until now in Banco de México? In 2019... Well, previously, let me go back first to 2004, the Central Bank developed the main payment system, which is called SPEI, and this is a very efficient payment system that is available 24/7, and it's a very strong infrastructure. After that, in 2019, we lounged our request to pay platform, which is based on QR codes and runs on the SPIE infrastructure.

Today, this platform needs for users to have a bank account, and now the bank is developing a new version of this platform where users don't need to have a bank account. So, we will have a temporary place to store the money and where

users, end-users and receivers, and also senders of the payments will be able to do the payments.

So, I think we are going in the right direction. We are aware that this is something that we need to develop quite quickly and are working very hard on that, on the National Institutional Framework, but also on the internal front of the bank.

Babak Abbaszadeh: Thank you very much, Irene. Just a quick follow-up question. That doesn't mean that there's no future for banks, right?

Irene Espinosa: Right. No, no. I think the idea is, as I said, to bring the proper incentives for innovation and competition, and the view is really to take the advantage of the sizes of the technology, but also on the side of the banks to add one from the other. This is also the view, and I think your follow-up question is very relevant. So it makes it more clear, the long-term view.

Babak Abbaszadeh: And it's interesting. Times have changed so much. Now we're trying to defend banks, right? Imagine what a decade can do. Ben, the next question is for you. Before I start, Ben, you'd be pleased to know we have close to 200 or so people who are tuned in one way or another, and our viewers are all the way from Argentina to Zimbabwe. So, all letters of the alphabet and countries are included.

So, with that in mind, my question to you is, we are witnessing the proliferation of activities or entities outside of the regulatory perimeter that are subject to unclear supervisory responsibilities. In fact, if you have a chance to look at the Global Mail this morning, there was an article referencing Governor Mark Carney, who was warning against the Uberization of money, right?

So, in our interconnected world, this could undoubtedly have an impact on traditionally well-regulated jurisdictions like Canada because the world is changing so fast. Ben, is this a thing that keeps you up at night and does OSFI consultation paper on technology risks in the financial sector intend to start a conversation on these issues?

Ben Gully: Thank you very much, again, for the invitation to be with you today and to look forward to the discussion. In terms of the topic, not many things keep me awake. I sleep pretty well. But certainly, it's a topic that keeps me focused in the daytime. It's definitely an interesting one and one that OSFI has prioritized.

The increased adoption of digital technologies by all segments of the economy has the potential, I think, to affect the institutions we regulate. For instance, we had increasing numbers of consumers opting to use payment platforms that lie outside the regulated financial system.

Digital technologies are transforming the financial sector, giving rise to greater competition between regulated institutions and emerging and often unregulated financial technology providers or Fintechs. There is a risk that these new providers may create strategic risks that can destabilize the established financial institutions that make the foundation of the financial services marketplace and thereby threaten the viability of their business models.

OSFI's Technology Risk discussion paper, which was released last September, sought feedback on a range of technology-related risk areas that were focused on, including cybersecurity, the use of advanced analytics and the technology third party ecosystem. And in May this year, we released a summary of all comments received and our plans for releasing new guidelines over the next year or so.

Some respondents commented that OSFI should treat Fintech arrangements similar to any other third-party arrangement. Many of the inherent risks posed by these firms are consistent with those presented by other third-party providers. It was also noted that we should wait until the recently announced regulations in Canada on Fintech networking are finalized to avoid potential overlap.

And just for background, in 2018, the Canadian parliament passed changes to the legislation governing federally regulated financial institutions that address the growing prevalence of Fintech. Once they come into force, these changes will give institutions opportunities to better compete in the area by giving them greater flexibility to engage in Fintech activities and invest in and acquire Fintech entities, each on an indefinite basis and without regulatory approval.

These legislative changes will come into force once related regulations are published and also come into force. When it comes to OSFI's guidelines on third-party risk management, which is a key focus of this area, we are planning to replace our existing guidelines that focus on outsourcing with broader approached guidelines.

Many third-party arrangements that institutions have today do not fall under the traditional outsourcing definition, including data sharing arrangements with Fintechs. Further, in the context of potential open banking systems, we would expect all players, Fintechs and other non-financial institutions in a new system to have sufficient operational and financial fitness and are working through those implications.

Another aspect that OSFI is looking at is big tech and their continuous interest in entering the financial services industry. While Fintech can bring lots of change, big tech presents a different dynamic altogether with the size and reach. It is a topic being discussed at the international level, and OSFI is well-placed to provide input to this work.

For us, it is about how we can enhance our supervisory practices to keep up with the changing landscape. So, if anything were to keep me up at night, I would find answers on how best to supervise or regulate big tech on that list. And finally, I would note that Fintech is occurring organically within regulated institutions, not necessarily discrete as separate entities.

This is changing fundamentally the nature of operational risks within the very organizations which are used to supervising. And we are obviously needing to consider how best to oversee these changes as part of our ongoing improvements within supervision. Thank you.

Babak Abbaszadeh: Thank you, Ben. And I think what I'm gathering from what you're saying is - First of all, I'm glad that you sleep at night because we need your waking energy. There are entities that are regulated by supervisors, you mentioned banks and others, and Fintech is within them, so that's a certain degree of power control.

There are entities that are regulated but not necessarily by financial authorities, like telcos in many developing countries, but at least the entity itself is regulated, not the activity. They have these big techs with their massive power, massive capitalization and social network. And we've seen how social networks can get distorted, right?

So essentially, what you are doing and what you guys are up to is pretty crucial, and it's a cost of change. Anyway, thanks. Irene, the next question is for you. I want to bring it back down to real people. Access to finance and poverty reduction are top priorities for the Mexican government, especially since the pandemic. The Bank of Mexico has shown impressive leadership in financial inclusion. Good for you. Could you elaborate on your efforts to deepen financial inclusion and expand access to finance in the context of this conversation? Thank you.

Irene Espinosa: Yes. Thank you, Babak. Yes, Banco de México has been very active on financial inclusion, and I would say on two fronts, as I already mentioned, in the national institutional front, but also at the internal activities of the bank. On the national front, as you know, Mexico has been very keen on financial inclusion, and this has been a top priority for over 10 years or so.

We have recognized that this needs a lot of... It must be based on coordination among authorities. That's why in 2010, the National Council for Financial Inclusion was installed with the participation of all the authorities, the financial authorities, and of course, the Central Bank is there. One of the products of the work of this council was released in 2020 with a National Financial Inclusion Policy.

This policy relies really on how to explore innovative technologies, how to eliminate traditional and non-traditional barriers for financial inclusion and something that is very important, at least in our country, is to foster the user's

trust in the financial services. So, Banco de México is working on a very long list of projects regarding all of these objectives, for example, incentivizing digital payments with CoDi, as I mentioned.

We also developed a platform for consumers to compare prices and financial products so that it can be easily managed and help people in making financial decisions. We also engaged in surveys to know about the financial health of the users of financial products because this is also one of the core objectives of the policy, not only to increase access and the usage of financial services but also to ensure that we have consumer protection.

And now we were talking about also personal data and also to have financial competencies so that we can make sure that the access and the usage of these financial products are really being welfare enhancing. So, I think that the information in the survey is very important.

We also have developed some specific financial products or accounts, for example, also accounts for underage, also for the beneficiaries of the social programs and also specific types of accounts for migrants and their families, so that they can safely send remittances and have all of these services available at one touch.

Another product that the bank developed is a simplified credit card statement. We used to have hundreds of types of credit card statements where people really got lost. So, we're trying to bring it, as you mentioned, down to earth. So we are working on all of these facilities or tools internally and also helping other financial authorities in their regulation.

Now, in the bank, this year, it just happened in March of 2021; the bank also established an Internal Financial Inclusion Committee. And the committee is aboard to help to print financial inclusion approach to all of the substantial and all of the activities of the bank so that every time we make a regulation or release a regulation, before that, we have to ask ourselves, "What does this mean in terms of financial inclusion? Or in terms of developing a product?" Whatever we do, we need to have a good answer for that question before releasing all of that. Thank you.

Babak Abbaszadeh: That's great. It's fantastic that you have that holistic view on it. And as I mentioned earlier on, there's a big relationship between financial inclusion and stability. It looks like the Bank of Mexico is really stepping up. Ben, turning to you, the pervasive use of technology to collect, store and use data in financial services has been accompanied by ever more sophisticated and frequent cyber attacks against financial institutions.

Why can't people just be good, right? I'm sure many government agencies, including OSFI are preoccupied with cyber risk; how is OSFI dealing with this

challenge in Canada's financial system, and what tools are effective for cyber supervision? Thank you.

Ben Gully: Thanks for the question. Cyber risk is a top risk for OSFI and for our financial institutions, very much top of mind as well. Information security and integrity is critical to preserving trust and confidence in the financial system. So cyber supervision needs to be, in our view, central to the work of regulators and supervisors and the financial institutions we oversee.

The good news is that the public and the private interests is likely to be very aligned on this very important priority. Our work is to work collaboratively with a range of different approaches and stakeholders, both inside and outside of the traditional boundaries of the financial system. This recognizes that the risks are many and varied and critically change rapidly.

It also recognizes that risk management skills may reside beyond the financial industry, and there are lessons to be learned from many different places in this regard. In addition to our investments and setting clear regulatory guidelines and risk management expectations, including a new cyber and tech risk guideline later this year, our supervisory efforts are focused on promoting sound practices and resiliency to operational cyber disruptions.

OSFI has a cybersecurity self-assessment tool published in October of 2013 that we encourage all our institutions to use. The outcome of this tool helps other institutions and OSFI get a view of the institution's cyber risk posture, and critically we're in the process of updating the tool in the next couple of months. So, stay tuned for those latest updates.

Additionally, OSFI has technology and cyber incident notification advisory also published that requires institutions to report material incidents to us. We use the advisory to ensure that our institutions are managing their risks appropriately throughout the incident life cycle, and OSFI receives a variety of notifications. Those vary from ransomware attacks to third-party breaches, but also include technology outages and system failures.

We are also aiming to update the advisory with the aim to enhance the timely reporting aspect in line with the evolving threat landscape, which I mentioned is very rapid. Additionally, OSFI started sharing intelligence bulletins with our regulated institutions that include timely threat intel. These intelligence bulletins are made of techniques, tactics, and procedures, TTP, of attacks that we received via our incident advisory.

OSFI is also a member of the Canadian Financial Sector Resiliency Group, CFRG, a forum of critical financial sector participants, both private sector and public. The CFRG's mandate is to support enhancements within operational resiliency of the financial sector by coordinating critical finance sector responses to

systemic level operational incidents and coordinating critical finance sector-wide resiliency initiatives.

As a member of the CFRG, OSFI actively participates in multiple initiatives, including a recent cyber tabletop exercise facilitated by the group in a very important part of testing resiliency in general. The emphasis of our work is risk management and crisis response, clearly recognizing that traditional prudential responses such as more capital and liquidity are not going to be as useful in responding to a cyber attack. So, risk management, resiliency and crisis preparedness is our focus. Thank you.

Babak Abbaszadeh: Thanks, Ben. It's very reassuring that there are so many lines on this, and we love to hear more, and as you said, we're staying tuned. Irene, the next question is for you. It's been mentioned that Mexico is the Fintech leader in Latin America. You get the Oscars for the continent. With more than 700 Fintechs in a variety of sectors, why might that be? And how do you safeguard Mexico's financial stability against the proliferation of Fintech players? Thank you.

Irene Espinosa: Yes. As you mentioned, Fintechs have been steadily growing in the Latin America area, and specifically in Mexico, mostly since 2014. And therefore the need to develop a financial technology institutions law that was released finally in 2018. And it's also one of the pioneer laws in the world regarding this Fintech area.

So why in Mexico? I think that there are three reasons. One is that there is a lack of financial inclusions. So, of course, developers saw a business opportunity to develop it in Mexico, and there was a gap to be filled. Financial services through technology would be a very good mean for that.

The second reason is that in Mexico there's really extensive use of the internet and of mobile technology. In 2017, more than 80 million people were using the internet, which is almost 80% of the population and also 86 million people were using mobile phones and nine out of 10 would have a smartphone. This would put the ingredients for the Fintech industry to have a very good development.

And also, the entrepreneurial ecosystem in Mexico is quite developed in terms of having a lot of financing from venture capital investors and innovation. And I think these are the reasons for the higher than expected development of Fintechs in Mexico. Now, of course, the Mexican authorities are very worried about how this very rapid development in terms of size and number could hinder financial stability. And I think we have two big pillars for that.

One is the regulatory framework; as I mentioned, this law was released in 2018, and we also have a financial innovation group. And let me go a little bit more on the detail, but before going into the detail, I would say that this framework is based on the principles of caution, but at the same time promoting innovation of being very keen on gathering information, on analyzing risks.

So, I would say that the umbrella principle is cautiousness. Now, this law that was released in 2018 doesn't regulate all of the Fintech system, all of the Fintech institutions. It really regulates two types. One is really crowdfunding and electronic payments, the other one is operations with virtual assets, but the law has a third party that is very important, which is a regulatory sandbox. And this tool is very important to develop and promote innovation in a secure environment. And I think that's one of the key issues.

Now, we have 14 entities that have authorization for crowdfunding and electronic payments. There are 32 more that are on the way of authorization, and we have not yet authorized any for operations with virtual assets. Now, this other part of the Fintechs sector that is not regulated under this law is regulated under other federal laws. So, it's not that it's not regulated at all, but it really has a minimum of other laws that are supervising money laundering and for the proper constitution of these institutions.

Now, for the second pillar that I was talking about, this financial innovation group, this is part of the institutional arrangement where we have a diverse group coming from the financial authorities, the private sector, the academic sector, and it's really a place to discuss and analyze a consulting group to see experiences, to exchange ideas, to develop tools to reduce the impact of any type of new technology or a new business model.

So, I think this is a philosophy of building together, of gathering information, of exchanging information, which will take us or lead us to a safe place for promoting innovation at the same time that we are being cautious about the risks.

Babak Abbaszadeh: Yeah. Thank you. No, you summarized the prudence very well and also at the same time on how out to cycle innovation. Ben, my last structured question goes to you, and we already have a few audiences Q&As, so this would be a good time if people want to add more questions.

So, Ben, according to a recent global survey, 82% of companies increased their cloud usage because of the pandemic, and a significant number see cloud usage as a strategic priority. Through shared software, hardware and vendors, incidents could spread more quickly, leading to higher losses for financial institutions and stress in the financial system. In your view, how should supervisors prepare for this challenge in the short and long terms? Thank you.

Ben Gully: Thanks for the question. And I mean the business of supervision is to consider what could go wrong and develop suitable mitigates. So clearly cloud has many significant benefits, as you implied, but our focus is obviously on what could potentially go wrong. And as a supervisor, my quick response would be to consider the implications to operational resilience. The ability to maintain critical processes and outcomes towards consumers and other stakeholders.

It's a key objective that's gauging outcomes; it's gaining traction internationally. The Basel Committee published papers on this very topic, and I think it's a useful companion to financial resilience and a way of framing supervisors. The ultimate objective's here, which is obviously to expect firms to evaluate their own operational resilience, to have suitable risk management and control structures around that objective so that we can more effectively understand the changes to the operating environment and how threats and mitigates can involve in what is increasingly a rapidly changing technological environment.

In terms of the specific question, OSFI's approach has always been principles-based and risk-focused. We don't incline it on a specific cloud provider or a specific technology. Having said that, as financial institutions embark on their cloud journeys or increase their existing footprint in the cloud, our focus is on how they manage the risk, including the potential for risk concentrations.

As you mentioned in the question, there are obvious benefits with institutions, particularly smaller institutions getting access to potentially best-in-class information security capabilities, among others. There are also risks and especially concentration risks in cloud providers. As part of our supervisory plans, we have been performing multiple reviews focused on clouds at our institutions.

The reviews focus on areas related to cloud strategy and governance, cloud configuration and change management, shared responsibility models, cloud data protection, disaster recovery, exit strategy, to mention a few. Additionally, internally for our supervisors, our new Technology Risk Division team is developing a cloud supervisory toolkit to arm and educate our supervisors on the topic and enable them to have risk-based discussions with our institutions on this evolving topic.

But with all things operational, it is important to use simulations and tabletops to draw our insights and vulnerabilities. The key will be to understand the implications of disruptions, identify vulnerabilities from the cloud and to prepare playbooks with clear accountabilities and actions based on lessons learned.

In terms of supervisory capabilities, this is an area that requires investment and expansion over the medium to long term in terms of talent and our own technology infrastructure. It's also an area that is testing the boundaries of supervisory oversight, especially with respect to big tech, as we noted before. This may require additional thinking around legal mandates, access to information and ultimately supervisory authority. Thank you.

Babak Abbaszadeh: Thank you very much, Ben. Certainly, a lot of work needs to be done on this. First, a big thank you to our speakers for managing your time extremely well. I didn't have to cut anyone off. So that leaves us with plenty of time for questions. I see a couple of questions from the courageous anonymous, but I think let's go with the people who have identified themselves by name.

Our friend, George Brady, has a question and I think, Irene, it is for you. As Mexico is trying to build back better, do you see success in tackling the gender protection gap and increasing empowerment of women through financial literacy and working with financial services providers? I mean, George is highlighting a specific, I mean to everyone who may know about it, so we're not here to ask you to endorse anything. But I'm just wondering, what have been your challenges, and do you think you're making good progress in this area?

Irene Espinosa: Yes. Of course, we are very concerned about inequalities, especially in access for financial services. Especially for women in Mexico, there are huge barriers to access for women. Nevertheless, I think there are several very innovative schemes of financing, especially through social bonds.

Recently there were three or four bands that were released, and I think they were very, very successful since they had a huge demand around four times the amount of the issuing and also in terms of the rates, which were all of them lower than the average of the other social bonds that were issued before. So I think we are going on the right side, on the right direction.

And as I mentioned internally, with this Financial Inclusion Committee, we will be asking ourselves on each of the fronts of whatever our faculties are, how are we enhancing the financial inclusion, mainly for the excluded groups, with the policies that we are promoting? So, I think we are in the right direction.

The pandemic has also affected more women, and we will have to tackle that. And we are also on the discussion with the government on how to implement recovery public policies with a gender perspective.

Babak Abbaszadeh: Thank you very much for that answer. And turning to another one of our good friends, Calvin, he's asking... I guess, Ben, I'm going to ask you to answer this. Either of you could take this, but let's go to Ben first. The BIS has recently become very active in promoting the central bank digital currency, as we know.

What do you think about this development? What changes do you think financial institutions, regulators and supervisors need to make if these digital currencies become a reality in Canada? I know that a lot of that is a remit of the Bank of Canada, but nonetheless, when it comes to supervision, you will be at the front and Centre. Any views on this?

Ben Gully: Yeah, thanks for the question. And I think my comments will apply to the anonymous question immediately preceding Calvin's question. I draw your attention to the Basel Committee paper that was released earlier this month on cryptocurrencies. And I think that does a very good job of framing the supervisory perspective on these developments.

I think the development of digital currencies is an innovation that is to be welcomed, is an innovation that is a part of the future clearly. But our focus as

supervisors, again, is always to focus on the downside, the potential for loss, the potential for loss not just in obviously financial loss, but also reputation, trust and confidence.

So, the committee paper is really exploring possible treatments for capital, in particular, of different cryptocurrencies based on how stable or not we think those asset values are likely to be over time. And clearly, that's an area of great interest, how much loss could be realized through the market as a result of these new and evolving asset classes and how best to reserve or control for that.

In addition, the paper does a good job of acknowledging there are additional and different operational risks that come with assuming and managing and risk overseeing such asset classes that we will also have to see, which may in fact, also consider capital requirements as well.

So, I think my short answer is safe innovations are to be welcomed, and our approach as supervisors is to make sure that we understand the potential for loss and do our best to ensure that the institutions we regulate are appropriately reserving and managing for those risks. Thanks.

Babak Abbaszadeh: Yeah. Thank you very much, Ben. And it's always a balance, right? I mean, if you go back and look at some of the presentations that were made to Canada's Senate Banking Committee in reviewing Canada's financial system decades ago, there was some resemblance of a scale, right?

The more you pay attention to financial stability, the fewer options might be available to consumers or reverse is also true. Which are you trying to preserve and protect? I know your mandate is to protect financial stability. And the public also wants to embrace these new innovations and then puts you in an awkward spot, right? That's part of it.

Ben Gully: I may push a little bit on that. I mean, it is true that we have a balance to consider on our mandate, which is to ensure that our firms are able to compete and take reasonable risks. I don't necessarily see them as mutually exclusive. I think if we don't have innovation, the system will fail because developments then will not occur as they should.

The question is, what does a reasonable risk look like, and what does safe and sound prudential practice look like around these currencies, which is why I think the committee paper does a good job of getting that thinking out of there.

Babak Abbaszadeh: And we'll make that paper available. Thank you so much. Back to you, Irene, there's a question from Leo. He's talking about, could you please share some insights in the Bank of Mexico's formulation of their cybersecurity framework?

Irene Espinosa: Well, yes. Cybersecurity incidents have been growing lately in terms of number and also diversity. So, this is one also of our top priorities, and we are working on a cybersecurity framework that covers, first of all, the systems of the bank that the bank operates, the payment systems and all the other systems that we operate, but also the whole network in the financial system.

And I think the bank has been doing a very good job in terms of setting minimum standards for cybersecurity for all the participants in the financial sector. So, it's been focused on how to mitigate the systemic risks, but also how to mitigate the individual risks of the financial institutions. And this is the work that has been undergoing for the last 10 years or so.

And this is also a front where there is a lot of cooperation among the different financial authorities. We also have incidents recovery group that includes not only financial authorities but also other type of authorities from the government and from the banking system, and other intermediaries.

So, we are aware that it's crucial to have information security technology as a top priority, and setting minimum standards and advancing on this is very important for the bank. Internally we have a joint responsibility framework for cybersecurity, and so we are also advancing well on this front.

Babak Abbaszadeh: Great. Thank you. And Ben, do you have anything to add on cybersecurity? We talked a little bit about it, and you seem to be plugged into some of the Basel discussions. Is there anything you want to compliment or take a different view of what Irene talked about?

Ben Gully: I think the overview I gave earlier is probably sufficient, and I think the references to operation resiliency. There's, again, those papers on operational risk management principles, as well as operational resilience, specifically that the committee came out with, I think in May. Those would be two good reference papers I would point colleagues to as well as our incident advisory on the web we've published.

And, as I said, our plan, I think this fall, is to target a new cyber and technology risk guideline that tries to bring together in one place an overarching set of expectations. Still principle-based and not reinventing the wheel when it comes to tech risk frameworks, of which there are many tech risk management frameworks. But I think with that as background, I'd probably just stop there. Thank you.

Babak Abbaszadeh: No, thank you. These are good references, and as I mentioned, we'll try to make them available as well because it's part of a big discussion. Irene, I want to ask you a question here that stems from some of the work that we've done. We have held four round tables in the margins of the World Bank and IMF. And I think Mexico has participated in some. These are small gatherings like Chatham House Rules.

But one of the observations we have, we have central bankers, supervisors from developed countries and emerging market ventures, right? So big mix. And early on, when we were discussing these issues around digitalization and financial inclusion, et cetera, there was a very big demarcation between developed countries and emerging markets.

So developed countries were more interested in protecting or dealing with issues around privacy and emerging market and developing countries were more grateful for the opportunity of expanding access to financial services.

And we see that people are generally, maybe sometimes are ahead or behind the regulator in the sense that they don't really value their privacy as much as the regulators and others view in some cases, especially young people. How do you deal with that in Mexico, as you're trying to expand access, and yet there are some legitimate privacy issues? How do you philosophically and practically deal with this question?

Irene Espinosa: Yes, we have some principles for our general policies. One of them is to deal with jurisdictional gaps. And I think what you're mentioning about the opinion coming from advanced economies regarding emerging markets pushing much more for innovation without looking so detailed on the protection of data is there are different levels of supervisory capacities, I think.

And it is important precisely those kinds of encounters have a lot of communication so that we all can cooperate on that front. And yes, we are also putting a lot of work on data governance as one of the main parts in terms of the development of new entities, of Fintechs, of innovation. This is one pillar that is very important for us to keep in mind. Client protection is key, and this is not something very visible and very easy to explain to developers and to users on the individual front.

This is really a national state issue that we have to be securing data protection. And yes, maybe there is this huge optimism on pushing for more innovation. But as Ben mentioned, we have to keep in mind a balance in terms of having deeper financial systems, more inclusive financial systems, but at the same time to have a very secure environment.

And in a way, one of the big risks that might arise, especially in the Fintech industry, is this orderly growth. I mean, if we have a very rapid scaling process in terms of the size of the Fintech industry, in terms of the participation of big techs, this can really be disruptive for the financial stability and also for the financial system.

We could be exposed to players that don't have the experience, don't have the tools for risk assessments or risk management policies that are properly managed. And so this is, of course, the governance in terms of risks, in terms of data protection, in terms of innovation. We need to keep in mind this balance

so that we don't compromise the financial stability of the system. With that, I will stop.

Babak Abbaszadeh: That's great. We've done really well with our time, and I'm going to try to bring this session to a close. Before I do that, Ben, do you have any final comments, words of advice, cautions for us?

Ben Gully: My only advice in this arena is to cooperate, exchange, network, build your expertise base well outside of the financial system. There are lots of people with very relevant expertise and insights that are keen to work with regulators in the financial area. So, all we can do to build our ecosystem and stay connected and use events like this to share expertise, I think, is incredibly valuable. That would be my main piece of advice.

Babak Abbaszadeh: That's great advice, Ben. And it's interesting where the cost of a lot of change is, and on the one hand, we can praise or complain about the rapid pace of technology. But I just ask each of you, if you have to sign a document with a wet signature, you realize how frustrating it is after having gone through all of this, so we all share the joys and tribulations of all this.

So, Irene, thank you so much for your time. Ben, thank you so much for your time. We really appreciate you devoting a bit of your time to us. I know how busy you are all in this difficult global time. You have our appreciation. We will make this session available to our cohorts who go through our training programs and also make them available publicly. So, you've really contributed to a very good sense of knowledge. So, thank you. Namaste. Take care. Bye.

Irene Espinosa: Thank you. Bye