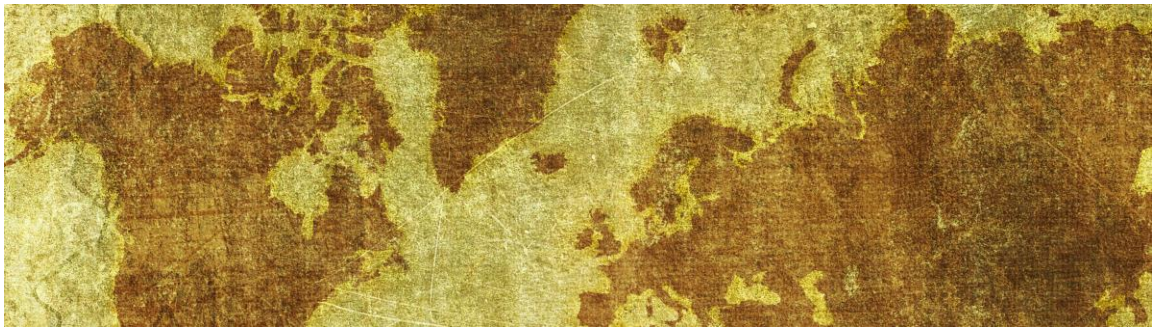
Solvency ii Association
1200 G Street NW Suite 800 Washington DC 20005-6705 USA
Tel: 202-449-9750 Web: www.solvency-ii-association.com



Solvency 2 News, January 2020

Dear members and friends,

The European Insurance and Occupational Pension Authority (EIOPA) has launched a consultation on guidelines on Information and Communication Technology (ICT) security and governance.

These guidelines shall provide guidance to national supervisory authorities and market participants on how regulation regarding operational risks set forth in Directive 2009/138/EC and in the Commission's Delegated Regulation 2015/35 and EIOPA Guidance set out in EIOPA's Guidelines on System of Governance is applied in the case of ICT security and governance. The consultation is open until Friday, 13 March 2020.

In line with its Joint ESA's Advice and in reply to the European Commission's FinTech Action Plan, EIOPA developed these guidelines addressed to national supervisory authorities with the following objectives:

- To create a common baseline for information security throughout the EU Member States

- To enhance convergence of supervisory practices in this area

In developing the Joint Advice, the ESAs' objective was that every relevant entity should be subject to clear and general requirements on governance of ICT, including cybersecurity, to ensure the safe provision of regulated services.

As these requirements are not in general 'sector-specific for the (re)insurance market, EIOPA also considered the most recent guidelines published by the European Banking Authority

EIOPA's Guidelines cover the following areas:

- Governance and risk management
- ICT operations security
- ICT operations management

For responding to this consultation you may visit:
https://ec.europa.eu/eusurvey/runner/ICT_GLs

The deadline for submission of feedback is Friday, 13 March 2020 at 23.59 hrs CET.

Unless requested otherwise, all contributions received will be published after the deadline for submission.

To read more:
https://eiopa.europa.eu/Publications/Consultations/guidelines_ICT_security_and_governance_12122019_for_consultation.pdf

EIOPA publishes annual report on the use of capital add-ons under Solvency II

The European Insurance and Occupational Pensions Authority (EIOPA) published today its annual report on the use of capital add-ons by national competent authorities (NCAs) under Solvency II.

The objective of the capital add-on measure is ensuring that the regulatory capital requirements reflect the risk profile of the undertaking or of the group.

Therefore, it is important that it is used by NCAs when needed and it is also important to ensure a high degree of supervisory convergence within the 31 European Economic Area (EEA) countries, including the EU Member States, regarding its use.

This analysis is based on 2018 year-end Solvency II data collected under Directive 2009/138/EC as reported by the undertakings and insurance groups complemented by a survey that entailed both qualitative and quantitative questions.

During 2018, eight NCAs set capital add-ons to 21 solo undertakings, out of 2819 (re)insurance undertakings under the Solvency II Directive in the EEA. These include 10 non-life undertakings, eight life undertakings, two reinsurers and one composite undertaking.

In 2017, six NCAs had set capital add-ons for a total of 23 solo undertakings. Hence, although the number of capital add-ons is extremely low and decreased slightly from 2017 to 2018, two more NCAs made use of this tool in 2018.

The amount of capital add-ons imposed on undertakings using the standard formula remains very low overall in 2018 accounting for 1% of the total Solvency Capital Requirement (SCR). However, the amount of capital add-on is not insignificant when considering the amount at individual level.

In sum, as of year-end 2018, the weight of the capital add-on increased to 32% (30% in 2017) when looking at the amount of capital add-ons as a percentage of the total SCR for those undertakings using the standard formula with capital add-ons.

The distribution of the capital add-ons as a percentage of the total SCR in 2018 for undertakings that imposed capital add-ons varies substantially once more.

In 2018, the largest percentage was 80% (83% in 2017), whereas the smallest percentage rounded close to 0% (1% in 2017). It should be noted that in all but five cases, if applied, the capital add-on increased the SCR by more than 10%.

The report:
https://eiopa.europa.eu/Publications/Reports/EIOPA_2018_Capital_add_ons_report_Final.pdf

Consultation on the proposal for Guidelines on information and communication technology (ICT) security and governance

End date: 13/03/2020, Status: Open

The objective of these Guidelines is to:

a) provide clarification and transparency to market participants on the minimum expected information and cyber security capabilities, i.e. security baseline;

b) avoid potential regulatory arbitrage;

c) foster supervisory convergence regarding the expectations and processes applicable in relation to ICT security and governance as a key to proper ICT and security risk management.

ICT and security risk	As a sub component of operational risk; the risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change ICT within a reasonable time and costs when the environment or business requirements change (i.e. agility). This includes cyber risks as well as information security risks resulting from inadequate or failed internal processes or external events including cyber attacks or inadequate physical security.

To read more:
https://eiopa.europa.eu/Publications/Consultations/guidelines_ICT_security_and_governance_12122019_for_consultation.pdf

Decision of the Board of Supervisors on the annual market and credit risk modelling comparative study

Article 1 - Scope

(1) Undertakings with a significant exposure to assets denominated in Euro and an approved internal model covering market and credit risk shall take part in the study.

The competent authorities, following consultation with EIOPA, may have discretion to determine whether an undertaking's Euro denominated assets represent a significant exposure.

Where several undertakings use a group internal model, only the group undertaking shall take part in the study.

In case the group does not take part, then individual undertakings could take part.

(2) The competent authorities, following consultation with EIOPA, may have discretion to determine the scope of the study by extending or limiting the scope of the default data request.

Article 2 – Features of the study

(1) In order to compare market and credit risk model outputs for a set of realistic asset portfolios, the comprehensive set of realistic asset portfolios shall reflect typical asset risk profiles of European insurance undertakings. The set shall be rich enough to construct specific asset portfolios, e.g. by country.

(2) The study shall explore the causes for the presumed variability of outcomes by analysing additional information such as individual risk charges, e.g. individual asset classes such as fixed income, equity, etc.

(3) The data request and modelling approach analysis shall provide valuable supporting tools to the competent authorities for the Supervisory Review Process (SRP) on internal models, inter alia for monitoring the development of models and their calibration over time and for assessing model changes.

Article 3 – Process

(1) The competent authorities shall inform undertakings which shall take part in the study. An undertaking which participates in the study shall provide the information described in the data request by the indicated deadline to the competent authority concerned.

(2) The competent authorities shall transmit the data received from undertakings to EIOPA. EIOPA shall make the data available for the EIOPA Project Group, which is responsible for the analysis. The storage and access to this data shall be subject to EIOPA's professional secrecy and confidentiality rules.

(3) The findings and conclusions shall be discussed and adopted by the Board of Supervisors by the end of the year. Individual feedback shall be provided to the participating undertakings by the competent authorities together with potential recommendations or follow-up actions.

To read more:
https://eiopa.europa.eu/Publications/Protocols/Decision%20on%20the%20Annual%20Market%20and%20Credit%20Risk%20Modelling%20Comparative%20Study.PDF

Stablecoins - a good or a bad solution to improve our payment systems?

Denis Beau, First Deputy Governor of the Bank of France, at the Stablecoin Conference "Which ambitions for Europe?", organized by Paris Europlace and ConsenSys, Paris, 15 January 2020.

Ladies and gentlemen,

The growing number and forms of crypto-assets in our payments landscape has triggered a significant and important debate about their virtues and risks, in case the role of these crypto-assets in our payment systems were to become less marginal than it currently is.

The emergence of so-called "stablecoins" has brought additional fuel to this debate as they could bring to the market new settlement assets and payment schemes, which may compete against and possibly, according to their promoters, replace those in commercial and central bank money, currently at the centre of the functioning of our payment systems.

In order to share with you a few thoughts on this debate, speaking as a central banker and a supervisor mindful of the benefits of innovation but also of the risks they could bring to financial and monetary stability, I will focus my remarks on two topics:

- Whether stablecoins can contribute to improving our payment landscape?

- How to respond to the public policy challenges they raise?

1 - Are stablecoins a brand new solution or a brand new problem?

From my perspective, they can be both. Let me explain.

Due to their specificities, stablecoins are a novelty in tune with some markets' needs.

In the context of the economy's digitalisation, the past decades have shown how Fintechs as well as Bigtechs have aimed at taking advantage of the latest advances in web-based technologies, notably blockchain, to provide new payment credit and investment services.

Often, they propose to achieve this through the creation of various new assets (coins, tokens, stablecoins, with or without smart contracts).

We all have in mind the first generation of crypto-assets such as Bitcoin and Ethereum, initially designed to be instruments of exchange in the digital world but suffering from a number of limitations, not least severe price volatility and a lack of guarantee of their convertibility and security.

A second generation is emerging in the form of « stablecoins », such as the JP Morgan Coin, UBS's Utility Settlement Coin or Facebook's Libra.

They share many of the features of crypto-assets but seek to stabilise the price of the "coin" by various means. They might therefore be more capable of contributing to the enhancement of payment systems, with a potentially global reach, especially those sponsored by large technology or financial firms.

In the retail market, stablecoin-based solutions seek to address evolving consumer preferences towards instantaneous, continuous, and standardized payments, as consumers become ever more mobile.

While this demand is largely already met through an increasingly diversified and digitalised supply by many payment services providers - be the new entrants or established players-, stablecoins could challenge the latter by offering cheaper, easier and instant anonymous and peer-to-peer payments.

In addition, at the global level, we are far from having a network (or set of interconnected networks) that could support quick and cheap transfers of funds.

The current supply of cashless means of payment lacks a universal and ergonomic cross-border solution akin to cash person-to-person payments. Stablecoins could be seen as a "universal" means of payment facilitating cross-borders payments in a single unit of account. As we know, this is an argument put forward by some global stablecoins promoters.

Furthermore, stablecoins could help remedy other limits of the existing payment ecosystem, even if the issues at stake might concretely vary between developed and developing countries.

In particular, their blockchain-based technology could help improve wholesale clearing and settlement mechanisms and facilitate Delivery-versus-Payment processes as well as cross currency settlements, while guaranteeing resilience and recovery from operational incidents.

However, stablecoins may also bring material risks to payment systems.

As many central bankers have pointed out, stablecoins do not satisfactorily offer the qualities expected from a settlement asset to be used interchangeably with commercial bank money and central bank money.

As intermediaries in exchanges, stablecoins are far less effective than a settlement asset with legal tender status, insofar as

(i) they are not entirely stable since their price stability depends on the value of a basket of assets, and

(ii) they offer no guarantee of a refund in the event of fraud.

The fact that they have no intrinsic value and that they offer no guarantee that they may be converted at par upon demand with commercial bank money or central bank money means that they cannot be used to create reliable stores of value.

In addition, as pointed out in the G7 report on stablecoins issued last year, stablecoin schemes are significantly exposed to risks of various nature, including legal, financial, operational and compliance risk concerning money laundering and terrorist financing, competition law, consumer and investor protection.

The risks identified must be seriously addressed if stablecoins are not to become the « weak links » undermining the safety of our payment systems.

This is all the more important as some of these risks would be amplified and new risks might arise if stablecoins are adopted at a global level.

Stablecoins of potentially large size and reach - so-called global stablecoins - may indeed pose additional challenges of system-wide importance both domestically and internationally, for the transmission of monetary policy, as well as for financial stability.

They could also have implications for the international monetary system more generally, including currency substitution, and could therefore pose challenges to monetary sovereignty.

2 - What role for regulatory and oversight authorities?

In this context, it is first and foremost the responsibility of the private sector to design stablecoin schemes that do not bring undue risks to our payment systems.

For that purpose, regulatory and oversight authorities have an important role to play in order to ensure that the risk management requirements to be met are clear, comprehensive and complied with, while preserving the potential for technological innovation offered by crypto-assets.

To that end, they should in my view focus on three main tasks:

- *Firstly, working on a regulatory response that preserves the positive potential impact stablecoins* might have on the efficiency of our payment systems.

Given the rapid pace of innovation, which is also characteristic of stablecoin initiatives, this pleads for developing an agile, pragmatic and proportionate regulatory response rather than setting up an ad-hoc, unique and comprehensive framework.

This would be simpler, faster to implement and to adjust, and be more likely to achieve level-playing field conditions.

In the European context, this is an encouragement for building on and adapting the functional coverage of existing regulatory frameworks and, in some cases extending their geographical coverage.

What comes to mind in particular is the framework for crypto-assets service providers created in France with the Pacte bill, and the European framework for e-money issuers, investment funds and financial market infrastructures.

This also calls for ensuring a consistent regulatory treatment of similar risks, irrespective of the framework or combination of frameworks under which stablecoins schemes might be operated.

- *Secondly, coordinating the adjustment of regulatory and supervisory frameworks at the international level.*

Whatever the final choice made for the European Union in terms of regulation strategy, such an adjustment of the regulatory framework should be part of broader adjustment at the global level, given the possible development of global stable coins.

Indeed, there is a need for overall consistency to prevent regulatory arbitrage under the "same activities, same risks, same rules" principle.

This is also necessary to address risks that fall outside existing frameworks, including risks to fair competition and monetary policy transmission.

Indeed, in July 2019, G7 Finance Ministers and Central Bank Governors agreed that possible stablecoins initiatives must meet the highest regulatory standards, be subject to prudent supervision and oversight and that possible regulatory gaps should, as a matter of priority, be assessed and addressed.

Accordingly, the Financial Stability Board is working on a global regulatory and supervisory approach towards stablecoins.

Developing shared public policy, regulatory and supervisory goals and principles should help capture activities that fall outside traditional regulatory boundaries.

It should also help prevent any discrepancies at domestic levels that may give rise to fragmentation and regulatory arbitrage which would be counterproductive for the development of these new instruments themselves.

These goals and principles should include common requirements vis-à-vis GSC operators before they start their operations, such as clear and proper risk management policies and means, regarding their stabilisation mechanisms, legal certainty of users' redemption rights and potential claims on underlying reserve assets, and regarding linkages and exposure between their core components and the other entities of the financial system.

In addition, there is a need to agree on adequate cross-border oversight principles and schemes between authorities in charge of jurisdictions impacted by the potential circulation of stablecoins.

To that end, we could take inspiration and review existing standards and principles for cross-border cooperation in the field of market infrastructures or AML-CFT.

- Thirdly, making concrete efforts - including live experimentations - to address weaknesses of the current payment and settlement landscape.

Adjusting the regulatory and oversight frameworks might not be enough as we have to make sure stablecoins do not become a bad solution to a real problem.

Our current financial system order rests on multiple issuers of settlement assets linked to the anchor settlement asset provided by central banks.

In order to preserve the incentives and benefits for innovation, efficiency and stability, central banks as issuers of the reference settlement asset need to revisit and possibly adapt the conditions under which they make that settlement asset available.

In that perspective, central banks could, for instance, issue their money in digital form, the so-called concept of Central Bank Digital Currency (CBDC).

This might be particularly appropriate for meeting settlement needs in central bank money between financial intermediairies.

Indeed, asset tokenization initiatives have proliferated among financial players, with the the risk that such developments may lead to disorderly approaches and heterogeneous adjustments of settlement processes, which are currently mainly handled through market infrastructures.

The Eurosystem, as a major provider of critical wholesale clearing and settlement services in euro, should therefore be open to experimenting the conditions under which it makes central bank money available as a settlement asset.

To that end, we, at the Banque de France, have started gaining experience with innovative solutions, including in particular recourse to DLT.

Experimentation is key in this area and this is why, as already announced by Governor Villeroy de Galhau, the Banque de France will launch a call for projects before the end of the first quarter of 2020.

Indeed, we wish to work with industry innovators and start running experiments rapidly to possibly integrate a "wholesale" CBDC into innovative procedures for exchanging and settling tokenised financial assets.

Another contribution from central banks could be to help address one of the major failings of the current payment systems which is cross-border retail payments.

This is one of the drivers of the development of crypto-assets such as stablecoins, and we believe we could help identify and support other concrete, useful and possibly complementary solutions.

In conclusion, let me stress 4 points:

- It is hard to anticipate the role that stablecoins and more generally crypto-assets might play in the payment system of the future, especially since the features of these assets look set to change considerably.

- While it is clear that they offer opportunities to improve our payment systems, they can also bring quite material risks which must be addressed. In that context, it is first and foremost the responsibility of private sector entities to design arrangements which do not bring undue risks to our payment systems.

- Regulatory and oversight authorities also have an important role to play in order to ensure that risk management requirements to be met are clear, comprehensive, coherent across-borders and complied with, while preserving the potential for technological innovation offered by stablecoins.

- Beyond contributing to the adjustment of the regulatory and oversight frameworks to address these risks, central banks may make further contributions, notably by revisiting and possibly adjusting the conditions under which they make central bank money available for settlement purposes.

  To that end, we should keep an open-minded approach and develop an in-depth understanding of innovations currently spreading across the financial sector, including through experimentations. This is critical for our capacity to help deliver a sound, proper and updated regulatory framework supporting innovation, and adequately mitigate their inherent risks. This is also critical for our capacity to adapt the performance of the different roles we play to fulfil our financial stability mandate and conduct efficient monetary policies.

Thank you for your attention.

Getting to the core of culture

John C Williams, President and Chief Executive Officer of the Federal Reserve Bank of New York, at "Working Together; An Interdisciplinary Approach to Organisational Culture", London School of Economics and Political Science, London.

Thank you for the warm introduction. It's an absolute pleasure to be back at the London School of Economics, where I completed my Master's degree in the late 1980s. Studying at the LSE, with remarkable professors like Richard Layard, Chris Pissarides, George Evans, and the late Tony Atkinson, inspired me to pursue a career in economics and public policy.

I owe a great debt of gratitude to this institution and am in awe of how it has evolved and grown in the past 30 years.

I will say that there are a few things I have not missed since my days in London: the food (yes, that has changed!), the high cost of living (some things never change), and the endless studying for and worrying about final exams. But I have missed the dear friends I made, the book shops, and the library.

It's ironic that I find myself back at the London School of Economics and NOT talking about economics. The views I bring to today's discussion come from professional and personal, rather than academic experience.

I've now led two major organizations, and culture is both the hardest and the most important thing to get right.

Culture is at the heart of behavior and norms, and the single most important factor driving the decision-making of employees. It's not an exaggeration to say that culture is critical-both when things go right, and when they go wrong.

Before I get any deeper into ideas about culture, I should give the standard Fed disclaimer that the views I express today are mine alone and do not necessarily reflect those of the Federal Open Market Committee or others in the Federal Reserve System.

Culture Shapes Our Working Lives

When we talk about company culture in the context of financial services, the first thing that comes to mind is the risky, unethical, and sometimes criminal behavior in the banking industry, particularly during the financial crisis.

And 10 years on from the crisis, this behavior persists. Instances of fraud, money laundering, and scandals related to foreign exchange and LIBOR continue to make the headlines.

This behavior puts a spotlight on the essential role of robust regulation and strict enforcement.

But illicit and unethical behavior is rarely the result of an isolated "bad apple." It's more often the symptom of a rotten culture. And rotten cultures don't appear overnight-nor for that matter do positive, inclusive ones, where people feel empowered and accountable to upholding the values of the organization.

Culture is created-intentionally or otherwise-by the structures, incentives, and behavioral norms that shape our working lives.

Today I want to move our attention away from the extreme behavior that makes the headlines, and think more deeply about organizational cultures.

What does a good culture look like? How can leaders in the industry establish a positive culture within their firms? And perhaps hardest of all, how do you ensure that a firm's culture adapts to the changing world, but still stays true to its values and purpose?

An Ethical Dilemma

Consider this:

A junior banker on a successful real estate investment team is asked to run projections for future rental income for a mall in Hong Kong. As part of her research she notices a number in a spreadsheet that inflates future cash flows by 4 percent.

She asks a senior analyst if the number should be flagged as an optimistic assumption, so it's clear it's not based on evidence. The senior analyst responds by saying the number is a more conservative estimate than many. He says it's a "judgment call" and that they can discuss it once the project has concluded.

But the project comes and goes, everyone is busy, and the senior analyst doesn't bring it up again.

This scenario raises numerous questions: Should the junior team member raise the issue again or should she let it go? What was driving the behavior of the senior analyst? And why did no one else on the team view the situation as an ethical dilemma?

These are the kinds of issues that people often face in a work environment. And this example demonstrates many of the ways culture influences behavior.

Employees may enter an organization with a strong sense of right and wrong. What they may not realize is that group norms can exert a powerful magnetic pull on their moral compass.

The junior banker knew the way the number was being presented was unethical, and yet she complied with her boss. The response from the senior analyst, describing the situation as a "judgment call," is a common phenomenon. Using a euphemism to describe the inflated statistic camouflages the wrongdoing and makes it sound more acceptable to others.

We see it in our daily lives-terms like "troublemaker" and "not being a team player" are often used to shift the onus from the person whose behavior is being challenged to the challenger.

Ann Tenbrunsel's work has been very important for revealing how we use language to disguise or excuse behavior we know to be unacceptable.

One of the other issues this example illustrates is how organizational norms affect our own sense of what's right and wrong and whether to speak up.

Many of you here today will be familiar with the Asch experiment, where students participated in a vision test. There was a control line and three other lines labelled A, B, and C. Participants had to state aloud which line was the same length as the control. But they had to do so after a group of actors had given an incorrect answer.

About one third of participants went along with the majority, even though it was readily apparent their answers were incorrect. When asked why they went along with the group they said it was because they wanted to fit in, or because they believed the group was better informed than they were.

Does the junior banker drop the issue in an effort to fit in? Does she raise the issue in private, or does she call a company hotline? The answer depends on the complex relationship between the individual and the culture in which they work.

I'm particularly looking forward to hearing from Celia Moore. She spoke at the New York Fed last year and discussed how organizations set goals and motivate people to achieve them.

Praise, penalties, and rewards all influence an individual's behavior. Signals from the organization's leadership also have a major role to play: do the higher echelons of management value divergent views? Do they foster a culture where people feel empowered to speak up?

All of these things shape how an individual will respond to an ethical dilemma, whether they will acknowledge it as such, and how they will lead others as they move up in an organization.

As financial services professionals with great technical expertise, we often fall into the trap of thinking we can solve all of our problems on our own. But we have so much to learn from experts in other fields.

Strengths as Blind Spots

One of the most important lessons I've learned as a CEO is that there's no fixed endpoint when it comes to shaping an organization's culture. You can never take a step back and say, "We've finished the culture project. Well done! Now it's time to focus our efforts elsewhere."

Culture is constantly evolving, and therefore needs to be constantly nurtured. One of the most challenging elements is that there's no clear benchmark for success. And sometimes your greatest strengths can become your blind spots.

As an organization with a public mission and regulatory responsibilities, the Fed needs to have a particular focus on compliance. But cultures with a heavy focus on compliance can breed a sense that individuals aren't responsible for their actions.

As a CEO, I've tackled these issues by focusing on principles and values rather than writing extensive policies that try to cover every potential decision. This puts a premium on individual accountability to do what's right and creating an environment where everyone has the ability and responsibility to speak up.

Somewhat paradoxically, focusing on principled decision making and accountability, rather than relying exclusively on rules and policies, can be the most effective safeguard against wrongdoing and unethical behavior.

What's the Way Forward?

Creating a positive work culture is challenging and ongoing work. And there's no silver bullet that can solve cultural problems overnight.

In terms of how to move forward I'd like to make three brief points before I close:

First, the fact that we're all sitting here in this room is a very positive sign. That so many leaders from major firms are here today, engaged in these issues, is a symbol of how organizational culture is moving up the agenda.

The second is that the Banking Standards Board survey is a terrific tool for getting a snapshot of what your organization's culture looks like and how it's changing over time.

It goes far beyond typical engagement questionnaires and provides powerful insights into the values of employees and the characteristics of an organization. It's impossible to make progress if you don't have an accurate picture of your starting point.

The third is that when it comes to culture, I encourage everyone to look beyond their own lens of expertise. The Fed couldn't do its work without the deep knowledge of economists, lawyers, and statisticians. But the solutions to challenges related to a firm's culture are unlikely to be found if we keep our focus narrowly trained on our own specialties. We have so much to learn from experts in psychology, ethics, and management.

That's one reason I've been so looking forward to today's panel discussion. It brings together experts from many of these fields, whose combined insights are the key to moving us all toward the business culture we want to see.

State of Vulnerabilities 2018/2019

The vulnerability ecosystem has matured considerably in the last few years. A significant amount of effort has been invested to systematically capture, curate, taxonomize and communicate the vulnerabilities in terms of severity, impact and complexity of the associated exploit or attack.

Standardisation in the description of vulnerabilities contributes not only to effective threat intelligence sharing, but also potentially efficient threat management, provided that organisations, vendors and security researchers actively seek to discover the vulnerabilities and respond in a timely fashion.

As the standardisation of cataloguing and modelling the vulnerabilities reaches the aforementioned maturity, public or private (i.e. commercial) databases containing information of the actual vulnerabilities (and some with their exploits counterparts) have emerged.

As there are a number of initiatives within the research community, quite naturally some databases could be considered to be more “authoritative” and/or “reliable” than others.

However, due to the nature of the vulnerability ecosystem, it is not a reasonable assumption that the databases will be complete (that is, contain all vulnerabilities), or reliable in the sense that the information captured is correct, in the sense that the samples gathered can be considered to reliably help in drawing conclusions on the whole population.

This is influenced by a number of factors, including the quality of analysis and assessment, the assessment framework itself, the economic aspects (such as the value of any available exploit), as well as the business models of the software vendors, threat intelligence services, and the overall security community.

The purpose of this report is to provide an insight on both the opportunities and limitations the vulnerability ecosystem offers. By using the vulnerabilities published during the year of 2018 and Q1-Q2 of 2019 as a vehicle, this report goes beyond the standard exploratory analysis, which is well captured by many industry whitepapers and reports, and attempts to answer questions related to the reliability, accuracy of the vulnerability sources and the widely accepted evaluation metrics.

The report: https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities/

A framework for all seasons?

Mark Carney, Governor of the Bank of England, at the Bank of England Research Workshop on "The Future of Inflation Targeting", London, 9 January 2020.

Introduction

Following a chequered history of high and volatile inflation in the post-war era, the UK finally found monetary success as an early adopter of inflation targeting in 1992.

The UK's current regime, launched in 1997, delegated operational independence for setting monetary policy to the Bank of England and included many institutional innovations that have stood the test of time – most notably a Monetary Policy Committee with a mix of internal and external members; transparent, independent voting; and a clear accountability framework.

Since operational independence for inflation targeting was delegated to the MPC, there have been a raft of improvements, both large and small.

Transparency has steadily increased with initiatives ranging from publishing detailed assumptions underlying forecasts ex ante to assessing forecast accuracy ex post as well as the simultaneous release of Monetary Policy Summaries, Minutes, and Inflation Reports.

More recently, the MPC has introduced layered communications, with simpler, more accessible language and graphics to reach the broadest possible audience, and we have launched the Monetary Policy Report in order to give greater prominence to the most pressing issues shaping each monetary policy decision.

A major improvement to the inflation targeting framework itself was to confirm explicitly beginning with the 2013 remit that the MPC is required to have regard to trade-offs between keeping inflation at the target and avoiding undesirably volatility in output.

In other words, the MPC can use the full flexibility of inflation targeting in the face of exceptionally large shocks to return inflation to target in a

manner that provides as much support as possible to employment and growth or, if necessary, promotes financial stability.

Even more fundamentally, the lessons of the global financial crisis prompted a radical overhaul of the Bank's broader policy framework.

The crisis exposed the limits of inflation targeting itself, notably how a healthy focus on price stability could become a dangerous distraction.

Central banks had won the war against inflation only to lose the peace as financial vulnerabilities built remorselessly during the Great Moderation. Price stability clearly is not a guarantee of financial stability.

With the deficiencies of the Tripartite regime1 on full and painful display, the decision was taken in 2012 to give the Bank of England responsibility for macroprudential and microprudential supervision.

Two new independent committees, the FPC and the PRC, were created and charged with maintaining financial stability and safety and soundness of banks and insurers, respectively.

In 2016, these committees were placed on equal footing with the MPC, underscoring the symbiotic roles that all three play in underpinning confidence in money and in promoting the best possible macro-economic outcomes.

Any consideration of the UK's monetary policy framework must take into account this unique and highly effective institutional structure. To set the stage for today's discussions, I would like to do two things.

First, I will review the conduct and performance of inflation targeting during my time as Governor.

This period, which roughly coincides with the post-crisis recovery and which has seen more than its share of shocks and structural developments, provides some insights to the ability of inflation targeting to deliver price stability and support macroeconomic outcomes.

I will suggest that, so far at least, inflation targeting has proven to be a framework for all seasons, an essential part of a robust foundation for economic prosperity.

It is important not to lose sight of the fundamental success in achieving price stability that has resulted from delegation of inflation targeting to an independent central bank.

In the two decades prior to independence, inflation averaged over 6%. Since independence, it has been close to 2% and one-fifth as volatile. Inflation expectations have remained well anchored throughout some of the largest economic shocks in postwar history

To read more:
https://www.bis.org/review/r200109b.pdf

European Commission publishes EU Cybersecurity Taxonomy

On 12 September 2018, the Commission has proposed a Regulation setting up a European Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres (COM/2018/630).

The overall mission of the Competence Centre and the Network (CCCN) is to help the Union retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market.

This goes hand-in-hand with the key objective to increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other European industries.

One of the first steps during the Impact Assessment of the Proposed Regulation was to provide a clear definition of the cybersecurity context, its domains of application, research and knowledge.

In this context, the first version of the proposed taxonomy was published with the goal of aligning the cybersecurity terminologies, definitions and domains.

The taxonomy was then used for the categorisation and mapping of existing EU cybersecurity centres (e.g. research organisations, laboratories, associations, academic institutions, groups, operational centres, etc.) according to their cybersecurity expertise in specific domains.

Based on this first analysis, a survey was also conducted where more than 600 institutions participated and registered their cybersecurity expertise.

In order to assess essential aspects of the CCCN regulation proposal, the Commission launched a pilot phase under Horizon 2020. In particular, the proposals CONCORDIA, ECHO, SPARTA and CyberSec Europe were selected as the four pilot projects to assist the EU in the establishment of a European Cybersecurity Competence Network of cybersecurity centres of excellence. The pilots bring together more than 160 partners, including big companies, SMEs, universities and cybersecurity research institutes, from 26 EU Member States.

The four pilot projects were asked to review the proposed taxonomy and provided feedback, which was used to improve the first version of the taxonomy in order to publish this second enhanced version.

For the purpose of this document, cybersecurity is considered an interdisciplinary domain. This starting point finds support in the Cybersecurity Report issued by the High Level Advisory Group of the EC Scientific Advice Mechanism in March 2017, where it is stated clearly that:

"cybersecurity is not a clearly demarcated field of academic study that lends itself readily to scientific investigation. Rather, cybersecurity combines a multiplicity of disciplines from the technical to behavioural and cultural. Scientific study is further complicated by the rapidly evolving nature of threats, the difficulty to undertake controlled experiments and the pace of technical change and innovation. In short, cybersecurity is much more than a science".

To read more:
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

Designing a prudential treatment for crypto-assets

BIS

The past few years have seen rapid growth in crypto-assets. The estimated market capitalisation of cryptoassets reached a historical peak exceeding $800 billion in January 2018.

While the crypto-asset market remains small relative to the size of the global financial system, and banks' exposures to crypto-assets are currently limited, its absolute size is meaningful and there continues to be rapid developments, with increased attention from a broad range of stakeholders.

As previously indicated, the Committee is of the view that the growth of crypto-assets and related services has the potential to raise financial stability concerns and increase risks faced by banks.

Cryptoassets are an immature asset class given the lack of standardisation and constant evolution. Certain cryptoassets have exhibited a high degree of volatility, and present risks for banks, including liquidity risk; credit risk; market risk; operational risk (including fraud and cyber risks); money laundering and terrorist financing risk; and legal and reputation risks.

While certain types of crypto-assets are at times referred to as "crypto-currencies", the Committee is of the view that such assets do not reliably provide the standard functions of money and can be unsafe to rely on as a medium of exchange or store of value.

These types of crypto-assets are not legal tender, and are not backed by any government or public authority. Therefore, if banks are authorised, and decide, to acquire crypto-assets or provide related services, the Committee is of the view that banks should apply a conservative prudential treatment to such exposures, especially for high-risk crypto-assets.

To that end, the Committee is publishing this discussion paper to seek the views of stakeholders on a range of issues related to the prudential regulatory treatment of crypto-assets, including:

(i) the features and risk characteristics of crypto-assets that should inform the design of a prudential treatment for banks' crypto-asset exposures; and

(ii) general principles and considerations to guide the design of a prudential treatment of banks' exposures to crypto-assets, including an illustrative example of potential capital and liquidity requirements for exposures to high-risk crypto-assets.

There have been recent initiatives related to some types of crypto-assets. For example, some initiatives seek to reduce the volatility exhibited to date by anchoring crypto-assets to a reference asset.

Other initiatives include redemption or repurchase assurances by a legal entity. These crypto-assets are sometimes referred to as 'stablecoins', although the stability of such assets has yet to be tested completely.

The scope of stablecoin initiatives vary, with some focusing on intragroup or interbank payment systems, while others seek to target a broader audience, including consumers globally.

While many of these types of crypto-assets have yet to become operational in practice, some may have the potential to become systemically important.

The Committee is of the view that these types of crypto-assets warrant further assessment and elaboration before specifying a prudential treatment.

A separate initiative relates to central bank digital currencies, where many central banks are continuing to look at the implications of this potential type of central bank money.

Such forms of digital currencies are outside the scope of this discussion paper. The responses to this paper will inform the Committee's development of a prudential treatment for crypto-assets at large, including for crypto-assets that are issued by regulated financial institutions, or that make use of stabilisation tools.

The Committee is continuing to assess the appropriate prudential treatment for such types of crypto-assets, and will consult on any specific measures.

To read more: https://www.bis.org/bcbs/publ/d490.pdf

US regulations and approaches to cryptocurrencies

Michael Held, Executive Vice President of the Legal Group of the Federal Reserve Bank of New York, at the BIS Central Bank Legal Experts' Meeting, Basel.

Thank you, Diego, for "volunteering" me to speak about digital currencies — a field in which I count myself as very much a trainee, not an expert. Today I will focus on the U.S. regulatory landscape for digital currencies, in particular on digital currencies issued by private organizations that are intended to be used like money.

As always, the views I express are my own, not necessarily those of the Federal Reserve Bank of New York or the Federal Reserve System.

Policy makers and regulators in the United States, to date, have not developed an overarching framework for regulating private digital currencies.

The field has been seen as too new for a comprehensive regulatory response. To be sure, the digital nature of new private currencies will raise challenges to which policy makers must respond.

In my view, however, we spend so much time wrestling with the novelty of digital currencies that we forget that private currency is nothing new.

The theme of my talk today is accordingly best encapsulated by a quote that is attributed—perhaps wrongly—to Mark Twain: "History may not repeat itself, but it does rhyme."

The Past Is Not Dead. It Isn't Even Past

So, let's take a little walk through the history of privately-issued currency. We begin in Michigan in 1837, when the state legislature passed the first "free" banking law in the United States.

Upon commencing business, free banks could issue banknotes—that is, private currencies—that were redeemable in specie—gold or silver. These banknotes were transferable debt backed by the general creditworthiness of the bank that issued them, plus assets like bonds and mortgages on real estate, and for a brief time, personal guarantees.

The statute permitted bank organizers to establish a bank by filing an application with the local county treasurer and county clerk. They did not need approval from the state banking commissioner. (At the time, the United States had no federal banking supervisor. Indeed, the "free banking" era generally begins with Congress's failure to recommission the Second Bank of the United States before its charter expired in 1836, and ends with the passage of the National Bank Act in 1863).

The result, predictably, was chaotic. The state banking commissioner was unsure of how many banks had even been established.

Some banks in Michigan were established with the intent to issue banknotes but without the intent to ever redeem them.

By 1839 almost the entire system had collapsed. After closing down one bank in Michigan, the commissioner found shards of window glass, lead, and nails where he should have found gold and silver coin.

Some of these free banks became known as "wildcat" banks. They set up offices in remote areas—where only the wildcats roamed—making it difficult to redeem notes for specie.

To read more: https://www.bis.org/review/r191212d.pdf

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.

Solvency II Association

At every stage of your career, our association provides networking, training, certification, information, updates, alerts, and services you can use. Join us. Stay current. Take advantage of the new opportunities. Read our monthly newsletter. Get certified.

You can explore what we offer to our members:

1. Membership – Become a standard, premium or lifetime member. You may visit: https://www.solvency-ii-association.com/How_to_become_member.htm

2. Monthly Updates – Visit the Reading Room of the association at: https://www.solvency-ii-association.com/Reading_Room.htm

3. Training and Certification – You may visit: https://www.solvency-ii-association.com/CSiiP_Distance_Learning_Online_Certification_Program.htm

For instructor-led training, you may contact us. We tailor Solvency II presentations, awareness and training programs for supervisors, boards of directors, employees, service providers and consultants.

4. Solvency II Association Authorized Certified Trainer (SOLV2A-ACT), Certified Solvency ii Professional Trainer (CSiiProT) program – You may visit: https://www.solvency-ii-association.com/SOLV2A_ACT.html