International Association of Potential, New and Sitting Members
of the Board of Directors (IAMBD)
1200 G Street NW Suite 800 Washington, DC 20005-6705 USA
Tel: 202-449-9750 Web: www.members-of-the-board-association.com

News for the Board of Directors, January 2018

Dear members and friends,

Around 20,000 people will visit Argentina in 2018 for the G20. The final event will be the Leaders' Summit on 30 November and 1 December.

Argentina took over the presidency of the G20 on 1 December 2017, with the forum's main activities taking place over the course of 2018: more than 45 meetings in 11 cities across the country.

Argentina will play host to over 20,000 participants from abroad, mainly officials from G20 member governments and international organizations, and members of the press.

The G20 meetings will cover a number of issues, including agriculture, the digital economy, education, employment, energy, finance, trade & investment, amongst others.

The three main priorities of the Argentine presidency – the future of work, infrastructure for development and a sustainable food future – are themes that will cut across the entire G20 agenda, as will other important transversal issues, such as gender equality.

The Argentine presidency's objective is to build consensus amongst the world's major powers for development that is both fair and sustainable, and that will generate opportunities for everyone.

It is closely in line with the concerns and aspirations of the region of Latin America and the Caribbean to harness its populations' great economic potential and boost efforts to eradicate poverty.

The first G20 meeting of the year is on the Data Gaps Initiative (DGI) and will take place on 29 and 30 January in Buenos Aires.

Organized by the National Institute of Statistics and Census of Argentina (INDEC), the meeting will address issues relating to collecting and disseminating comparable, integrated and standardized statistics of high quality to craft public policies.

The G20 agenda includes a further five meetings in February, also in the Argentine capital. On 12-13 March, the city of Rosario will become the third city after Bariloche and Buenos Aires to host a G20 meeting, in this case, the first meeting of Agriculture Deputies.

In the lead up to the annual Leaders' Summit, numerous meetings will take place at technical ('working group'), deputy minister, and minister levels.

The latter is the most important of these, attended by ministers of G20 countries and their equivalents in G20 partner organizations. The first minister-level meeting of the year will be the first of five meetings of Finance Ministers and Central Bank Governors, taking place on 19-20 March in Buenos Aires.

Other cities across Argentina will host G20 ministerial, deputy and working group meetings. These are Salta, San Salvador de Jujuy and San Miguel de Tucumán in the northwest; Puerto Iguazú in the northeast; Mendoza in the west; Rosario and Córdoba in the centre; Mar del Plata and Buenos Aires in the east; and Bariloche and Ushuaia in the south.

The G20 working year concludes in Buenos Aires with the Leaders' Summit on 30 November and 1 December, which will close with a joint declaration of the G20 heads of state and government.

The calendar:
https://www.g20.org/en/calendar

Configuration Security Program to Make Network-Connected Systems Less Vulnerable

The rise of network-connected systems that are becoming embedded seemingly everywhere–from industrial control systems to aircraft avionics–is opening up a host of rich technical capabilities in deployed systems.

Even so, as the collective technology project underlying this massive deployment of connectivity unfolds, more consumer, industrial, and military players are turning to inexpensive, commodity off-the-shelf (COTS) devices with general-purpose designs applicable for a range of functionalities and deployment options.

While less costly and more flexible, commodity components are inherently less secure than the single-purpose, custom devices they are replacing.

"With commodity devices, software and configuration settings now govern behaviors that were physically impossible in special-purpose hardware, creating security risks and increasing system vulnerability," said Jacob Torrey, program manager in DARPA's Information Innovation Office (I2O).

"Certain functionality built into COTS components may not be necessary for all users or applications, and unwanted functionality can be hard to detect and turned-off. For instance, an unneeded maintenance or diagnostic service left enabled could create an opportunity for an attacker to circumvent other security controls and use the system's as-deployed functionality to generate a malicious effect.

This opaqueness is creating challenges for system operators who must rely on component configurations to reduce attack surfaces created by unnecessary functionality."

To address the challenges created by the proliferation of COTS devices and help harden the security surface of network-connected composed systems, DARPA has launched a new program called Configuration Security (ConSec).

The program, just announced today, aims to develop a system to automatically generate, deploy, and manage inherently more secure configurations of components and subsystems for use in military platforms.

“Through ConSec we hope to gain a better understanding of the available functionality across COTS devices and what’s needed for the task at hand and then use system configurations to create the functionality that’s actually required while minimizing the excess that can be used as an attack surface,” said Torrey.

“While our objective is to build this capability for military platforms, there is the potential for the program to have broader applications for commercial and industrial systems as well.”

Prospective performers are tasked with finding ways to automate the traditionally more manual process of system configuration. To tackle this feat, the program is divided into two technical areas.

The first area focuses on reducing the amount of human-in-the-loop time required to understand what capabilities a system needs to deliver across different operating environments, the functionality required to achieve its mission in each operating environment, and the possible component configurations needed to create the desired functionality.

“Consider, for example, a naval vessel. Its functionality when at sea is likely different than what’s required of it while at port, or in dry-dock undergoing maintenance,” said Torrey. “Our aim is to automate the process of identifying these different operating environments, the system’s expected functionality in each scenario, and the components needed to make it all happen, which is currently a manual, labor intensive process.”

To accomplish this, DARPA is asking researchers to develop models and functional specifications of systems based on human-friendly information formats–such as checklists, operating manuals, and other written human standard operating procedures (SOPs)–as well as an analysis of the system’s underlying components’ hardware and firmware.

Input from these analyses should help determine how settings in a component’s configuration space might impact its functionality, how the behavior of human operators impacts system behavior, and what operational and mission contexts pertain for the full, composed system.

The ConSec program's second technical area focuses on uncovering component configurations that will enable the composed system to achieve its mission under different, relevant operational contexts.

Here proposers are asked to leverage the models and functional specifications that emerge from work in the first technical area to find ways of identifying secure configurations that eliminate unused and unnecessary functionality as a way to shrink the system's vulnerabilities to attack.

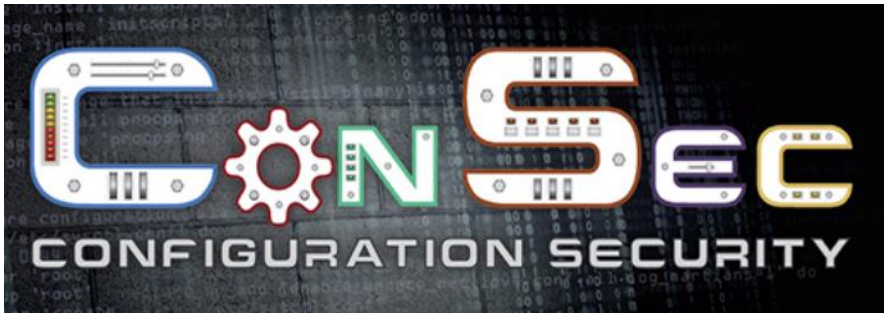
"Essentially we're asking potential performers to determine how to take all of the best pieces and functionality and combine them to fulfill the requirements of a high-level composed system while turning off all of the things we don't need," said Torrey.

Torrey expects that the program will roll out in three phases over the next three-and-a-half years.

The deadline for proposals for the ConSec program is February 8, 2018.

Additional details about the program can be found via the DARPA Broad Agency Announcement, found at:

https://www.fbo.gov/index?s=opportunity&mode=form&id=c889999b044a8b485da8884d7fbab391&tab=core&_cview=1



A blind spot in today's macroeconomics?

Panel remarks by Mr Claudio Borio, Head of the Monetary and Economic Department of the BIS, at the BIS-IMF-OECD Joint Conference on "Weak productivity: the role of financial factors and policies", Paris.

A standard presumption in today's macroeconomics is that when making sense of first-order macroeconomic outcomes we can treat the economy as if its output were a single good produced by a single firm.

This means that issues of resource misallocation can be safely ignored.

But the link between resource misallocations and macroeconomic outcomes may well be tighter than we think.

This speech illustrates the point with reference to two examples that highlight the link between finance and macroeconomics: the impact of resource misallocations induced by financial booms and busts on productivity growth, and an intriguingly close relationship between the growing incidence of "zombie" firms and declining interest rates since the 1980s.

To read more:
https://www.bis.org/speeches/sp180110.pdf

Current developments in the area of financial stability in Switzerland

Introductory remarks by Mr Fritz Zurbrügg, Member of the Governing Board of the Swiss National Bank, at the Media News Conference of the Swiss National Bank, Berne.

In my remarks today, I would like to address some of the developments currently taking place in the field of financial stability.

I shall look at the big banks first before turning to the domestically focused banks. I will conclude with a few words on the new banknote series.

Big banks

As Thomas Jordan has already noted, the international economic environment has continued to improve since the last news conference in June.

Conditions on the financial markets have remained stable.

Premia for bank credit default swaps, for instance, have barely changed since June. Premia have thus settled at lower levels again following the turbulence in 2016.

Against this positive backdrop, both of Switzerland's big banks remain on track to meet the requirements of the 'too big to fail' regulations with respect to resilience.

This first pillar of the regulations covers requirements pertaining to the going-concern loss-absorbing capacity of systemically important banks. Both Credit Suisse and UBS already comply fully with the final1, risk-weighted requirements.
However, further improvement is needed with respect to the leverage ratio. Both of the big banks have also made progress on the second pillar of the regulations, 'resolution', which covers the orderly restructuring and wind-

down of a bank that can no longer function as a going concern and is thus deemed to have become a gone concern.

With a view to managing such a crisis scenario, Credit Suisse as well as UBS have increased their gone-concern loss-absorbing capacity by issuing further bail-in instruments, which can be converted into equity in the event of impending insolvency.

As we explained in our Financial Stability Report published in June, since the 'too big to fail' regulations came into force, Credit Suisse and UBS have also taken important organisational steps to improve their resolvability.

Despite these positive developments, the two big banks still need to make further progress if they are to fully comply with the second-pillar requirements.

This applies both to their gone-concern loss-absorbing capacity and their resolution planning. Full compliance with all of the 'too big to fail' requirements will further strengthen the big banks' going and gone-concern loss-absorbing capacity as well as improve their resolvability in a crisis.

Both of these sets of requirements must be addressed if Switzerland's 'too big to fail' problem is to be solved. Domestically focused banks I would now like to turn to the domestically focused banks. These institutions' biggest risks continue to stem from the mortgage and real estate markets.

I will make three points in this regard.

First, imbalances on the mortgage and real estate markets persist. Although mortgage growth has remained relatively low in 2017 – as in the previous year – developments on the real estate market show a somewhat different picture: price growth in the residential property segment had been falling since 2013, but recently transaction prices have started to pick up again.

Moreover, with the exception of a few quarters (including the third quarter of 2017), prices in the residential investment property segment have risen markedly since 2013.
As prices over this period have increased more strongly than fundamentals such as rents, risks have accumulated in this segment; it is thus especially vulnerable to a substantial correction in the medium term.

This situation is compounded by brisk construction activity in the rental apartments segment, which could lead to oversupply. Signs of this can already be seen in rising vacancy rates.

Second, the risk appetite of domestically focused banks remains high. This is particularly evident from the affordability risk data. The share of new mortgages with high loan-to-income ratios has risen significantly in recent years and has reached a historical high.

The interest rate risk of domestically focused banks likewise remains high, while their interest margin continued to decline in the first half of 2017. As long as there is pressure on margins, incentives for domestically focused banks to increase risk-taking will remain substantial.

Third, notwithstanding the risks in the macroeconomic environment and the banks' high risk appetite, SNB stress tests continue to suggest that, overall, domestically focused banks' resilience remains adequate.

Thanks to robust capitalisation, most of these banks would be able to absorb the losses likely to be incurred in adverse scenarios; given the risks I have outlined, this is welcome.

In the future, too, it will be decisive for the stability of the financial system that banks hold sufficient capital to cover the risks on their books – irrespective of ongoing margin pressure.

What's going on in Europe?

Dr Andreas Dombret, Member of the Executive Board of the Deutsche Bundesbank, at the Hong Kong Monetary Authority, Hong Kong.

1. Introduction

Dear Norman Chan
dear Eddie Yue
dear colleagues

It's a pleasure for me to be invited back to the Hong Kong Monetary Authority. I value very highly the excellent cooperation, not only between the Hong Kong Monetary Authority and the Bundesbank, but also more generally between our two countries. This contributes to the strong friendship of Hong Kong and Germany.

In my remarks today, I will give you an overview on what's going on in Europe.

Some of you may have become used to quite negative news from the European continent, as we not only endured the global financial crisis but also witnessed how it triggered the euro area crisis. As a result, the last ten years were something of a dry spell for the EU's economy.

But things have actually changed for the better of late: the economic recovery is gaining momentum and has spread to all EUcountries. Today, I will paint a positive picture of the current development and will also talk about the positive outlook.

Yet in my remarks I will also focus on the two big challenges the EU faces, namely Brexit and euro area reform.
My main point is that we now have a vibrant economic situation that gives us an opportunity not only to manage but to master these challenges such that the recovery becomes a sustainable story.

2. Finally, a broad-based recovery of the EU economy

Until last year, the economic recovery following the financial crisis was rather disappointing - and that despite extensive monetary easing by the European Central Bank. Entering the second half of 2017, however, growth momentum began.

Recent figures for the third quarter of 2017 show a sound GDP growth of 0.6%, quarter on quarter - after 0.7% in the preceding quarter. Euro area unemployment stood at 8.8% in October - well down from its peak of 12.1% in 2013 and the lowest level since January 2009.

And a recent study by Ernst & Young expects 1.8 million new jobs to be created over the course of 2018.

What is important is that the upswing has become more broadly based - across countries as well as sectors. And this is also reflected in the positive economic sentiment. In December last year, the European Commission index reached a 17-year peak to record the highest value since October 2000.

And at the same time, inflation is slowly rising. The Eurosystem staff macroeconomic projections forecast annual HICP inflation of 1.5% in 2017, 1.4% in 2018, 1.5% in 2019 and 1.7% in 2020. There is some indication, then, that the volume of expansionary monetary stimulus could be lowered.

The euro area recovery is in considerable part driven by the healthy upswing of the German economy, which is ongoing: 2017 was the fourth consecutive year in which GDP growth outpaced potential output. And the Bundesbank expects a further rise of 2.5% for 2018, while growth in 2019 is seen at 1.7%.

3. A solid outlook for the EU economy

Coming back to the euro area and looking ahead, the very high level of confidence among firms and households suggests, moreover, that the upswing will continue well into 2018. The outlook for the euro area's economy is quite solid. This is in considerable part due to the robust projection for the world economy.
The World Bank recently estimated that growth will be 3.1%; this means that the world economy's growth potential will be fully or almost fully reached for the first time since 2008.

The strongest driver of global growth will be the East Asian economies, China in particular. The World Bank sees emerging markets growing by 4.5% in 2018 and by 4.7% in 2019.

The global and emerging market growth has positive effects on the euro area economy as well. And I am convinced that the strong ties between the euro area and Asia, notably between Germany and Asia, will contribute to the success stories of both Asian and European countries.

With this in mind, we should further deepen our political and economic relationships. And this should be based on the principles of free trade and market economies, while leaving some room for legitimate differences in rule-setting.

Both the IMF and the ECB staff recently upped their growth expectations for the euro area.

According to the December 2017 Eurosystem staff macroeconomic projections, the annual real GDP is set to rise by 2.3% in 2018, 1.9% in 2019, and 1.7% in 2020. Compared with the September projections, the outlook for GDP growth has been revised upwards substantially.

The Eurosystem expects the economic expansion to continue, as private spending and consumption growth are reinforced by lower deleveraging needs and better labour market conditions.

Furthermore, the recovery in business investment is supported by improvements in corporate profitability and the very favourable financing conditions. At the same time, euro area exporters are benefiting from the ongoing global economic expansion.

These figures give some comfort as to the EU's economic future. And I personally am confident that this trend can and will continue.

However, challenges are looming: two particularly serious ones are Brexit and euro area reform. The current, upbeat trajectory has to be harnessed as we set about mastering these historical challenges.

4. Brexit looming

The first challenge, Brexit, began in June 2016, when the majority of UK voters decided to leave the EU. Where are we now?

Brexit is definitely happening, and it is more and more likely to be a hard Brexit - by which I mean that there will be a complete exit rather than a partial one. The UK and the EU will go their separate ways.

Since December of last year, there is a better chance of reaching a sensible agreement before the deadline of March 2019.

The EU Council agreed in December on the Brexit divorce issues: basic compromises were reached on three fundamental questions, namely the rights of EU citizens in the UK after Brexit (and vice versa), the border between Ireland and Northern Ireland, and the UK's financial contributions to the EU budget over the coming years.

This compromise allows us to move forward to negotiate the terms of our future partnership. But let's keep in mind that substantial progress has yet to be made on the details of the three separation issues I just mentioned.

Now, since negotiations have been going rather slowly, there may be a transition period of two years from 2019 to 2021 - during which the old rules would still apply and the terms of the new partnership could be implemented. What kind of economic partnership this will be has yet to be determined.

If no solution is found, the EU and the UK will trade under rules set by the World Trade Organization - which is in nobody's interest, but is likely to be particularly harmful to the UK economy, while the economic impact on Europe will be limited by comparison.

Take Germany for instance. The UK is an important export market, accounting for ca. 7% of German exports. But this implies only 2% of value added to the German economy.

My hope is that all the parties involved will be able to negotiate an economic partnership that underscores the close political amity between the UK and the EU.

With a view to future economic relations, we must work hard to reach a deal that, on the one hand, minimises frictions in trade and supply chains. In that context, I also think that a substantial transition period is in the interest of both economies.

On the other hand, however, this deal must also give the UK and the EU the freedom to develop their own agendas in economic policy and rule-

setting - this would ensure the possibility of institutional diversity, where each society can develop rules according to its own specific, historically grown circumstances and current preferences.

5. Euro area crisis and reform

Mastering Brexit is probably the biggest mid-term challenge facing the European economy, and we all need to take a pragmatic approach. Much is at stake. Yet as is always the case in life, problems and challenges never come alone, but in groups, or at least in pairs.

The second big economic challenge we need to focus our attention on in 2018 is the reform of the euro area. This is also emphasised by the weight that this topic has in the current negotiations to build a new government coalition in Germany. I will come back to this in a moment.

The euro area will remain vulnerable as long as one fundamental stumbling block remains in place: its asymmetric institutional design. Member states surrendered sovereignty in monetary policy matters to the ECB on the one hand, but retained ownership of their fiscal and economic policies on the other.

This creates two major problems: first, a common monetary policy for economies that are at different developmental stages - compare France and Greece, for instance - and at different stages of the business cycle. Second, the moral hazard that arises when governments, firms and households borrow too much to take advantage of lowered interest rates as a result of averaging in the currency union.

We need answers to both these problems. For the economic convergence of the euro area will take time. Currently, the potential German coalition partners are debating quite sensible approaches on how to foster social inclusion, limit a race to the bottom in tax policies, and foster the convergence of the euro area economies. It's too early to judge these positions.

The second problem - excessive debt, and high borrowing by governments in particular - could, in theory, be solved much more easily. However, the necessary political reforms have seen little progress so far.

But here, again, the recent proposals of the potential German coalition partners are promising. The creation of a European Monetary Fund seems

to go in the direction that we, the Bundesbank, have been advising for quite some time.

Formally, the EU has a set of fiscal rules that restrict public borrowing - the Stability and Growth Pact. Yet these were regularly violated before the financial crisis, without any meaningful consequences.

In response, the EU reformed the Stability and Growth Pact in 2005, but the outcome was to expand the discretionary scope even further.

The European Commission, despite its role as guardian of the Stability and Growth Pact, has already exploited its scope on several occasions and interpreted the rules rather generously in doing so. Indeed, some euro area countries have been breaching the rules for nine years now.

What is needed to strengthen the fiscal rules is a simple and transparent design and implementation of the rules.

The transfer of responsibility for fiscal surveillance from the European Commission to an independent institution would be a big step towards a less political approach. One promising measure would be to strengthen the role of the European Stability Mechanism, ESM for short.

Thus far, the ESM has been tasked with providing financial assistance to euro area countries experiencing or threatened by severe financing problems.

However, if member states retain their fiscal autonomy, the sustainability of public finances will need further safeguards beyond rules alone.

It is therefore essential that the binding force of the rules be additionally shored up by the disciplining effect of the market. In other words, interest rate levels and, therefore, financing costs have to be realigned more closely with the risks in government budgets.

The only way to achieve that, however, is to restore the credibility of the no bail-out clause in the Maastricht Treaty. Investors have to perceive a more credible threat of losing money if they buy bonds from governments that have unsound public finances.

One proposal put forward by the Bundesbank envisages changing the contractual terms for sovereign bonds in the euro area by introducing an

automatic maturity extension for them as soon as the issuing government applies for an ESM programme.

Up to now, a large part of the assistance loans have ended up being used to pay off the original creditors. This means that the original creditors, such as banks, are then let off the hook - at the taxpayers' expense.

In contrast, extending maturities would leave the original creditors on the hook, and they could still be held liable if debt restructuring became necessary at a later point in time.

6. Conclusion

To sum up, the European Union has entered a period of broad-based, stable economic growth and, having done so, has overcome the economic repercussions of the financial crisis and the euro area crisis.

Yet it would be a huge mistake to consider our mission successfully accomplished. It is a solid basis on which the EUneeds to build its efforts in 2018 to tackle not only the political challenges it faces but also the two biggest economic challenges in the shape of Brexit and the reform of the euro area.

We must do all we can to achieve a close and friendly political and economic partnership between the UK and the EU after Brexit - anything else is in no-one's interest.

With regard to the euro area, it is crucial that we improve the asymmetric institutional design to prevent another euro crisis.

If we take these challenges seriously, the euro area will become an economic success story. Thank you for your attention.

Central banks as risk managers

Speech by Benoît Cœuré, Member of the Executive Board of the ECB, at the 53rd SEACEN Governors' Conference/ High-Level Seminar and the 37th Meeting of the SEACEN Board of Governors, Bangkok.

It is a great pleasure for me to be here today.

Before I comment on this panel's topic, let me express my gratitude and satisfaction with the strategic partnership between the ECB and SEACEN, which got off to a successful start this year.

Many cooperation activities, ranging from seminars on macroprudential analysis to central bank governance, have already been launched and more is being planned for 2018. I look forward to strengthening our cooperation over the coming years.

The topic of this panel deals with the implications of political risks for central banks. Given the independence of central banks and their legal separation from the political dimension, this is obviously a complex issue – and one where monetary policymakers need to tread very carefully.

For this reason, I would first like to spell out how the ECB generally incorporates different kinds of risk into its monetary policy strategy, and how this has influenced our actions over the last few years. I will argue that every central bank is to a considerable extent a risk manager, reflecting the forward-looking nature of monetary policy.

I will then explain why political risks cannot be addressed in the same way as economic risks. Central banks should not prejudge political outcomes through their actions. Rather, they should address their effects if and when they become visible in the economic and financial data that are relevant for their price stability mandates.

Monetary policy and risk management

My starting point is that monetary policy works with long and variable lags.

In the euro area, for example, the full transmission of interest rate decisions to output has been estimated to be between one and two years, and even longer for inflation.

So, if we were to decide policy on the basis of past outcomes, we would always be behind the curve. Monetary policymakers therefore have to look at the economy in a forward-looking way.

To do this, we produce forecasts, on a regular basis, that indicate our central expectations for the economy – the baseline. In principle, this should be enough to form a view on how policy should be designed today. But we all know that this would be a bad idea. Policymakers are typically poor forecasters, and central bankers are no exception.

This is nothing to be ashamed of. It merely testifies to the fact that the past is often a poor predictor of the future.

You can see this quite clearly for the euro area on my first slide. We call it the "spaghetti chart". It shows the repeated inflation forecast misses over the past few years. On each and every occasion there were good reasons to assume the economy would go the predicted way. But on each and every occasion unpredictable shocks hit our economy that made our central forecast redundant.

The implication is that we would likely have made severe policy mistakes if we had based our policy decisions entirely on our baseline.

And bear in mind that the economy can be more or less elastic to different types of shock. A tail risk, if it materialises, may cause the economy to react in a non-linear and potentially disruptive way – hyperinflation and deflation being typical examples of risks central banks want to avoid.

For all these reasons, central banks usually augment their forecasts with an assessment of the risks surrounding them. This comprises a distribution of risks – the range of possible outcomes and the likelihood of their happening – which, in turn, allows us to form a view on the balance of risks, i.e. whether they are overall tilted to the upside or downside, and on the probability of tail events.

Such risk assessments are not an exact science and there is no automatic link between them and policy decisions. But we do at times apply what Alan Greenspan famously called a "risk management" approach to monetary policy.

If the balance of risks is tilted very strongly in one direction, or if the distribution of risks is especially wide, there might be a case for us to act.

For example, we might need to provide forward guidance, i.e. specifying how we would react to particular risks. Alternatively, we might need to change our policy stance pre-emptively, especially in situations where tail risks are material and it becomes cost-efficient to truncate that part of the distribution.

The ECB's monetary policy since mid-2014 illustrates these two aspects well.

Around that time, we saw the balance of risks to the inflation outlook shift decisively downwards, while the distribution of risks widened to encompass outright deflation, as you can see by comparing the blue and red lines on my second slide. If they had materialised, those risks would have fundamentally compromised medium-term price stability, and so our strategy required us to respond – even though our central forecast at that time was for a low but positive rate of inflation in the years ahead.

We responded in two main ways.

First, we clarified our reaction function to the main risks we saw and the instruments we would use if each of those risks materialised.

This sent a clear signal to observers that we were ready to respond in the case of adverse contingencies.

Then, when those contingencies arose, we followed through with our forward guidance and introduced a set of policy measures that was designed to cover the full downside distribution of risks – that is, a very accommodative policy stance to combat disinflationary forces, and an option to be even more accommodative if the situation deteriorated into outright deflation.

Thanks to these policy interventions, the distribution of risks has narrowed considerably over time – as you can see from the yellow line – and we no longer see a meaningful probability of deflation. The balance of risks has

also shifted upwards as the economic recovery has gathered steam. The current economic expansion in the euro area is stronger than it has been for a decade and broader than for two decades.

This improving picture is the main reason for our recent decision to recalibrate our policy by reducing the pace of our monthly asset purchases from €60 billion to €30 billion, starting in January.

Of course, risks emanate not only from our own jurisdiction, the euro area, where we can respond with our monetary policy, but also from the rest of the world. Indeed, while the ECB's Governing Council currently sees the risks surrounding the euro area's growth outlook as broadly balanced, it sees downside risks relating primarily to global factors.

But here too we can manage risks effectively by cooperating closely with other central banks.

This does not mean that we decide jointly on policy actions. It rather means that through our regular bilateral contacts, and dialogues in multilateral fora such as the IMF, the BIS and the G20, we can achieve a better understanding of global risks and their channels of propagation. And when risks do turn into shocks, this cooperation allows us to build up readiness and have the tools in place to react.

Perhaps most importantly, since 2011, the ECB has operated a permanent network of swap lines with the Bank of England, the Bank of Japan, the Federal Reserve and others, allowing all participating central banks to obtain foreign currency in the event of a liquidity squeeze.

In 2013, the ECB also established a swap agreement with the People's Bank of China in recognition of its growing systemic importance as well as the rapidly growing bilateral trade and investment between the euro area and China.

Factoring in political risks

So how do we factor political risks into our decision-making?

I would argue that central banks cannot process political risks in the same way as economic risks, for two reasons.

The first relates to the degree of uncertainty that surrounds political risks.

Here it is useful to recall Frank Knight's classic distinction between risk and uncertainty.

Risk is present when future events occur with measurable probability. Uncertainty arises when the likelihood of future events is indefinite or incalculable. In conditions of uncertainty, it is not possible to manage risk in the sense of quantifying a range of outcomes. Decision-making then depends on qualitative judgement.

To be sure, this is sometimes the situation central banks find themselves in when surveying the economic outlook. The economy is always characterised by both risk and uncertainty, and there are certain situations – for instance, financial crises – in which models fail and uncertainty prevails. In these cases, central banks still have to take decisions and judgement is the only basis we have.

Yet, I would venture that economic risks are, on the whole, more quantifiable than political ones, and hence more conducive to active risk management. This is because we have workable models of the economy with broadly established parameters and regularities. And even when the parameters of those models appear to change – like the Phillips curve today – they still provide us with a framework to think about those deviations and attempt to explain what we are seeing.

For politics, however, we rarely have such tools.

We may be able to gauge from opinion polls the likelihood of a political change of course happening. We may even be able to weigh up political parties' manifestos and estimate some of the economic consequences of their coming to power.

But fundamentally, we know little about how consumers and firms will react to political developments, and especially to the types of seismic political change that are macroeconomically relevant. Indeed, for such events to be considered a risk they are usually unprecedented.

This means that if we were to engage in managing political risks ex ante, most of the time we would be operating in uncertain circumstances and making judgement calls. I would question whether this could really be called risk management at all. Worse still, it would project us into the political domain on very shaky analytical foundations.

This brings me to the second reason why economic and political risks have to be treated separately, and it relates to the endogeneity between monetary policy and risks. In the economic realm, such endogeneity has been recognised as desirable and is a key reason why central banks have become much more transparent over the past two decades or so.

A clear understanding by the public of how the central bank will react to economic risks automatically reduces the likelihood of such risks materialising.

For instance, if markets expect central banks to react to adverse shocks by providing monetary accommodation, easier financial conditions will immediately follow. Such anticipation effects can increase the effectiveness of monetary policy.

For political risks, however, establishing such expectations would not be desirable. If we were to communicate that we will take decision "X" in response to political outcome "Y", financial conditions would move as the probability of that outcome rose, and this would potentially prejudice the result. That would be controversial in the case of global political risks. For domestic ones, it would be unacceptable.

Even if the central bank had perfect foresight of the economic consequences, such a reaction function would be seen as undue interference in the political process and it could undermine the effectiveness of monetary policy, instead of increasing it.

And since our assessment would be largely based on judgement not analysis – for the reasons I mentioned – we would find ourselves being accused of political meddling. This is a position that no independent central bank would want to be in.

So when it comes to political risks, we have to be data-driven. We do not prejudge political outcomes. And we do not try to risk-manage their effects on the economy, since we can rarely predict those effects accurately – and worse, we may end up influencing political developments and thereby compromising our independence.

The only way in which we can include political risks in our policy framework is by responding to their visible impact on economic and financial conditions. This does not mean being complacent: we can and must plan for all eventualities. But we react to data, not to political events themselves.

In some ways, this is analogous to the debate about "leaning versus cleaning" of financial bubbles: faced with so much uncertainty about what constitutes a bubble, most of the time it is more efficient for central banks to use macroprudential tools to prick bubbles, or to ease policy after they burst, rather than to try and identify bubbles in advance and deflate them by hiking rates. The risk of false positives is just too high.

Two episodes in the recent history of Europe illustrate our data-dependent reaction function: the threat of a break-up of the euro area in 2012; and the threat of a country leaving the European Union in 2016, namely the United Kingdom.

In the first case, we had plenty of data showing that political risks were spilling over dangerously into the economy and financial system. Markets began pricing in redenomination risk. Financial conditions tightened significantly in some Member States.

Bank lending contracted and the euro area entered a second recession. Uncertainty in the euro area, as measured by the VStoxx, was on the rise – as the grey shaded area on my third slide shows.

Although at this point inflation was still being buoyed up by energy prices and indirect taxes, it was plain to see that political risks had become economic ones, and were in turn endangering the medium-term outlook for price stability.

We therefore responded by launching a new monetary policy programme – Outright Monetary Transactions (OMTs) – which brought this episode of market turmoil to an end.

We did this, however, in a way that did not pre-empt political decisions. We took stock of the clear commitment of European leaders to hold our monetary union together and make it more solid by establishing a banking union. And we made the OMT programme conditional on countries participating in an assistance programme with the European Stability Mechanism.

In the case of the UK's vote to leave the EU, the situation was different, however. Various forecasts predicted severe market turbulence and macroeconomic fallout, so we had contingency plans in place for a range of outcomes. But as the slide illustrates, there were few signs of uncertainty in euro area financial markets in the run-up to the vote or after it. And, so far,

there turned out to be no economic consequences with medium-term impact.

So our policy stance remained consistent with the data: unchanged. And the same logic, incidentally, can be applied to the recent political crisis in Catalonia. Though we monitored the situation very closely, we saw no changes in financial conditions or the economy that would have warranted a monetary policy shift.

Conclusion

Let me conclude.

Monetary policy is a forward-looking enterprise and policymakers always have to think in terms of risks. On several occasions in recent years the ECB has changed its monetary policy in response to emerging tail risks, even when our central forecasts for inflation painted a less alarming picture.

This can be seen as applying a risk management approach to monetary policy, in which we prioritised truncating the most dangerous tails of the distribution rather than targeting our policy at the modal point. The frequent central forecast misses we experienced suggest we were right to do so and we avoided much worse outcomes as a result.

When it comes to political risks, however, central banks cannot be risk managers, since this would bring us too close to being political actors. We can monitor political risks, and we can put in place plans for responding to them – but we can only act when the data justify such a step, and in a way that does not pre-empt political decisions.

Our actions during the crisis clearly demonstrated this reaction function.

Thank you.

Early Observations on Improving the Effectiveness of Post-Crisis Regulation

Vice Chairman for Supervision Randal K. Quarles, at the American Bar Association Banking Law Committee Annual Meeting, Washington, D.C.

It is a pleasure to be here with you at the American Bar Association banking law committee annual meeting.

Thank you to Meg Tahyar, my longtime friend and colleague, for inviting me to speak today. These are still the early days of my tenure at the Federal Reserve--last weekend marked my first three months as the first Vice Chairman for Supervision.

In those three months, people have had a lot of questions for me, but the most frequently asked question has been: What's next? Today I hope to give you some insights into how I am approaching the work of evaluating and improving the post-crisis regulatory regime and to outline some specific areas that are emerging as areas of focus early in my tenure.

Some of those areas are closer to being ready for action, while others are topics that I believe are important and would benefit from more attention and discussion. My hope is that you will come away from our time together with a better sense of my preliminary thinking for charting a course forward on financial regulation.

Efficiency, Transparency, and Simplicity of Regulation

Before I delve into specifics, let me say a few words about the principles that are guiding my approach to evaluating changes to the current regime. The body of post-crisis financial regulation is broad in scope, complicated in detail, and extraordinarily ambitious in its objectives.

Core aspects of that project have resulted in critical gains to our financial system: higher and better quality capital, an innovative stress testing regime, new liquidity regulation, and improvements in the resolvability of large firms.

We undoubtedly have a stronger and more resilient financial system due in significant part to the gains from those core reforms. These achievements are consistent with the responsibility of the Federal Reserve to be a steward of a safe financial system, and with the goal of maintaining the ability of banks to lend through the business cycle.

That said, the Federal Reserve and our colleagues at other agencies have now spent the better part of the past decade building out and standing up the post-crisis regulatory regime. At this point, we have completed the bulk of the work of post-crisis regulation, with an important exception being the U.S. implementation of the recently concluded Basel III "end game" agreement on bank capital standards at the Basel Committee.

As such, now is an eminently natural and expected time to step back and assess those efforts. It is our responsibility to ensure that they are working as intended and--given the breadth and complexity of this new body of regulation--it is inevitable that we will be able to improve them, especially with the benefit of experience and hindsight.

In undertaking this review and assessment, in addition to ensuring that we are satisfied with the effectiveness of these regulations, I believe that we have an opportunity to improve the efficiency, transparency, and simplicity of regulation.

By efficiency I mean the degree to which the net cost of regulation--whether in reduced economic growth or in increased frictions in the financial system--is outweighed by the benefits of the regulation. In other words, if we have a choice between two methods of equal effectiveness in achieving a goal, we should strive to choose the one that is less burdensome for both the system and regulators.

Efficiency of regulation can be improved through a variety of means. For example, it can mean achieving a given regulation's objective using fewer tools. It can mean addressing unintended adverse consequences to the industry and the broader public from a regulation or eliminating perverse incentives created by a regulation. It can mean calibrating a given regulation more precisely to the risks in need of mitigation.

It can also mean simpler examination procedures for bank supervisors, or less intrusive examinations for well managed firms. In our approach to assessing post-crisis regulation, we should consider all of these ways of improving efficiency.

Transparency is an objective that ought to particularly resonate with this audience. As lawyers, we were all trained to view transparency as a necessary precondition to the core democratic ideal of government accountability--the governed have a right to know the rules imposed on them by the government. In addition, as any good lawyer also recognizes, there are valuable, practical benefits to transparency around rulemaking; even good ideas can improve as a result of exposure to a variety of perspectives.

Finally, simplicity of regulation is a principle that promotes public understanding of regulation, promotes meaningful compliance by the industry with regulation, and reduces unexpected negative synergies among regulations. Confusion that results from overly complex regulation does not advance the goal of a safe system.

Common Ground Areas of Improvement

When I arrived at the Federal Reserve, the early stages of reflection on how to improve the cost-benefit balance of post-crisis regulation had already begun, mainly in a few narrow areas of focus.

These were areas of low-hanging fruit in which relatively broad consensus was reached that efficiency enhancements were available with no material cost to the resiliency or resolvability of the banking system.

My colleague and Chairman-nominee Jay Powell spoke about five of these areas last summer when he served as the Board's oversight governor for supervision and regulation: small bank capital simplification, burden reduction in resolution planning, enhancements to stress testing, leverage ratio recalibration, and Volcker rule simplification.

I wholeheartedly support these initiatives, and I am pleased that some of them have progressed even in the months since the summer.

The banking agencies recently proposed changes to the capital rules for smaller firms, consistent with last year's Economic Growth and Regulatory Paperwork Reduction Act report, which is a positive step toward meaningful burden relief for smaller banks.

The Federal Reserve, along with the Federal Deposit Insurance Corporation, extended the upcoming resolution planning cycles for the eight most systemic domestic banking firms and for foreign banks with limited U.S. operations in order to allow for more time between submissions.

I believe we should continue to improve the resolution planning process in light of the substantial progress made by firms over the past few years, including a permanent extension of submission cycles from annual to once every two years and reduced burden for banking firms with less significant systemic footprints.

And, most recently, the Federal Reserve released a package of proposed enhancements to the transparency of our stress testing program, which is currently out for comment.

The progress you have seen in those areas represents constructive early steps.

Leverage ratio recalibration also is among the Federal Reserve's highest-priority, near-term initiatives. We have made considerable progress on that front in the past few months, and I expect that you will see a proposal on this topic relatively soon.

Finally, the relevant agencies have begun work on a proposal to streamline the Volcker rule. This project is a quite comprehensive and substantial undertaking as well as a five-agency endeavor.

As such, it will naturally take a bit of work for the agencies to congeal around a thoughtful Volcker rule 2.0 proposal for public review. Volcker rule reform remains a priority in the Federal Reserve's regulatory efforts.

Emerging Areas for Review

With that update on the familiar, I will turn to my own impressions of what is next for post-crisis regulation. In my early days as the Vice Chairman for Supervision, I asked our staff to conduct a comprehensive review of the regulations in the core areas of reform that I outlined earlier--capital, stress testing, liquidity, and resolution.

The objective is to consider the effect of those regulatory frameworks on resiliency and resolvability of the financial system, on credit availability

and economic growth, and more broadly to evaluate their costs and benefits.
This is a comprehensive and serious process, and work is still underway. I should note, however, that I have already formed views on a few areas that warrant more focus, and that I will be working with my colleagues on the Board to constructively consider.

I will start with the issue of tailoring supervision and regulation to the size, systemic footprint, risk profile, and business model of banking firms.

The Federal Reserve has devoted considerable energy in its post-crisis regulatory work to incorporate the tailoring concept in its regulation and supervision across the spectrum of small, medium, and large firms.

A recent example of this approach is our late 2017 proposal to simplify capital requirements for small- and medium-sized banking firms. In my view, there is further work for the Federal Reserve and the other banking agencies to do on the tailoring front.

I would emphasize that tailoring is not an objective limited in scope to a subset of the smallest firms. As my colleagues and I have said before, the character of our regulation should match the character of the risk at the institution.

Accordingly, we should also be looking at additional opportunities for more tailoring for larger, non-Global Systemically Important Banks, or non-G-SIBs.

In this regard, I support congressional efforts regarding tailoring, whether by raising the current $50 billion statutory threshold for application of enhanced prudential standards or by articulating a so-called factors-based threshold.

Irrespective of where the legislative efforts land, I believe we at the Federal Reserve have the responsibility to ensure that we do further tailoring for the institutions that remain subject to our rules to ensure that regulation matches the risk of the firm.

Take for example large non-G-SIBs whose failure would not individually pose a risk to U.S. financial stability.

Even without financial stability implications, the distress or failure of these firms still could harm the U.S. economy by, for example, significantly disrupting the flow of credit to households and businesses.

In my view, this tranche of the U.S. banking system ought to be subject to regulations that are generally stricter than those that apply to small banking firms, but that are also meaningfully less strict than those that apply to the G-SIBs.

The Board has effected this sort of G-SIB versus non-G-SIB tailoring among large banks in many areas of the regulatory framework.

Most notably, each of the risk-based capital requirements, leverage requirements, stress testing requirements, and total loss-absorbing capacity (TLAC) requirements is calibrated substantially more strictly for G-SIBs than for large non-G-SIBs.

However, in some key regulations, there is no distinction between the requirements for large non-G-SIBs and G-SIBs.

Liquidity regulation, for example, does not have a G-SIB versus non-G-SIB gradation.

In particular, the full liquidity coverage ratio (LCR) requirement and internal stress testing requirements of enhanced prudential standards apply to large, non-G-SIB banks in the same way that they apply to G-SIB banks.

I believe it is time to take concrete steps toward calibrating liquidity requirements differently for large, non-G-SIBs than for G-SIBs.

And I see prospects for further liquidity tailoring in that the content and frequency of LCR reporting are the same for the range of firms currently subject to the modified LCR as they are for the large non-G-SIBs that are subject to the full LCR.

We should also explore opportunities to apply additional tailoring for these firms in other areas, such as single counterparty credit limits and resolution planning requirements.

Another area that I think we should revisit are the "advanced approaches" thresholds that identify internationally active banks.

These thresholds are significant not only for identifying which banking firms are subject to the advanced approaches risk-based capital requirements, but also for identifying which firms are subject to various other Basel Committee standards, such as the supplementary leverage ratio, the countercyclical capital buffer, and the LCR.

The metrics used to identify internationally active firms--$250 billion in total assets or $10 billion in on-balance-sheet foreign exposures--were formulated well over a decade ago, were the result of a defensible but not ineluctable analysis, and have not been refined since then.

We should explore ways to bring these criteria into better alignment with our objectives.

A third area in which I will be working with my Board colleagues is a meaningful simplification of our framework of loss absorbency requirements.

There are different ways to count the number of loss absorbency constraints that our large banking firms face--which is perhaps in itself an indication of a surfeit of complexity if we can't be perfectly sure of how to count them--but the number I come up with is 24 total requirements in the framework.

While I do not know precisely the socially optimal number of loss absorbency requirements for large banking firms, I am reasonably certain that 24 is too many.

Candidates for simplification include: elimination of the advanced approaches risk-based capital requirements; one or more ratios in stress testing; and some simplification of our TLAC rule.

I am not the first Federal Reserve governor to mention some of these possibilities, and we should put them back on the table in the context of a more holistic discussion of streamlining these requirements.

Let me be clear, however, that while I am advocating a simplification of large bank loss absorbency requirements, I am not advocating an enervation of the regulatory capital regime applicable to large banking firms.

Although not a post-crisis regulation, the Board's complex and occasionally opaque framework for making determinations of control under the Bank

Holding Company Act (BHC Act) is another area that is ripe for re-examination through the lenses of efficiency, transparency, and simplicity. As you know, a determination of control under the BHC Act is significant because even remote entities in a controlled group can be subject to the BHC Act's restrictions on activities and a host of other regulatory requirements.

Under the Board's control framework--built up piecemeal over many decades--the practical determinants of when one company is deemed to control another are now quite a bit more ornate than the basic standards set forth in the statute and in some cases cannot be discovered except through supplication to someone who has spent a long apprenticeship in the art of Fed interpretation.

The process can be burdensome and time-consuming both for the requester and Federal Reserve staff. We are taking a serious look at rationalizing and recalibrating this framework.

Finally, as I mentioned earlier, an enhanced stress testing transparency package was released for public comment last month. I personally believe that our stress testing disclosures can go further.

I appreciate the risks to the financial system of the industry converging on the Federal Reserve's stress testing model too completely, so I am hesitant to support complete disclosure of our models for that reason.

However, I believe that the disclosure we have provided does not go far enough to provide visibility into the supervisory models that often deliver a firm's binding capital constraint.

It is important in any proposal to receive comments, and I can say that I and my colleagues on the Board will be paying particularly close attention to your comments on how we might improve this current proposal.

Concluding Remarks

To conclude, I hope that these remarks give you a sense of our approach to analyzing and improving post-crisis regulation.

As I mentioned earlier, the areas of core reform--capital, liquidity, stress testing, and resolution--have produced a stronger and more resilient system and should be preserved.

We have made great progress, but there is further work to do. Some clear improvements are in the offing in the relatively near future.
Other areas will benefit from longer term discussion. I look forward to engaging with you and the public more broadly as I help to chart a course for the important work ahead.

Raising Our Game: Cyber Security in an Age of Digital Transformation

Christopher Wray, Director, Federal Bureau of Investigation.
Fordham University - FBI International Conference on Cyber Security,
New York City, New York

Good morning. It's great to be here with you, and great to be back here in my hometown. Thank you all for joining us. I want to thank Father McShane and Fordham for continuing to help us bring people together to focus on cyber security.

Let me start by saying how honored I feel to be here representing the men and women of the FBI. The almost 37,000 agents, analysts, and staff I get to work with at Headquarters, in our field offices, and around the world are an extraordinary, dedicated, and quite frankly, inspiring bunch.

Not a day goes by that I'm not struck by countless examples of their patriotism, courage, professionalism, and integrity. And I could not be more proud, but also humbled, to stand with them as we face the formidable challenges of today—and tomorrow.

The work of the FBI is complex and hits upon nearly every threat facing our country. Today, I'd like to focus on the cyber threat.

Most of you have been thinking about the challenges in this particular arena for a long time. Before taking this job a few months ago, the last time I had to think seriously about cyber security through a law enforcement or national security lens was 12 years ago.

Back then, I was head of the Justice Department's Criminal Division, which included the Computer Crimes and Intellectual Property Section and handled cyber investigations.
It's safe to say that no area has evolved more dramatically since then, particularly given the blistering pace of technological change. And I've

spent much of the past few months getting caught up on all things cyber. So maybe the most useful thing I can do today is to offer the viewpoint of someone who's looking at this world with fresh eyes.

I'd like to talk to you about what the cyber threat picture looks like today; what the FBI is doing about it; and most important of all, what's the way forward? Where's the threat going? And where do we need to be to meet that threat? And then if we have time, I hope to answer a few questions.

The cyber threat has evolved dramatically since I left DOJ in 2005. Back then, social media didn't really exist as we know it today, and "tweeting" was something only birds did.

Now…well, let's just say it's something that's a little more on my radar. Today, we live much of our lives online, and everything that's important to us lives on the Internet—and that's a scary thought for a lot of people. What was once a minor threat—people hacking for fun or for bragging rights—has turned into full-blown economic espionage and lucrative cyber crime.

This threat now comes at us from all sides. We're worried about a range of threat actors, from multi-national cyber syndicates and insider threats to hacktivists. We're seeing an increase in nation-state sponsored computer intrusions. And we're also seeing a "blended threat"—nation-states using criminal hackers to carry out their dirty work. We're also concerned about a wide gamut of methods, from botnets to ransomware.

So what's the FBI doing about the cyber threat? Realistically, we know we can't prevent every attack, or punish every hacker. But we can build on our capabilities. We can strengthen our partnerships and our defenses. We can get better at exchanging information to identify the telltale signs that may help us link cyber criminals to their crimes. We can impose a variety of costs on criminals who think they can hide in the shadows of cyber space.

We can do all these things—and we are doing all these things.

We're improving the way we do business, blending traditional investigative techniques with technical capabilities. We're now assigning work based on cyber experience and ability, rather than on jurisdiction. We now have Cyber Action Teams of agents and experts who can deploy at a moment's notice, much like our Counterterrorism Fly Teams. We also now have Cyber Task Forces in every field office—much like our Joint Terrorism Task Forces—that respond to breaches, conduct victim-based investigations, and collect malware signatures and other actionable intelligence.

So we've strengthened our investigative capabilities, but we need to do our best to actually lay hands on the culprits and lock them up. And even where we can't reach them, we're now using all the tools at our disposal—we're "naming and shaming" them with indictments, and we're seeking sanctions from the Treasury Department.

We're also building on our partnerships. We're working more closely with our federal partners, because this threat is moving so quickly that there's no time for turf battles. It doesn't matter if you call us, or DHS, or any other agency—we all work together, so your information will get where it needs to go and you'll get the help you need. We care less about who you call than that you call, and that you call as promptly as possible.

We're also working more closely with our foreign partners. We now have cyber agents embedded with our international counterparts in strategic locations worldwide, helping to build relationships and coordinate investigations.

We're also trying to work better with our private sector partners. We're sharing indicators of compromise, tactics cyber criminals are using, and strategic threat information whenever we can. I'm sure you can appreciate there are times when we can't share as much as we'd like to, but we're trying to get better and smarter about that.

The good news is, we've made progress on a number of important fronts. Just this past summer, we took down AlphaBay—the largest marketplace on the DarkNet. Hundreds of thousands of criminals were anonymously buying and selling drugs, weapons, malware, stolen identities, and all sorts of other illegal goods and services through AlphaBay.

We worked with the DEA, the IRS, and Europol, and with partners around the globe, to dismantle the illicit business completely. But we were strategic about the takedown—we didn't want to rush it and lose these criminals. So, we waited patiently and we watched.

When we struck, AlphaBay's users flocked to another DarkNet marketplace, Hansa Market, in droves—right into the hands of our Dutch law enforcement partners who were there waiting for them, and they shut down that site, too.

So we're adapting our strategy to be more nimble and effective. But the bad news is, the criminals do that too.

I mentioned the "blended threat" earlier. Recently we had the Yahoo matter, where hackers stole information from more than 500 million Yahoo users. In response, last February we indicted two Russian Federal Security Service officers and two well-known criminal hackers who were working for them. That's the "blended threat"—you have intelligence operatives from nation-states like Russia now using mercenaries to carry out their crimes.

In March, our partners in the Royal Canadian Mounted Police arrested one of the hackers in Canada. The other three are Russian citizens living in Russia, but we made the judgment that it was worth calling them out, so now they're also fugitives wanted by the FBI—so their vacation destinations are more limited.

So we're making strides and we've had a number of successes—but the FBI still needs to do more to adapt to meet the cyber challenge.

For example, we want to do more to mitigate emerging threats as they spread. While we may not be able to stop all threats before they begin, we can do more at the beginning to stop threats before they get worse. We can share information, identify signatures, and stop similar attacks from happening elsewhere. But to do that, we need the private sector to work with us.

At the FBI, we treat victim companies as victims. So, please: When an intrusion affects critical infrastructure; when there's a potential for impact to national security, economic security, or public health and safety; when an attack results in a significant loss of data, systems, or control of systems; or when there are indications of unauthorized access to—or malware present on—critical IT systems, call us. Because we want to help you, and our focus will be on doing everything we can to help you.

Another thing driving the FBI's work is that at some point, we'll have to stop referring to all technical and digital challenges as "cyber." Sophisticated intrusions and cyber policy issues are very much at the forefront of the conversation. But we also have to recognize that there's a technology and digital component to almost every case we have now.

Transnational crime groups, sexual predators, fraudsters, and terrorists are transforming the way they do business as technology evolves. Significant pieces of these crimes—and our investigations of them—have a digital component or occur almost entirely online. And new technical trends are making the investigative environment a lot more complex. The Internet of

Things, for example, has led to phenomena like the Mirai botnet—malware that uses all these connected devices to overwhelm websites, like the attacks that took down Netflix and Twitter last year.

The digital environment also presents new challenges that the FBI has to address—all kinds of twists for us in terms of what's coming down the pike. Advances like artificial intelligence or crypto currencies have implications not only for the commercial sector, but for national security.

Encrypted communications are changing the way criminals and terrorists plan their crimes—I'll have more to say on that in a moment. And the avalanche of data created by our use of technology presents a huge challenge for every organization.

I'm convinced that the FBI—like a lot of other organizations—hasn't fully gotten our arms around these new technologies and their implications for our national security and cyber security work. On our end, we know we need to be working with the private sector to get a clearer understanding of what's coming around the bend.

We need to put our heads together, in conferences like this and in other ways, so we're better prepared, not just to face current threats, but the threats that will come at us five, 10, and 15 years from now.

When I was last in government, I saw how the 9/11 attacks spurred the FBI to fundamentally transform itself into a more intelligence-based national security organization. In the same way, I believe the new digital environment demands further fundamental transformation from us.

Over the years, FBI investigators have made huge strides in responding to the investigative challenges posed by the digital realm. We have pockets of excellence and talent that we've relied on to tackle our most complex technical challenges. But with the wholesale rise of digital challenges, this model won't work for us anymore.

As a big organization spread across 56 field offices and over 80 international offices, we need a new approach. We've got to increase our digital literacy across the board.

Some of our smartest people are looking at these challenges and thinking strategically about how the entire FBI can evolve in this rapidly changing environment. We're focused on building our digital capabilities. We're also

focusing on our people, making sure we continue to attract the right skills and talent—and develop the right talent internally.

One issue I'm fixated on is whether we're recruiting, hiring, and training now the kind of tech-savvy people we'll need in five or 10 years. We know that we need more cyber and digital literacy in every program throughout the Bureau—organized crime, crimes against children, white-collar crime, just to name a few.

Raising the average digital proficiency across the organization will allow all of our investigators to counter threats more efficiently and effectively, while freeing our true cyber "black belts" to focus on the most vexing attacks, like nation-state cyber intrusions.

We also need to focus more on innovation, approaching problems in new ways, with new ideas—which isn't something, to be honest, that always comes naturally in government. We can't just rely on the way we've always done things.

And I don't mean just technological innovation; I mean innovation in how we approach challenges, innovation in partnerships, innovation in who we hire, innovation in how we train, and innovation in how we build our workforce for the future.

So we need more innovation, and more of the right people. But the FBI can't navigate the digital landscape alone. We also need to build stronger partnerships—with our counterparts in federal agencies, with our international counterparts, with the cyber research community, and with the private sector.

And we need to do a better job of focusing our combined resources—trying to get our two together with your two to have it somehow equal more than four; to make it five or six or seven.

Finally, in some cases we may need lawmakers to update our laws to keep pace with technology. In some ways, it's as if we still had traffic laws that were written for the days of the horse-and-carriage.

The digital environment means we don't simply need improved technical tools; we also need legal clarifications to address gaps.

I want to wrap up by talking about two challenges connected to the digital revolution.

The first is what we call the "Going Dark" problem. This challenge grows larger and more complex every day. Needless to say, we face an enormous and increasing number of cases that rely on electronic evidence. We also face a situation where we're increasingly unable to access that evidence, despite lawful authority to do so.

Let me give you some numbers to put some meat on the bones of this problem. In fiscal year 2017, we were unable to access the content of 7,775 devices—using appropriate and available technical tools—even though we had the legal authority to do so. Each one of those nearly 7,800 devices is tied to a specific subject, a specific defendant, a specific victim, a specific threat.

I spoke to a group of chief information security officers recently, and someone asked about that number. They basically said, "What's the big deal? There are millions of devices out there." But we're not interested in the millions of devices used by everyday citizens. We're only interested in those devices that have been used to plan or execute criminal or terrorist activities.

Some have argued that having access to the content of communications isn't necessary—that we have a great deal of other information available outside of our smart phones and our devices; information including transactional information for calls and text messages, or metadata. While there's a certain amount we can glean from that, for purposes of prosecuting terrorists and criminals, words can be evidence, while mere association between subjects isn't evidence.

Being unable to access nearly 7,800 devices is a major public safety issue. That's more than half of all the devices we attempted to access in that timeframe—and that's just at the FBI. That's not even counting a lot of devices sought by other law enforcement agencies—our state, local, and foreign counterparts. It also doesn't count important situations outside of accessing a specific device, like when terrorists, spies, and criminals use encrypted messaging apps to communicate.

This problem impacts our investigations across the board—human trafficking, counterterrorism, counterintelligence, gangs, organized crime, child exploitation, and cyber. And this issue comes up in almost every conversation I have with leading law enforcement organizations, and with

my foreign counterparts from most countries—and typically in the first 30 minutes.

Let me be clear: The FBI supports information security measures, including strong encryption. But information security programs need to be thoughtfully designed so they don't undermine the lawful tools we need to keep this country safe.

While the FBI and law enforcement happen to be on the front lines of this problem, this is an urgent public safety issue for all of us. Because as horrifying as 7,800 in one year sounds, it's going to be a lot worse in just a couple of years if we don't find a responsible solution.

The solution, I'll admit, isn't so clear-cut. It will require a thoughtful and sensible approach, and may vary across business models and technologies, but—and I can't stress this enough—we need to work fast.

We have a whole bunch of folks at FBI Headquarters devoted to explaining this challenge and working with stakeholders to find a way forward. But we need and want the private sector's help. We need them to respond to lawfully issued court orders, in a way that is consistent with both the rule of law and strong cybersecurity. We need to have both, and can have both.

I recognize this entails varying degrees of innovation by the industry to ensure lawful access is available. But I just don't buy the claim that it's impossible.

For one thing, many of us in this room use cloud-based services. You're able to safely and securely access your e-mail, your files, and your music on your home computer, on your smartphone, or at an Internet café in Tokyo. In fact, if you buy a smartphone today, and a tablet in a year, you're still able to securely sync them and access your data on either device.

That didn't happen by accident. It's only possible because tech companies took seriously the real need for both flexible customer access to data and cyber security. We at the Bureau are simply asking that law enforcement's lawful need to access data be taken just as seriously.

Let me share just one example of how we might strike this balance. Some of you might know about the chat and messaging platform called Symphony, used by a group of major banks. It was marketed as offering "guaranteed data deletion," among other things. That didn't sit too well with the regulator for four of these banks, the New York State Department

of Financial Services. DFS was concerned that this feature could be used to hamper regulatory investigations on Wall Street.

In response to those concerns, the four banks reached an agreement with the Department to help ensure responsible use of Symphony. They agreed to keep a copy of all e-communications sent to or from them through Symphony for seven years. The banks also agreed to store duplicate copies of the decryption keys for their messages with independent custodians who aren't controlled by the banks. So the data in Symphony was still secure and encrypted—but also accessible to regulators, so they could do their jobs.

I'm confident that with a similar commitment to working together, we can find solutions to the Going Dark problem. After all, America leads the world in innovation. We have the brightest minds doing and creating fantastic things. If we can develop driverless cars that safely give the blind and disabled the independence to transport themselves; if we can establish entire computer-generated virtual worlds to safely take entertainment and education to the next level, surely we should be able to design devices that both provide data security and permit lawful access with a court order.

We're not looking for a "back door"—which I understand to mean some type of secret, insecure means of access. What we're asking for is the ability to access the device once we've obtained a warrant from an independent judge, who has said we have probable cause.

We need to work together—the government and the technology sector—to find a way forward, quickly.

In other parts of the world, American industry is encountering requirements for access to data—without any due process—from governments that operate a little differently than ours, to put it diplomatically.

It strikes me as odd that American technology providers would grant broad access to user data to foreign governments that may lack all sorts of fundamental process and rule of law protections—while at the same time denying access to specific user data in countries like ours, where law enforcement obtains warrants and court orders signed by independent judges.

I just cannot believe that any of us in this room thinks that paradox is the right way to go. That's no way to run a railroad, as the old saying goes.

A responsible solution will incorporate the best of two great American traditions—the rule of law and innovation. But for this to work, the private sector needs to recognize that it's part of the solution. We need them to come to the table with an idea of trying to find a solution, as opposed to trying to find a way to build systems to prevent a solution.

I'm open to all kinds of ideas, because I reject this notion that there could be such a place that no matter what kind of lawful authority you have, it's utterly beyond reach to protect innocent citizens. I also can't accept that anyone out there reasonably thinks the state of play as it exists now—and the direction it's going—is acceptable.

Finally, let me briefly mention another issue that has a huge effect on the FBI's national security work, including cyber—the re-authorization of Section 702 of the Foreign Intelligence Surveillance Act, or FISA.

The speed and scope of the cyber threat demands that we use every lawful, constitutional tool we've got to fight it. Section 702 is one of those tools.

I want to stress once again how vital this program is for the FBI's national security mission. Section 702 is an essential foreign intelligence authority that permits the targeted surveillance of non-U.S. persons overseas. It's especially valuable to the FBI, because it gives us the agility we need to stay ahead of today's rapidly changing global threats.

I bring all this up today because unless renewed by Congress, Section 702 is set to expire later this month. Without 702, we would open ourselves up to intelligence gaps that would make it easier for bad cyber actors and terrorists to attack us and our allies—and make it harder for us to detect these threats.

We simply can't afford for that to happen. So the FBI has spent an enormous amount of time, as have our partners in the intelligence community, working together with Congress to find a way to re-authorize Section 702 while addressing their concerns.

My fervent hope is that before the extension expires, Congress will re-authorize Section 702 in a manner that doesn't significantly affect our operational use of the program, or endanger the security of the American people.

So that's a perspective on cyber from the new guy back on the block.

If one thing's become clear to me after immersing myself again in this world for the past few months, it's the urgency of the task we all face. High-impact intrusions are becoming more common; the threats are growing more complex; and the stakes are higher than ever.

That requires all of us to raise our game—whether we're in law enforcement, in government, in the private sector or the tech industry, in the security field, or in academia. We need to work together to stay ahead of the threat and to adapt to changing technologies and their consequences—both expected and unexpected. Because at the end of the day, we all want the same thing: To protect our innovation, our systems, and, above all, our people.

Thank you all for everything you're doing to make the digital world safer and more secure, and for joining us here in New York. I look forward to working with you in the years to come.

Now I'd be happy to take a few questions.

Typosquatting is still big business

National Cyber Security Centre
a part of GCHQ

Typosquatting (also known as cybersquatting or url hijacking) is the deliberate act of registering misspelt popular website domains, to capitalise on internet users accidently typing incorrect characters for a website address into the address bar of a web browser.

Instead of visiting the correct website, users will be taken to an alternative website intended for a variety of malicious purposes, including the theft of personal information, fraud and the installation of malicious software.

A recent study by cyber security company Sophos found that typosquatting is still a huge industry and there are a significant number of fake domains registered, including sites targeting users of popular websites such as Google, Facebook, Twitter, Microsoft and Apple.

Specifically, it was found that 80% of all possible one-character variants of Facebook, Google, and Apple website domains are registered.

The issue of typosquatting is not new but can seriously impact individual users as well as businesses, organisations and government websites across the globe.

Although there are solutions including the legitimate purchase of common misspelt domains as part of brand protection, this could amount to hundreds of possible domain name variants which might not be practical or cost effective, particularly for small businesses.

Individual users are advised to double check their url spellings before accessing a website. It is also advisable to bookmark favourite websites and, if in doubt, check url spellings in a popular search engine to make sure they are correct.

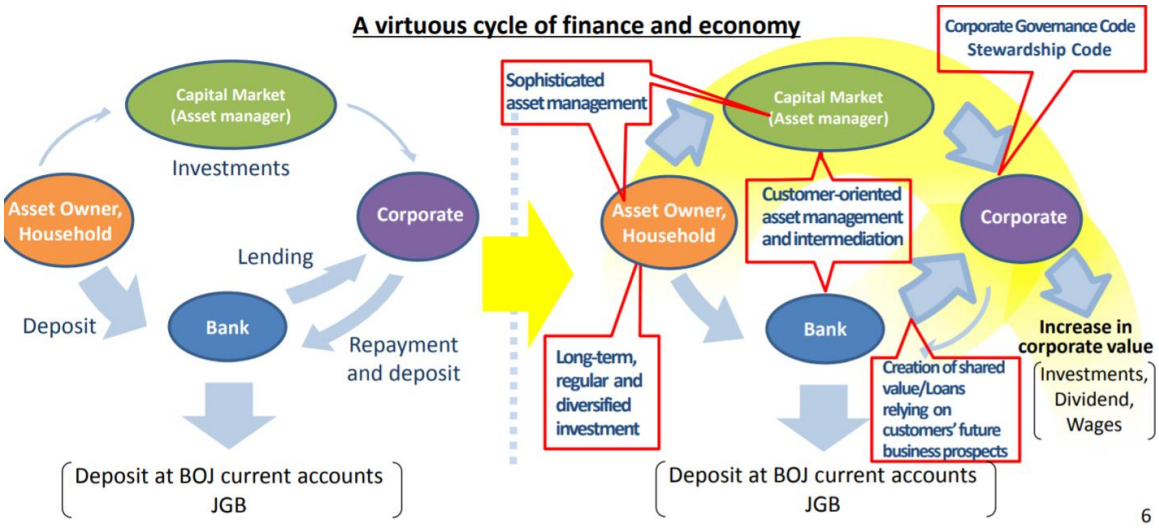
Japanese Financial Service Agency (JFSA)
Summary Points from
Strategic Directions and Priorities, 2017-2018

Financial Services Agency

The Financial Service Agency (JFSA) annually publishes the Strategic Directions and Priorities to clarify its policy goals for each program year since 2015.

The JFSA is committed to continuous enhancement of the quality of regulation and supervision through the PDCA cycle. The Strategic Directions and Priorities corresponds to the "Plan" stage, and, after the completion of each program year, the JFSA reviews the progress made and identifies the remaining tasks and emerging issues.

The findings are summarized in the Progress and Assessment of the Strategic Directions and Priorities in the "Check" stage.



To read more:
http://www.fsa.go.jp/en/news/2018/2017StrategicDirectionsSummary-English.pdf

Ransomware fears cause companies to hoard Bitcoin

National Cyber Security Centre
a part of GCHQ

Companies are reportedly stockpiling cryptocurrencies to hedge against the possible need to pay off cyber criminals.

Some firms are said to be investing in Bitcoin and Ethereum to ensure that they have cryptocurrency funds available if they are affected by a ransomware attack.

A survey carried out earlier this year by Citrix found that 42% of companies surveyed were building cryptocurrency stockpiles for ransomware payments, with 28% holding more than 30 bitcoins.

The cost of paying ransoms is increasing rapidly along with the value of the cryptocurrencies in which they are paid, so by investing now, some companies hope to ensure that the cost of a ransom is less pricey than it might be later.

However, this approach comes with its own risks, as such holdings may themselves be targeted. With a single bitcoin now worth over $17,000 (£12,000), a company's cryptocurrency wallet can be worth a substantial amount to a cyber criminal.

The NCSC's website provides further advice to organisations that may be affected by ransomware. The NCSC does not offer advice on whether or not companies should invest in Bitcoin. While it is a matter for the victim whether or not to pay a ransom, the National Crime Agency encourages industry and the public not to do so.

You may visit:
https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

To count or not to count - the future of internal models in banking regulation

Dr Andreas Dombret, Member of the Executive Board of the Deutsche Bundesbank, at the EBA Policy Research Workshop "The future role of quantitative models in financial regulation", London.

1. Introduction

Ladies and gentlemen

Dear Andrea Enria

Thank you for the invitation and your kind introduction. After I accepted to give the keynote at this risk modelling conference, a colleague shared with me an unflattering comparison of financial risk modellers with weather forecasters. He asked: Why do you think weather forecasters like financial risk modellers so much? His answer: Because the only kind of storm less well predicted than hurricanes and tornadoes are financial storms.

In my keynote today, I will frame this conference in a more positive tone, as I see a lot of merit in financial risk modelling - and in weather forecasting, too, for that matter.

Yet during and after the financial crisis we witnessed severe instances of risk model failure - where internal calculations of many banks grossly underestimated actual risks.

Remember for example the systematic underestimation of a market freeze or a price bubble before the sub-prime crisis broke. The many unexpected lawsuits pointed to further blind spots - all of which suddenly led to capital cushions melting away.

However, focusing on these failures alone misses the fact that, overall, financial risk modelling has improved risk measurement substantially. It

has inspired us to reconsider the role and the liberties of internal modelling.

And this is partly why you are at today's EBA workshop - to improve internal models. Your agenda includes challenging topics. My aim is far more modest. In my statement this morning I will take stock of risk modelling and the "lessons learned" from the financial crisis.

I will highlight both the limitations and the strengths of internal modelling. Second, I will present general principles that should guide future work. And, third, I will outline my take on where current and future EU projects on internal models should be heading.

2. Financial crisis, regulatory reform and internal models

But first, let's take a step back. Fifteen years ago, internal risk models were considered the gold standard for optimising capital allocation. What made them so successful was the efficient use of capital and their high risk sensitivity - which was made possible by granting banks substantial freedom in using their internal models for regulatory capital calculation.

Even though Basel II limited the freedom of banks by setting several parameters for the internal ratings-based (IRB) approaches, IRB banks had substantial room for manoeuvre when calculating their capital ratios.

This made internal risk models prone to abuse. But those who pointed to these shortcomings, or just to their unrealistic assumptions, have frequently been called unscientific and opposed to innovation.

Then the financial crisis erupted, changing almost everything in finance. Models played their part in contributing to the turmoil. Risk modelling moved from panacea to placebo or even steroid. Individual calculations of many banks were not crisis-proof, as their assumptions were way too optimistic. In fact, some models even fostered herding behaviour.

In 2010, the Basel Committee decided to take a closer look at the root problems of internal models. The core question was whether differences in capital ratios of banks were due to differences in portfolios or due to illegitimate differences in modelling practices.

In three studies we assessed the risk-weighting of banking and trading book assets. Material variances in regulatory capital ratios were found. Only a part of these could be explained by differences of risk profiles.

But another substantial part of the variation arose not from differences in the riskiness of bank portfolios, but instead from other factors that are due to modelling problems - for example, some banks gamed model weaknesses, and some of the terms specified by supervisors proved to be problematic.

One of the main reasons for these unwarranted differences is that models were even applied to portfolios where the statistical presumptions are violated. For example, in low default portfolios you simply do not have enough historical cases of default to calculate a reliable credit default figure.

Another prominent example is that extreme events, meaning crises, occur more often in real life than the distribution of most models assumes.

But there is an even bigger threat when applying modelling techniques. The big mistake is to believe that financial risk models can ever be fully accurate or even close to it. The point is fundamental, yet simple: risk models have fundamental limits that can never be fully remedied - which is why strong regulatory boundaries and supervisory controls are indispensable.

To make my point, I have to get a bit philosophical. There are two types of limits, and let us turn to a great economist to define their nature. In 1921, Frank Knight differentiated between risk and uncertainty.

Uncertainty describes the unexpected events. The first limit of models is that they cannot capture uncertainty. Uncertainty is fundamental, because we do not know what the future will bring - it is hardly manageable. It is quite substantial when it comes to financial risk modelling.

That's because financial risk modelling is a social science. The models can only provide a simplified heuristic of real social interaction, but it is impossible to fully grasp the complexity.

The second limit of models concerns how Knight defined risk. Risk is what we can somehow manage, thanks to the law of large numbers, with a margin of error. Risk is what we can model. Yet, even in this comfort zone of risk models some limitations exist: real events can only be forecasted, like weather, but cannot be predicted - data as well as methods face natural limitations.

All in all, this means: Modelling is probably as scientific as it can get in banking regulation. However, models can never get a calculation fully right.

To limit mis-measurement, we have to deal with risk and uncertainty:

- First, close gaps in the regulation of risk measurement. This includes data limitations: we can only model where sufficient data are available. Defaults in sovereign bonds, for example, clearly do not fulfil this condition.

- Second, work is needed on methodological shortcomings: we have to insist on robustness checks and need to limit the degrees of freedom for financial institutions, for example with regard to assumptions about distributions.

- Third, one has to accept Knightian uncertainty and protect regulation against it - human behaviour changes, irrational exuberance prevails, extreme events like herding behaviour repeat themselves, and market actors will always test the limits of models. We cannot model these challenges away. That's why we need backstops. Models need checks and balances, since a sole focus on model-based capital minimisation would be dangerous for financial stability.

3. Benefits of internal models

So, internal risk modelling for regulatory purposes clearly has its weaknesses. Nevertheless, I am convinced that the benefits very much outweigh the drawbacks.

The first advantage of risk models doesn't sound very encouraging, but it is nevertheless quite important. Their strength is that they get it less false than any other approach we have.

For as long as we work on the approach of risk-based regulation, we have to somehow quantify risks; and there is no way we can do without educated guessing. Any minimum capital requirement we impose on institutions requires more or less uncertain assumptions about the riskiness involved.

This holds true not only for internal models, but also for standardised approaches to risks. Even the rather conservative regulatory risk weights of standardised approaches may result in over-optimistic capital charges - just look at sovereign bonds.

Moreover, institutions using standardised approaches can engage in "risk shifting" - that is the search for the most profitable, but also the most risky assets among equal risk weights.

Thus, even if we banned models entirely from regulation, we would still end up with a vulnerable way to measure risk. Risk models are the better imperfect options.

The second strength of models actually is their variation. For not all of the variability of internal models is necessarily undesired. There may be good reasons for divergent capital requirements based on similar credit portfolios, for instance because of dissimilar effectiveness of risk management in banks or given a different legal environment in which banks are operating.

Also, model variability reduces the risk of herding behaviour, which would arise if every bank were to use the same standardised approach.

The third - and in my view most important - strength of risk models is their high degree of risk sensitivity. For each type and each category, capital requirements calculated by an institution's own models is typically a lot more in line with historically observed risk.

And this, in turn, has positive consequences. For example, it incentivises risk-adequate behaviour in financial institutions in general. From a supervisory point of view, we are especially interested in the additional incentives it offers to banks to develop and maintain a thorough risk assessment approach - which also supports and strengthens the internal risk management.

4. To count or not to count: internal models after regulatory reform

So far I have reminded us why internal model-based capital calculation - despite its weaknesses - remains a worthwhile regulatory tool. Accordingly, the post-crisis regulatory agenda still builds on the principle of risk-based regulation and still encourages the use of internal modelling techniques.

The Basel Committee has decided to remove only one internal approach in its entirety - the Advanced Measurement Approach for operational risk, AMA for short. Apart from that, models still play an important role in the Basel III finalisation package. And as I have mentioned, there are good reasons for that.

Yet, moving forward, we need to incorporate the "lessons learned" into regulation and into supervisory processes.

We have done this by installing additional constraints and backstops to close gaps that internal models cannot close - most prominently the leverage ratio and the output floor.

Further safeguards are implemented by more rigorous methods, data rules and input floors. This means that regulation has become multi-polar - supervisors rely on various, complementary requirements.

But at the same time there is also a need to support the benefits of internal models. On the Basel Committee, the German representatives resolutely argued in favour of maintaining risk sensitivity in regulation, because this is the best way to capture the actual risks of a financial institution and to set the right incentives, thereby discouraging excessive risk-taking.

This especially concerns the subject of calibrating the output floor, which is - as most of you know - a limit to internal model calculations based on the standardised approaches.

With the advantages of internal modelling in mind, this topic is understandable. And for me, the current state of negotiations - an output floor of 72.5 per cent - is too high; but it is still enough for models to remain an attractive tool. While risk sensitivity will be diminished by setting the output floor at this level, it still represents a far better outcome than the originally envisioned output floor of 80 per cent.

Basel III is better than its critics claim: While some countries may gold-plate their national regulations through a ban of internal models - the new standard also enables the Basel countries to continue the use of internal models. And this is an important outcome.

5. You can count on that: better models for the future

Now we have to look ahead. We should take the Basel III reforms and implement them in a manner that improves risk models further.

Banks have to build better models, models that not only focus on the efficient use of capital but also ensure that a bank can weather future storms. Both goals must weigh equally, meaning that the storm-forecasting part has to be given much more attention.

Authorities like the SSM and EBA on the other hand will have to roll up their sleeves and build a regulatory and supervisory framework for the future of risk measurement.

This will be challenging not only for the sheer technical complexity, but also because we have to strike two balances at once:

- The first balance is to maintain the incentives for fine-tuned risk measurement and management on the one hand, while improving the checks and balances on risk models on the other.

- When pursuing this balance, we obviously have to do this on EU level. In that context, we need to strike the second balance: in order to guarantee the same high standards in the entire SSM, we have to achieve EU- and SSM-wide harmonisation on the one hand; on the other hand, however, we should not go too far, meaning that we cannot achieve an exhaustive list for each and any model decision. While we need harmonisation of definitions and supervisory procedures - in order to close relevant gaps - supervisory agencies should not be condemned to taking a box-ticking approach. Since every model is different, the box-ticking approach would only undermine a critical review of a bank's model.

I believe it to be important that we keep these balances in mind when we come to design new rules or redesign old ones.

Let me now outline the priorities for future work on improving internal models in the EU from the Bundesbank's point of view.

With regard to credit risk and the boundaries for the IRB approaches, it's important that we implement the Basel III compromise in a rigorous way. This means that input and output floors will prevent the internal calculations of regulatory capital requirements from going too low. But at the same time, it maintains the internal modelling approach and, with that, substantial freedoms for banks to calculate regulatory capital.

Another important point concerns credit risks, but also other risk type models. The targeted review of internal models, the TRIM project, by the SSM should be conducted in a responsible and considered manner - it needs to strike the two balances that I highlighted. This means specifically:

- The biotope of risk modelling approaches must be kept diverse. A right understanding of harmonisation means not only treating equal things

equally, but also treating unequal things unequally. TRIM must ensure, that the playing field for banks is levelled, but not create a monoculture of models driven by supervisory rules.

- Furthermore, it means that we have to balance conservativism and precision. Supervisors will always be tempted to make risk estimates more conservative - which is, of course, prudent. Being too conservative, however will make risk models less attractive for banks to use it not only as a regulatory instrument but also as an effective internal risk management tool.

- Finally, changes that we will introduce through the TRIM project must be implemented in a reasonable manner. Banks need a transitional period to adopt the new standards.

Let me close these policy guidelines with a clear statement: Throughout all regulatory and supervisory projects to finalise the reform agenda for internal modelling, the Bundesbank will advocate the retention of risk sensitivity.

6. Conclusion

Ladies and gentlemen

You have a full agenda of challenges in risk modelling ahead of you. Moreover, during the coming years you hopefully will help to make financial risk models better.

My key take-aways for these one and a half days and your future work are:

- First, internal models have rightfully lost their sacrosanct status, as they revealed big weaknesses during the last financial crisis. Models will never be perfect. We always have to be aware of the underlying assumptions and their shortcomings.

- Second, after regulatory reform, internal models rightly continue to play a big role, but now a complementary one. Limits have been set. But we shouldn't overreact. It is also important to maintain incentives for banks with regard to a risk-sensitive framework. This is why, on the Basel Committee, German authorities have resolutely argued in favour of sufficient incentives for internal models.

- Third, on the basis of the limits set by the Basel III reforms, we have to look forward now, and NCAs, EBA and SSM have to set about improving internal models further so that they can contribute to efficient and stable financial markets - at the service of the real economy.

Again, many thanks for inviting me - I wish all of you a fruitful workshop. Thank you for your kind attention.

U.S. Departments of Commerce, Homeland Security Release Preliminary Report on Promoting Action Against Botnets and Other Automated Threats

The U.S. Department of Commerce and the U.S. Department of Homeland Security released a draft report to President Trump in response to the May 11, 2017, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

"Cybersecurity is perhaps one of the most serious threats we face," said Secretary Ross. "President Trump understands the necessity of strengthening our networks and this Administration is doing everything in its power to prevent bad actors from infiltrating our critical cyber infrastructure."

The report, which was created with broad input from stakeholders and experts, summarizes the opportunities and challenges in reducing the botnet threat, and offers supporting actions to be taken by both the government and private sector in order to reduce the threat of automated cyber-attacks.

The report lists five complementary goals that would improve the resilience of the ecosystem:

1. Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace.

2. Promote innovation in the infrastructure for dynamic adaptation to evolving threats.

3. Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior.

4. Build coalitions between the security, infrastructure, and operational technology communities domestically and around the world.

5. Increase awareness and education across the ecosystem.

"Botnets represent a system-wide threat that no single stakeholder, not even the federal government, can address alone," said Walter G. Copan, Under Secretary of Commerce for Standards and Technology and Director of the National Institute of Standards and Technology.

"The report recommends a comprehensive way for the public and private sectors, as well as our international partners, to work together and strengthen our defenses."

You may visit:

https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the-president/draft/documents/enhancing-resilience-against-botnets-draft.pdf

Leverage ratio

Basel Committee on Banking Supervision
BANK FOR INTERNATIONAL SETTLEMENTS

Introduction

1. An underlying cause of the global financial crisis was the build-up of excessive on- and off-balance sheet leverage in the banking system.

In many cases, banks built up excessive leverage while reporting strong risk-based capital ratios.

At the height of the crisis, financial markets forced the banking sector to reduce its leverage in a manner that amplified downward pressures on asset prices.

This deleveraging process exacerbated the feedback loop between losses, falling bank capital and contracting credit availability.

2. The Basel III framework introduced a simple, transparent, Non-risk-based leverage ratio to act as a credible supplementary measure to the risk-based capital requirements.

The leverage ratio is intended to:

• restrict the build-up of leverage in the banking sector to avoid destabilising deleveraging processes that can damage the broader financial system and the economy; and

• reinforce the risk-based requirements with a simple, non-risk-based "backstop" measure.

3. The Committee is of the view that a simple leverage ratio framework is critical and complementary to the risk-based capital framework, and that the leverage ratio should adequately capture both the on- and off-balance sheet sources of banks' leverage.

Read more at page 140 of the Basel III reform paper (12/2017) at:
https://www.bis.org/bcbs/publ/d424.pdf

Finalising Basel III In brief

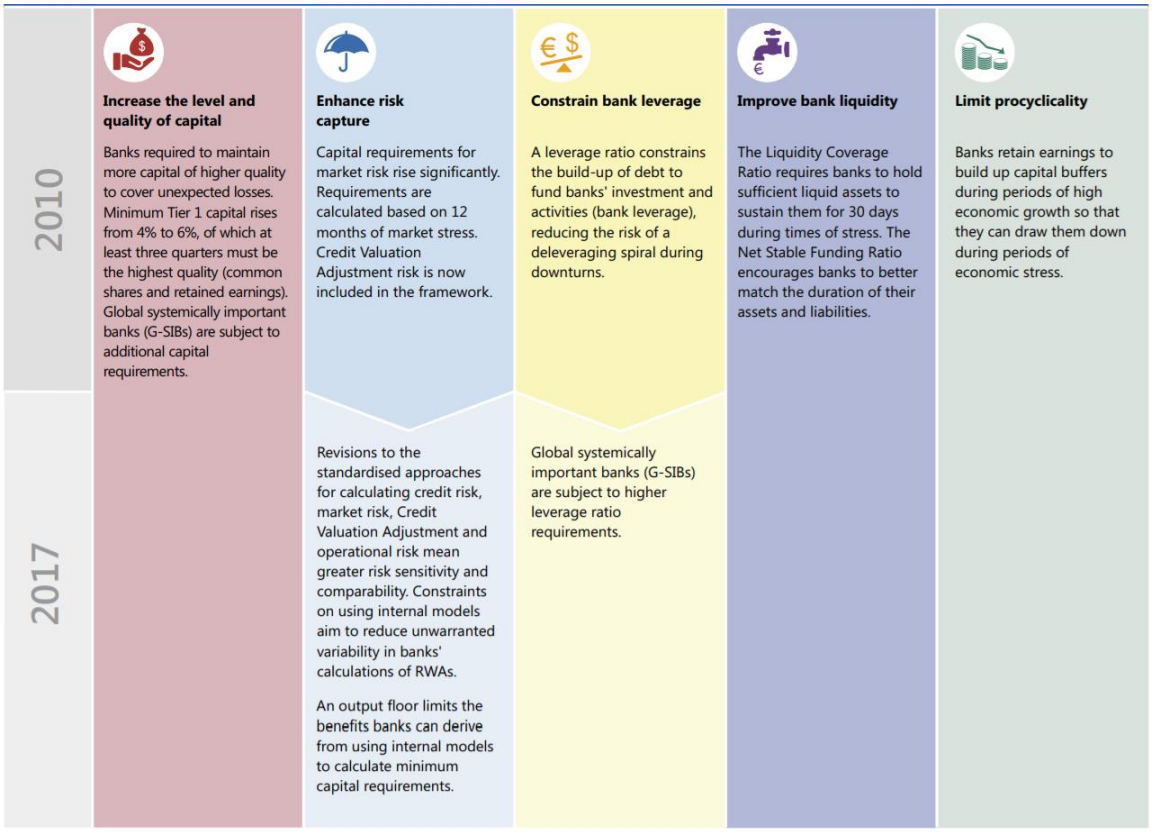
Basel Committee on Banking Supervision
BANK FOR INTERNATIONAL SETTLEMENTS

The Basel III reforms complement the initial phase of the Basel III reforms announced in 2010.

The 2017 reforms seek to restore credibility in the calculation of risk weighted assets (RWAs), and improve the comparability of banks' capital ratios.

RWAs are an estimate of risk that determines the minimum level of regulatory capital a bank must maintain to deal with unexpected losses.

A prudent and credible calculation of RWAs is an integral element of the risk-based capital framework.



To read more:
https://www.bis.org/bcbs/publ/d424_inbrief.pdf

Increase in HTTPS phishing attacks

National Cyber Security Centre
a part of GCHQ

Over the past few years website owners have been encouraged to adopt HTTPS website domains rather than HTTP. With HTTPS, data in transit is encrypted; this provides additional security for transiting data, such as login credentials, which may contain information of use to attackers.

HTTPS domains are verified by SSL Certificate Authorities, who issue and authenticate certificates. The padlock symbol in the URL field links to the certificate provider's website, and users are often advised to trust webpages with this symbol.

However, while the padlock shows that encryption is used, it does not guarantee the legitimacy of the website. It is possible for attackers to compromise sites using HTTPS domains and use them to host malicious links. It is also easy for attackers to obtain legitimate certificates (often for free) and use them to set up their own malicious website.

Although this rising attack trend has been previously reported, recent research by cyber security company PhishLabs highlights a common misconception amongst average internet users, that websites using SSL and HTTPS, as signified by the padlock, are safe and secure to use.

This is not necessarily the case and attackers have increasingly exploited this misunderstanding. In the third quarter of 2017, PhishLabs found that nearly a quarter of all phishing attacks observed were hosted on HTTPS domains.

To avoid becoming a victim of HTTPS phishing attacks, users and organisations should not rely on a padlock or link to an SSL certificate alone to verify the legitimacy of a website. Other methods include paying close attention to the URL spelling and comparing it to a known and trusted version, and looking at the email source code to find the real name of a website or its IP address.

The NCSC provides guidance to help companies and individuals know what to worry about when using HTTPS to protect data. You may visit: https://www.ncsc.gov.uk/guidance/tls-external-facing-services

EIOPA'S stress test identifies spill-over risks into the real economy from shocks to the European Occupational Pensions Sector.

- European Institutions for Occupational Retirement Provision (IORPs) providing defined benefits and hybrid pension schemes have, in aggregate, insufficient assets to cover their liabilities.

- Sponsors of over a quarter of IORPs might face challenges meeting their obligations.

- Vulnerabilities could spill-over to the real economy either through the adverse impact on sponsors and/or on beneficiaries through benefit reductions.

- Recovery mechanisms mitigate the short-term effects on financial stability, but in the longer-term put the burden of restoring the sustainability of pension promises disproportionately on younger generations.

The European Insurance and Occupational Pensions Authority (EIOPA) published the results of its 2017 Occupational Pensions Stress Test.

This year's exercise assessed the resilience of Institutions for Occupational Retirement Provision (IORPs) to a "double-hit" scenario, combining a drop in risk-free interest rates with a fall in the price of assets held by IORPs.

The exercise also assessed the potential transfer of shocks from IORPs to the real economy and financial stability through sponsor support and benefit reductions.

The stress test is not a pass-or-fail exercise for the participating IORPs. The stress test covered defined benefit (DB) and hybrid as well as defined contribution (DC) schemes.

Overall, 195 IORPs from twenty member states of the European Economic Area (EEA) participated in the exercise, representing a coverage rate of 39% of total assets.

EIOPA's target coverage rate of 50% was not reached in some Member States due to the lack of power of the respective national competent authority to require participation in the exercise.

Such inadequate supervisory powers constitute an additional risk because relevant authorities are not able to assess vulnerabilities during adverse market conditions.

The European DB and hybrid occupational pension sector has, on average, insufficient assets to meet pension liabilities on the national balance sheet, both in the baseline and adverse market scenario.

These vulnerabilities are even more pronounced on the common, market-consistent balance sheet, providing a more comparable and realistic view of the financial position of the IORPs.

The shortfalls on the common balance sheet - EUR 349 billion in the baseline and EUR 702 billion in the adverse scenario - would need to be covered by increased sponsor support and/or by benefit reductions.

The DC occupational pension sector would experience a drop of 15 % in the market value of investment assets in the adverse scenario, reducing the individual accounts of DC pension scheme members and, in case the scenario persists, leading to lower pension income when the members enter retirement.

More than a quarter of IORPs providing DB and hybrid schemes are covered by a sponsor that may not be able to (fully) support the pension promise following the adverse scenario.

In addition, the stress test results show that pension obligations may exert substantial pressure on the solvency and future profitability of companies with a potential spill-over to the real economy.
In particular, for 25% of participating IORPs the value of sponsor support on the common balance sheet exceeded 42% of the sponsors' market value under the pre-stress and 66% under the adverse scenario.
Benefit reductions have similar negative effects on the real economy by reducing household income and consumption, but also resulting in lack of trust in the pensions system.

National recovery mechanisms do allow sponsor support and benefit reductions to be spread over substantial timeframes.

IORPs in financial difficulties are usually subject to long-term recovery plans.

Moreover, high discount rates – relative to risk-free interest rates – provide an optimistic view of the funding situation of IORPs and act to delay recovery plan measures.

Such prudential mechanisms may contribute to mitigating the short-term spill-over effects to the real economy and financial stability.

However, in case the necessary adjustments are postponed too far, restoring the sustainability of IORPs can only be achieved by putting a disproportionate burden on the younger generations.

Gabriel Bernardino, Chairman of EIOPA, said: "The stress test results show that the risks stemming from shocks on the European IORPs sector could also spill-over into the real economy with negative implications on economic growth and employment triggered by increased sponsor support or benefit reductions.

To gain further insights and to deepen supervisory understanding EIOPA will conduct a horizontal assessment of potential systemic risk drivers such as search for yield, flight to quality or herding behaviour.

Environmental, social and governance (ESG) aspects including climate change will be of growing importance for the pensions sector and will require cautious assessment of any financial stability implications.

Younger generations should not suffer and carry a disproportionate burden because of today's complacency and lack of required actions."

The Report of the results of EIOPA's 2017 Occupational Pensions Stress Test is available via EIOPA's Website at:
https://eiopa.europa.eu/Pages/Financial-stability-and-crisis-prevention/Occupational-Pensions-Stress-Test-2017-.aspx

Progress report on supervisory colleges published by the Basel Committee

The Basel Committee on Banking Supervision has issued a Progress report on the implementation of principles for effective supervisory colleges. Supervisory colleges play an important part in the effective supervisory oversight of international banking groups.

The report concludes that the effectiveness of colleges has improved since 2015 in the areas of information-sharing, coordinated risk assessment and crisis preparedness. Yet challenges still remain, including those related to legal constraints on information-sharing, supervisory resource constraints and expectation gaps between home and host supervisors.

To overcome these challenges, the report sets out sound practices that include placing emphasis on the work between (or outside) formal college meetings, and encouraging home and host supervisors to reach out to each other to clarify expectations.

The Basel Committee's Principles for effective supervisory colleges were first published in 2010 and updated in 2014. The Committee monitors member jurisdictions' adoption of these principles, and identified three areas to improve the effectiveness of colleges as noted above in its July 2015 Progress report on the implementation of principles for effective supervisory colleges.

To read the report:
https://www.bis.org/bcbs/publ/d430.pdf

Fraudulent YouTube Video

CAYMAN ISLANDS
MONETARY AUTHORITY

The Cayman Islands Monetary Authority ("the Authority") has become aware of a YouTube video with the title "Cayman monetary authority awards grants to customers" published by a user named "Channel One News".

The video is purporting that the "EFG bank Cayman" has been mandated by the Cayman Islands Monetary Authority and "United Nations Fund Monitoring" to "accord customers" named in the video to receive a grant to be able to have the financial capacity to finalise their various transactions.

In addition, the video claims that an agreed percentage of the customers' delayed funds will be released to customers within a few days.

The video advises viewers (customers) to follow the process urgently which will help the effected customers to travel to Cayman next year January to meet with bank officials to process and claim the remaining funds.

The Authority wishes to advise the public that the above mentioned video was not published or authorised by the Caymans Islands Monetary Authority and it appears to be a scam.

Although the Authority regulates an entity called "EFG Bank", the regulated entity is not the fraudulent entity named in the video mentioned above.

Members of the public are advised not to follow the advice contained in the aforementioned video or communications received from individuals involved in this scam.

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

International Association of Potential, New and Sitting Members of the Board of Directors (IAMBD)

1. Membership - Become a standard, premium or lifetime member.

You may visit:
www.members-of-the-board-association.com/HowToBecomeMember.html

2. Monthly Updates - Subscribe to receive (at no cost) Basel II / Basel III related alerts, opportunities, updates and our monthly newsletter:

http://forms.aweber.com/form/77/609193677.htm

3. Training and Certification - Become a Certified Member of the Board of Directors (CMBD), Certified Member of the Risk Committee of the Board of Directors (CMRBD) or Certified Member of the Corporate Sustainability Committee of the Board of Directors (CMCSCBD).

You must follow the steps described at:
www.members-of-the-board-association.com/Distance_Learning_and_Certification.htm

www.basel-iii-association.com/Basel_III_Distance_Learning_Online_Certification.html

For instructor-led training, you may contact us. We can tailor all programs to your needs.