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.iambd.org

News for the Board of Directors, June 2020

Dear members and friends,

Financial policymakers and international standard setters have met virtually with private sector executives to discuss international policy responses to COVID-19.

Organised by the FSB's Standing Committee on Supervisory and Regulatory Cooperation (SRC), in cooperation with Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the International Association of Insurance Supervisors (IAIS) and the International Organization of Securities Commissions (IOSCO), the meeting brought together senior representatives from central banks, regulatory authorities and finance ministries as well as about 30 international banks, insurance firms, asset managers, market infrastructures and credit rating agencies.

The meeting was chaired by Himino Ryozo, Chair of the SRC and Vice Minister for International Affairs, Japan Financial Services Agency.

The meeting explored the effectiveness of prudential and other financial policy measures taken to date, including experiences with their implementation.

Participants also discussed policy issues going forward, notably how financial institutions can better cope with the challenges resulting from rising solvency risks, and exchanged views on potential areas that may warrant further policy coordination.

After the call, Himino Ryozo said: "The global financial system entered the crisis with much enhanced resilience and, with central bank intervention, the liquidity stress in March was largely contained. But the world still faces an unprecedented level of uncertainties.

Participants discussed issues which may arise in different phases of the crisis under a range of scenarios. Insights gained today will help the private

and official sectors act to ensure financing to the economy, financial stability, and eventually, a strong recovery."

The discussion at the meeting will help inform ongoing work in the FSB, BCBS, CPMI, IAIS, and IOSCO, and serve as input into the FSB's report on COVID-19 policy responses to the July G20 meeting.

Introductory remarks by the Himino Ryozo, Chair, FSB Standing Committee on Supervisory and Regulatory Cooperation

Thank you everyone for joining this conversation.

Facing the COVID-19 pandemic, the financial sector needs to meet three challenges: supporting the economy, sustaining itself, and preparing for the recovery.

The official sector has strived to assist the private sector's efforts to meet these challenges.

National authorities have taken agile actions: there are already 1,600 policy actions registered in the FSB database.

Standard-setting bodies issued a series of guidance to extend the implementation timelines and to encourage the use of flexibility.

Individual jurisdictions tailored their responses to their own conditions but have coordinated with each other with the following five principles in mind:

• First, we monitor and share information to address risks;

• Second, we use the flexibility built into existing financial standards;

• Third, we seek opportunities to temporarily reduce operational burdens on firms and authorities;

• Fourth, we act consistently with international standards, and will not roll back reforms; and

• Fifth, we will coordinate on the future timely unwinding of the temporary measures taken.

And these principles were endorsed by the G20 Finance Ministers and Central Bank Governors in April.

The global financial system has entered the crisis with much enhanced resilience, as a result of your efforts and the G20 regulatory reforms.

We have to admit that the shock in March was beyond the self-healing ability of the market: massive central bank actions were required to end the heightened volatility.

But the banking sector has continued to finance the real economy and, in late March, capital markets started to resume their normal functions.

Financial market infrastructures, including CCPs, have functioned well, despite the challenging external conditions, both financial and operational.

But we cannot be complacent. The world still faces an unprecedented level of uncertainty. We need to be prepared for a wide range of scenarios.

What I would like to discuss today is how we should act at different phases of the crisis under a range of scenarios.

Looking back, what lessons can we draw from the policy measures already taken?

What measures seem to be working well and what are not?

Have we observed operational frictions or obstacles, trade-offs and potential unintended effects?

How can we enhance the effectiveness of the measures taken?

And looking forward, what kind of possible developments should we be attentive to?

Which risks are you particularly worried about?

Liquidity, solvency or operational risks?

Under a range of scenarios, how can the official sector ensure financing to the economy, financial stability, and eventually, a strong recovery?

How should we take into account intertemporal trade-offs and macroprudential effects arising from the feedback loop between the various segments of the financial system and the real economy?

What roles should stress tests play?

The official sector side is represented today by central banks, regulatory authorities, finance ministries, the Basel Committee on Banking

Supervision, the Committee on Payments and Market Infrastructures, the International Association of Insurance Supervisors and the International Organization of Securities Commissions.

We are keen to hear your inputs to better discharge our policy work so that the efforts by the private and official sectors will work together well to help overcome the pandemic and ensure strong recovery.

I look forward to a rich discussion today.

Audits Involving Cryptoassets
Information for Auditors and Audit Committees

PCAOB
Public Company Accounting Oversight Board

One of the PCAOB's strategic objectives is to monitor the development and implementation of emerging technologies to analyze their implications for the quality of audit services.

PCAOB staff has observed that cryptoassets have recently begun to be recorded and disclosed in issuers' financial statements.

In addition, when performing inspections of auditors of some smaller issuers, PCAOB staff has observed situations where transactions involving cryptoassets were material to the financial statements.

Observations from these inspections indicate the need for a greater focus by some auditors on the identification and assessment of the risks of material misstatement to the financial statements related to cryptoassets, as well as the planning and performing of an appropriate audit response.

This document highlights considerations for addressing certain responsibilities under PCAOB standards for auditors of issuers transacting in or holding cryptoassets.

We also suggest questions that audit committees may consider asking their auditors when transactions involving cryptoassets or holdings of cryptoassets are material to the issuer's financial statements.

The information in this Spotlight may be of particular interest to the auditors and audit committee members of issuers that are beginning to transact in, or hold cryptoassets.

This Spotlight does not specifically address any other applications of blockchain, distributed ledger, or other technology.

As of the date of this publication, many types of cryptoassets (including Bitcoin, the largest by market value) have been created and are being traded.

An issuer's involvement with cryptoassets can be multifaceted. Transactions involving cryptoassets may include, for example, earning a fee, or "reward," for validating new blocks on a blockchain (which for some cryptoassets, such as Bitcoin, is commonly known as "mining"), purchasing goods or services in exchange for cryptoassets, exchanging one cryptoasset

for another, or selling cryptoassets for a fiat currency, such as the US dollar.

Transactions involving cryptoassets may also include, for example, providing trading services to third parties or acting as an intermediary, such as between a customer and a trading platform or mining operation.

Information for Audit Committees

Questions Audit Committees Could Consider Asking their Auditors

The following sample questions are designed to provide audit committees of issuers that are new to transacting in, or holding cryptoassets, or audit committee members who are new to cryptoassets, with ideas of the types of questions they may consider—at their discretion—asking their auditors.

- ✓ What is the experience of the engagement partner and other senior engagement team members with cryptoassets? Would the firm be able to supplement the engagement team's expertise if necessary (e.g., by engaging relevant specialists)?
- ✓ What is the auditor's understanding of the technology underlying the issuer's cryptoasset-related activities?
- ✓ Are specialized technology-based audit tools needed to identify, assess, and respond to risks of material misstatement?
- ✓ What is the auditor's understanding of the legal and regulatory (including KYC and AML) implications of the issuer's cryptoasset-related activities?
- ✓ How does the audit firm monitor auditor independence considerations associated with audit engagements involving cryptoassets (e.g., monitoring whether its staff invests in cryptoassets)?
- ✓ What policies and procedures does the audit firm have regarding conducting and monitoring audit engagements involving cryptoassets, including considering the risks associated with performing such audits?

To read more: https://pcaobus.org/Documents/Audits-Involving-Cryptoassets-Spotlight.pdf

European insurers face increased risk exposures due to Covid-19, but market perceptions and imbalances remained at medium level

The European Insurance and Occupational Pensions Authority (EIOPA) published its updated Risk Dashboard based on the fourth quarter 2019 Solvency II data.

Despite the fact that some indicators used in this Risk Dashboard do not capture the latest market development in the context of Covid-19 outbreak, the expected deterioration of the relevant indicators reflecting all available information in a forward looking perspective has been considered in the assigned risk levels. This addresses the current situation of high uncertainty in the insurance market.

The results show that the risk exposures of the European Union insurance sector increased as the outbreak of Covid-19 strongly affected the lives of all European citizens with disruptions in all financial sectors and economic activities.

Macro and market risks indicators deteriorated in March 2020, moving from high to very high level.

The macroeconomic environment has been affected strongly by the global lockdown.

GDP estimate points to a strong downturn for the first quarter 2020 and latest forecasts predict a recession worldwide for 2020.

Inflation forecasts have been revised downwards for the next four quarters.

Monetary policy support has been activated by all major central banks.

Financial markets have been characterized by sell-off across asset classes, increased volatilities for bond and equity markets, increasing risk premia and flight to quality investment behaviour in March 2020.

Credit risk has increased across all asset classes, in particular CDS of government bonds, financial and non-financial corporate bonds have increased sharply.

Liquidity and funding risks have been raised to high level due to potential additional strains on the disposable liquidity of insurers in the medium to long-term horizon.

For Q4-2019 liquidity indicators were broadly stable, however some are expected to worsen, triggered by possible decrease in premiums and new business, potential increase in claims and illiquid level of certain assets. Profitability and solvency risks have increased to high level.

Although for Q4-2019 insurers solvency positions remained relatively stable, looking ahead profitability and solvency risks are expected to deteriorate, given the double-hit scenario negatively affecting insurers on both asset and liability side. Insurance risks also raised to high level.

While broadly stable in Q4-2019, negative effects via income reduction and increase in claims are expected going forward.

Market perceptions remain at medium level albeit deteriorating. The EU insurance sector underperformed the market, both life and non-life businesses lines, and the median price-to-earnings ratio of insurance groups in the sample decreased since the last assessment.

Insurers' external ratings and rating outlooks do not show sign of deterioration as of end March 2020, however credit quality is expected to deteriorate.

Risks	Level	Trend
1. Macro risks	Very High	↑
2. Credit risks	High	↑
3. Market risks	Very high	↑
4. Liquidity and funding risks	High	↗
5. Profitability and solvency	High	↗
6. Interlinkages and imbalances	Medium	→
7. Insurance (underwriting) risks	High	↗
8. Market perceptions	Medium	↗

Background

This Risk Dashboard based on Solvency II data summarises the main risks and vulnerabilities in the European Union insurance sector through a set of risk indicators of the fourth quarter of 2019 complemented with market data and other available information.

This data is based on financial stability and prudential reporting collected from 96 insurance groups and 2837 solo insurance undertakings.

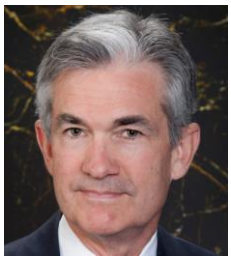
To read more:
https://www.eiopa.europa.eu/risk-dashboard

https://www.eiopa.europa.eu/sites/default/files/financial_stability/risk_dashboard/eiopa-bos-20-274-april-2020-risk-dashboard.pdf

Macro risks[2]	
	Level: very high
	Trend: increase
Macro risks increased from high to very high given the global impact of the outbreak of COVID on economic activities. GDP growth forecasts have been revised significantly downwards for all geographical areas, while inflation is expected to decrease slightly. The indicator on the 10 year swap rates decreased reaching new lows, after a flattening of all swap curves on the long end. Unemployment rate is expected to increase, due to steep fall of business activities fiscal balances are expected to deteriorate as government announced their interventions to sustain the halted economies. Monetary support has been activated by all major central banks.	

Coronavirus and CARES Act

Testimony by Mr Jerome H Powell, Chair of the Board of Governors of the Federal Reserve System, before the Committee on Banking, Housing, and Urban Affairs, US Senate, Washington DC.



Chairman Crapo, Ranking Member Brown, and other members of the Committee, thank you for the opportunity to discuss the extraordinary steps the Federal Reserve has taken to address the challenges we are facing.

I would like to begin by acknowledging the tragic loss and tremendous hardship that people are experiencing both here in the United States and around the world.

The coronavirus outbreak is, first and foremost, a public health crisis, with the most important responses coming from those on the front lines in hospitals, emergency services, and care facilities.

On behalf of the Federal Reserve, let me express our sincere gratitude to those individuals who put themselves at risk day after day in service to others and to our nation.

The forceful measures that we, as a country, are taking to control the spread of the virus have substantially limited many kinds of economic activity. Many businesses remain closed, people have been advised to stay home, and basic social interactions have been greatly curtailed.

People have put their lives and livelihoods on hold at significant economic and personal cost. All of us are affected, but the burdens are falling most heavily on those least able to carry them.

It is worth remembering that the measures taken to contain the virus represent an investment in our individual and collective health. As a society, we should do everything we can to provide relief to those who are suffering for the public good.

Available economic data for the current quarter show a sharp drop in output and an equally sharp rise in unemployment.

By these measures and many others, the scope and speed of this downturn are without modern precedent and are significantly worse than any recession since World War II.

Since the pandemic arrived in force just two months ago, more than 20 million people have lost their jobs, reversing nearly 10 years of job gains. This precipitous drop in economic activity has caused a level of pain that is hard to capture in words, as lives are upended amid great uncertainty about the future.

In addition to the economic disruptions, the virus has created tremendous strains in some essential financial markets and impaired the flow of credit in the economy.

The Federal Reserve's response to this extraordinary period has been guided by our mandate to promote maximum employment and stable prices for the American people, along with our responsibilities to promote stability of the financial system.

We are committed to using our full range of tools to support the economy in this challenging time even as we recognize that these actions are only a part of a broader public-sector response.

Congress's passage of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was critical in enabling the Federal Reserve and the Treasury Department to establish many of the lending programs that I discuss below.

In discussing the actions we have taken, I will begin with monetary policy.

In March, we lowered our policy interest rate to near zero, and we expect to maintain interest rates at this level until we are confident that the economy has weathered recent events and is on track to achieve our maximum - employment and price-stability goals.

In addition to monetary policy, we took forceful measures in four areas: open market operations to restore market functioning; actions to improve liquidity conditions in short-term funding markets; programs in coordination with the Treasury Department to facilitate more directly the flow of credit to households, businesses, and state and local governments; and measures to allow and encourage banks to use their substantial capital and liquidity levels built up over the past decade to support the economy during this difficult time.

Let me now turn to our open market operations and the circumstances that necessitated them.

As tensions and uncertainty rose in mid-March, investors moved rapidly toward cash and shorter-term government securities, and the markets for Treasury securities and agency mortgage-backed securities, or MBS, started to experience strains.

These markets are critical to the overall functioning of the financial system and to the transmission of monetary policy to the broader economy.

In response, the Federal Open Market Committee undertook purchases of Treasury securities and agency MBS in the amounts needed to support smooth market functioning. With these purchases, market conditions improved substantially, and thus we have slowed our pace of purchases.

While the primary purpose of these open market operations is to preserve smooth market functioning and effective policy transmission, the purchases will also foster more accommodative financial conditions.

As a more adverse outlook for the economy associated with COVID-19 took hold, investors exhibited greater risk aversion and pulled away from longer-term and riskier assets as well as from some money market mutual funds.

To help stabilize short-term funding markets, we lengthened the term and lowered the rate on discount window loans to depository institutions.

The Board also established, with the approval of the Treasury Department, the Primary Dealer Credit Facility (PDCF) under our emergency lending authority in section 13(3) of the Federal Reserve Act. Under the PDCF, the Federal Reserve provides loans against good collateral to primary dealers that are critical intermediaries in short-term funding markets.

Similar to the largescale purchases of Treasury securities and agency MBS I mentioned earlier, this facility helps restore normal market functioning.

In addition, under section 13(3) and together with the Treasury Department, we set up the Commercial Paper Funding Facility, or CPFF, and the Money Market Mutual Fund Liquidity Facility, or MMLF.

Both of these facilities have equity provided by the Treasury Department to protect the Federal Reserve from losses.
Indicators of market functioning in commercial paper and other short-term funding markets improved substantially and rapid outflows from prime and tax-exempt money market funds stopped after the announcement and implementation of these facilities.

To read more:
https://www.bis.org/review/r200519a.pdf

European solidarity put to the test by the health crisis

François Villeroy de Galhau, Governor of the Bank of France, at the digital conference at the Bocconi University, Milan.

Ladies and Gentlemen, cari professori e studenti,

I am delighted to share this moment with you. I would like to extend my warmest thanks to all of those who made this virtual meeting possible in particular Rector Gianmario Verona, and Vice-Rector Stefano Caselli together with Francesco Daveri.

To me, Bocconi represents a major source of influence for European integration. Think of some great "bocconiani" who played a fundamental role in building our Economic union: from Luigi Einaudi – the father of the fathers of Europe – to my friend Mario Monti.

I also want to honour the memory of Tommaso Padoa-Schioppa who passed away ten years ago. In the difficult times we are facing, his vision and ability to translate European ideals into active fights – such as the euro – remain inspirational.

Today I stand before you as a committed European, a central banker, but also a friend of Italy. I first and foremost want to express my deep solidarity: Italy – like France – has been one of the countries hardest hit by the pandemic.

I am also well aware of the criticism about Europe being too slow or reluctant to help.

So my purpose today is a challenging one, as I will address the issue of Europe's alleged lack of solidarity.

I will first argue that in fact Europe – and the Eurosystem at the frontline – has broadly risen to the challenge during this acute phase of the crisis.

But we need to do more, and I will then sketch the broad outlines of an effective and collective exit strategy.

I. The Eurosystem at the front line of the European response during the acute phase of the crisis

The lockdown measures have a major impact on the European and so on the Italian economy, which – according to the European Commission – could contract by 9.5% in 2020.

Confronted with this unprecedented and totally unforeseen crisis, the policy response of European Governments – including Italy's – was immediate and strong.

But on both sides of our borders, there is a common temptation to blame Europe for not doing enough.

In reality, Europe is taking action, and more than has been acknowledged. The debate on "Coronabonds" has divided Europeans, but the exceptional monetary action taken by the European Central Bank (ECB) – which is much more significant – should bring us together.

In order to fulfill its mandate, the Eurosystem has always been clear in its commitment to ensure appropriate financial conditions in all parts of the euro area, and decisive in its action to fight fragmentation within the euro area.

We will not allow adverse market dynamics to lead to unjustified interest rate increases in some countries, which would put at risk the smooth transmission of our common monetary policy.

To put it simply: yields and spreads do matter, even if we don't target fixed levels. Hence, and consistent with the risk of still lower inflation, we announced on 18 March a EUR 750 billion Pandemic Emergency Purchase Programme (PEPP).

In implementing the PEPP, we are and will remain flexible; the Eurosystem should be guided more by market dynamics and liquidity conditions than predetermined volumes of purchases.

To read more:
https://www.bis.org/review/r200515a.pdf

Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities

United States Government Accountability Office

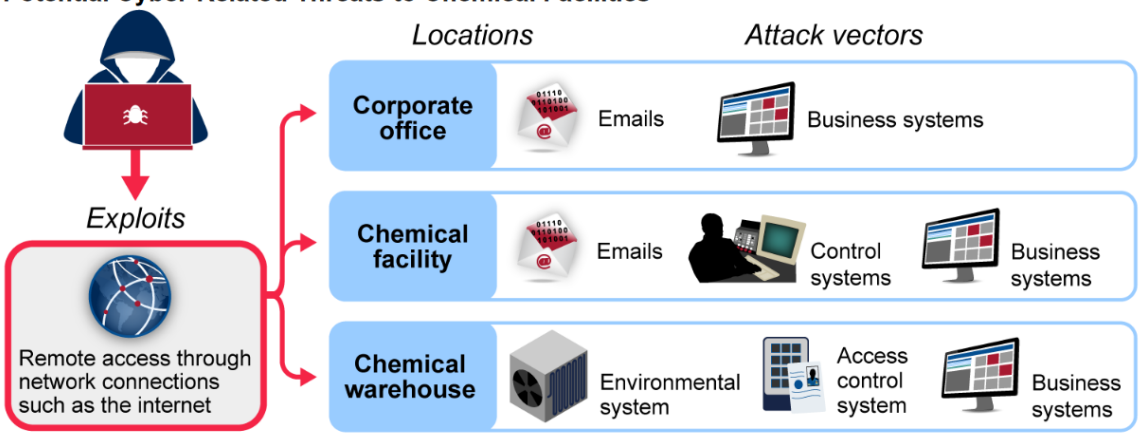
Report to Congressional Requesters

The Chemical Facility Anti-Terrorism Standards (CFATS) program within the Department of Homeland Security (DHS) evaluates high-risk chemical facilities' cybersecurity efforts via inspections that include reviewing policies and procedures, interviewing relevant officials, and verifying facilities' implementation of agreed-upon security measures.

GAO found that the CFATS program hasguidance designed to help the estimated 3,300 CFATS-covered facilities comply with cybersecurity and other standards, but the guidance has not been updated in more than 10 years, in contrast with internal control standards which recommend periodic review.

CFATS officials stated that the program does not have a process to routinely review its cybersecurity guidance to ensure that it is up to date with current threats and technological advances. Without such a process, facilities could be more vulnerable to cyber-related threats.

Potential Cyber-Related Threats to Chemical Facilities



Source: GAO analysis of potential cybersecurity threats to chemical facilities. | GAO-20-453

The CFATS program developed and provided cybersecurity training for its inspectors, but GAO found that the CFATS program does not fully address 3 of 4 key training practices, or address cybersecurity needs in its workforce planning process, as recommended by DHS guidance.

Specifically:

• The CFATS program does not:
(1) systematically collect or track data related to inspectors' cybersecurity training or knowledge, skills, and abilities;

(2) develop measures to assess how training is contributing to cybersecurity-related program results; or

(3) have a process to evaluate the effectiveness of its cybersecurity training in improving inspector skillsets.

• The program also has yet to incorporate identified cybersecurity knowledge, skills, and abilities for inspectors in its current workforce planning processes or track data related to covered facilities' reliance on information systems when assessing its workforce needs.

Fully addressing key training practices will help ensure that CFATS inspectors have the knowledge, skills, and abilities for cybersecurity inspections, and identifying cybersecurity needs in workforce planning will help the program ensure that it has the appropriate number of staff to carry out the program's cybersecurity-related efforts.

To read more:
https://www.gao.gov/assets/710/706972.pdf

Data and Technology Research Project Update Spotlight

PCAOB
Public Company Accounting Oversight Board

Advancements in technology are affecting the nature, timing, preparation, and use of financial information.

Some audit firms are making significant investments in personnel and other resources to expand their use of technology-based audit tools, including software used to perform data analytics (technology-based tools), to plan and perform audits.

In light of the increasing use of technology by auditors and preparers, the Board's strategic plan highlights that we must anticipate and respond to these innovations and their corresponding opportunities and risks.

The PCAOB's Office of the Chief Auditor established a research project on data and technology to assess whether there is a need for guidance, changes to PCAOB standards, or other regulatory actions.

As part of assessing whether regulatory action is necessary in response to the evolving audit landscape, we have gathered information from PCAOB oversight activities, reviewed changes to firms' methodologies, and studied relevant academic research.

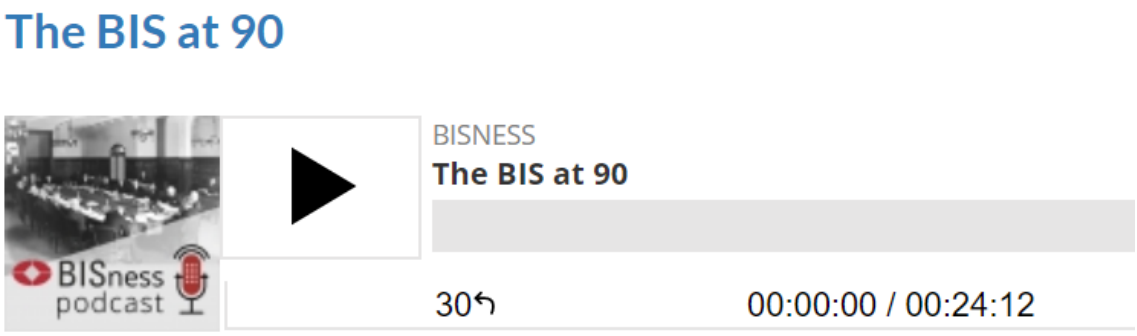
We have engaged with key stakeholders on their experiences with data and technology and have monitored the activities of other standard setters and regulators.

Our work has also been informed by the PCAOB Data and Technology Task Force (Task Force), whose members provide additional insights into the use of technology by auditors and preparers.

This Spotlight shares certain observations from our research and outreach activities. To read more: https://pcaobus.org/Documents/Data-Technology-Project-Spotlight.pdf

The BIS at 90

Piet Clement explains the origins of the BIS and the roles it has played since opening on 17 May 1930.



The BIS was created in 1930 by the Hague Conference as an international financial organisation.

Ever since, its key mandate has been to foster cooperation among central banks and other agencies in pursuit of monetary and financial stability.

Initially mainly focused on Europe, the BIS, from the 1960s onward, became increasingly global in its activities and outreach.

Today it brings together sixty member central banks, representing countries from around the world that together make up about 95% of world GDP.

Apart from its headquarters in Basel, Switzerland, the BIS has two representative offices, one for Asia and the Pacific in Hong Kong SAR (since 1998), and one for the Americas in Mexico City (since 2002).

Throughout its history, the BIS has been involved in many historical events and developments in the monetary and financial sphere.

These include the repercussions of the world financial crisis of 1931, the rebuilding of European multilateral payments in the 1950s, the transatlantic management of the Bretton Woods system in the 1960s, and the international efforts to deal with the fall-out of inflation and of the banking and debt crises in the 1970s through the 1990s.

The BIS played an important role in the early history of European monetary unification (before the foundation of the European Monetary Institute in Frankfurt in 1994).

It also hosts the experts from the global banking regulation and supervision community, who have been responsible for developing an International Capital Framework (known consecutively as Basel Accord, Basel II and Basel III), a global agreement aimed at strengthening capital adequacy rules for internationally active banks.

You may visit:
https://bispodcast.libsyn.com/the-bis-at-90

BIS Working Papers, No 865 - The drivers of cyber risk

Iñaki Aldasoro, Leonardo Gambacorta, Paolo Giudici, Thomas Leach
Monetary and Economic Department

BIS

Information technology (IT) has become a critical component of well-functioning economies, underpinning economic growth over the past decades.

Organisations of all sizes in both the public and private sector are becoming ever more interconnected and reliant on IT products and services, such as cloud-based systems and artificial intelligence.

Accordingly, there is a growing exposure to cyber risks.

Cyber risk commonly refers to the risk of financial loss, disruption or reputational damage to an organisation resulting from the failure of its IT systems.

These episodes include malicious cyber incidents (cyber attacks) where the threat actor intends to do harm (e.g. ransomware attacks, hacking incidents or data theft by employees).

In the wake of recent high-profile cyber attacks such as the WannaCry incident in May 2017, public awareness of these threats is on the rise (see Figure 1).

Notes: Number of online searches for "cyber risk" and "operational risk" over the last decade. Worldwide search interest is relative to the highest point (=100). Data accessed on 7 Feb 2020.
Source: Google Trends.

Figure 1
Interest on cyber risk is on par with operational risk.

Firms actively manage cyber risk and invest in cyber security. However, cyber costs are difficult to quantify. In the financial sector, cyber risks are a key "known unknown" tail risk to the system and a potential major threat to financial stability.

More broadly, cyber risk in sectors that play a critical role in the economic infrastructure could have systemic implications and should be viewed as a matter of national security (Brenner, 2017).

Despite the acknowledgement of such consequences, information concerning the costs, drivers and potential mitigating factors of cyber incidents is relatively scarce.

This paper seeks to help fill this gap.

The analysis uses a detailed dataset of over 100,000 cyber events across all sectors of economic activity.

We first document some stylised facts.

The frequency of cyber incidents rose strongly in the decade to 2016, but has since receded somewhat.

This reduction could reflect increased investment in cyber security, but also delays in discovery or reporting.

The average cost of cyber events has been increasing constantly over the last decade.

We find that certain economic sectors display a greater resilience to cyber incidents: for example, the financial sector has experienced a higher frequency of cyber incidents but these have been on average relatively less costly.

Regarding the type of incident, privacy violations and phishing/skimming scams fraud in short are the most frequent but least costly.

Data breaches, in turn, are both relatively frequent and costly, while business disruptions are quite infrequent but can have high costs.

The richness of the database also allows us to examine the relationship between firm, sector and eventspecific characteristics and the relative cost of cyber events.

The main empirical results can be summarised as follows.
First, we identify the key drivers contributing to the costs of cyber-related events.

Firm size measured in terms of total revenues is positively correlated with the average cost of an event, implying that larger firms tend to incur larger costs.

However, the elasticity is quite low: a 1% increase in total revenues is associated with a 0.2% increase in cyber costs.

We also find that that cyber events which impact multiple firms at the same time (i.e. “connected” events) are also associated with higher costs.

Cyber-related incidents can occur unintentionally by human error, e.g. a bug in some internally developed software; or can also be caused by an actor with malicious intent.

Malicious cyber attacks have, on average, lower costs, because most incidents simply reflect general discontent.

However, some actors seek a profit or to inflict the largest possible losses and damage.

Indeed, a quantile analysis reveals that at the tail of the sample distribution this relationship is reversed and in fact malicious incidents are associated with higher costs.

This finding indicates that, while most attackers are stopped before they can do considerable harm, a successful attacker can go on to cause extensive damage.

Incidents related to crypto exchanges, which are largely unregulated, produce higher losses. We then look at the role of developing technological capabilities to reduce cyber costs.

Many firms, especially if they are smaller, could lack the specific knowledge needed to make rational decisions about which software or cyber security provider to choose.

Information asymmetries between firms can further exacerbate problems when investments in new technologies do not pan out as expected (Zhu and Weyant, 2003).

How can firms mitigate these risks? We find that investment in technological skills pays off in terms of reducing the cost of cyber events. In particular, firms in sectors that employ more IT specialists, use more computers and provide more IT training to staff, are better equipped to mitigate the costs stemming from a cyber event.

From a policy perspective, these findings can inform governments and cross-sector regulators regarding the mitigating steps that can be taken to reduce the cost of cyber incidents and which sectors are lacking in such areas.

Cybersecurity activities provided by third-party service providers are an alternative to risk transfer mechanisms.

Rowe (2007) argues that, if multiple organisations share the same service provider, economies of scale and information-sharing can create positive externalities.

Cloud technology can reduce IT costs, improve resilience and enable firms to scale better (Financial Stability Board, 2019).

However, the technology strengthens interdependence across firms that have shared exposures to similar (or even the same) cloud service providers.

For example, several cloud suppliers may use a common operating system so that, if the operating system has a vulnerability, it could create a correlated risk across all cloud suppliers.

By analysing the cost-benefit trade-off, we find that the use of cloud services is associated with lower costs of cyber events.

While this speaks to the resilience of cloud technology, it should be interpreted with caution.

As firms' exposure to cloud services increases and cloud providers become systemically important, cloud dependence is likely to increase tail risks (Danielsson and Macrae, 2019).

Of particular concern is the exposure to cyber risk of financial institutions and infrastructures, given the critical services they provide (Kopp et al., 2017; Committee on Payments and Market Infrastructures, 2014).

Following the financial crisis, banks in particular became a target for activists. We interact a finance sector dummy variable with our baseline regressors to assess average costs of losses relative to other sectors.

While the frequency of attacks in the financial sector is high relative to others, the sector is better at mitigating the cost of attacks.

This could be the outcome of more proactive policy, regulation and investment in risk management and governance practices with respect to information technology.

Cryptocurrencies have emerged as a challenge to established financial institutions and currencies.

Despite initial claims of superior security, the cryptocurrency space has suffered numerous cyber attacks.

This notoriety stems both from attacks on crypto-exchanges due to poor security standards and due diligence on internal controls, as well as from the use of cryptocurrencies as ransomware that is difficult to trace, e.g. WannaCry (Kshetri and Voas, 2017).

We find that the average cost of crypto-related events is significantly higher.

These costs are not independent of the soaring price of cryptocurrencies in recent years.

We document the existence of a strong positive correlation between the price of bitcoin and the intensity of attacks on crypto-exchanges.

To quantify this relationship, we use a Probit model to show that an increase in the price of bitcoin increases the likelihood of future attacks on crypto-exchanges.

However, the inverse relationship is not found to be significant, i.e. there is no price decrease following cyber incidents related to cryptocurrencies.

To read more:
https://www.bis.org/publ/work865.pdf

Google's "Scam Spotter" program

SLOW DOWN

Watch out for sudden urgency

Even if the romance has built slowly over time, a scammer's request for money can come on quite urgently.

SPOT CHECK

Do a search of your admirer

Often scammers will set up accounts using stolen photos from the internet. Search for their name or their photo to verify that they are who they say they are.

STOP! DON'T SEND

Say no to gift cards

In extraordinary situations, you might offer to buy your suitor a physical item. If they insist on a gift card or wire transfer instead, it's a scam.

SLOW DOWN

Ask clarifying questions

Government employees aren't paid on commission. If a scammer gets irritated when you try to slow it down, they're probably a fraud.

SPOT CHECK

Check with the organization directly

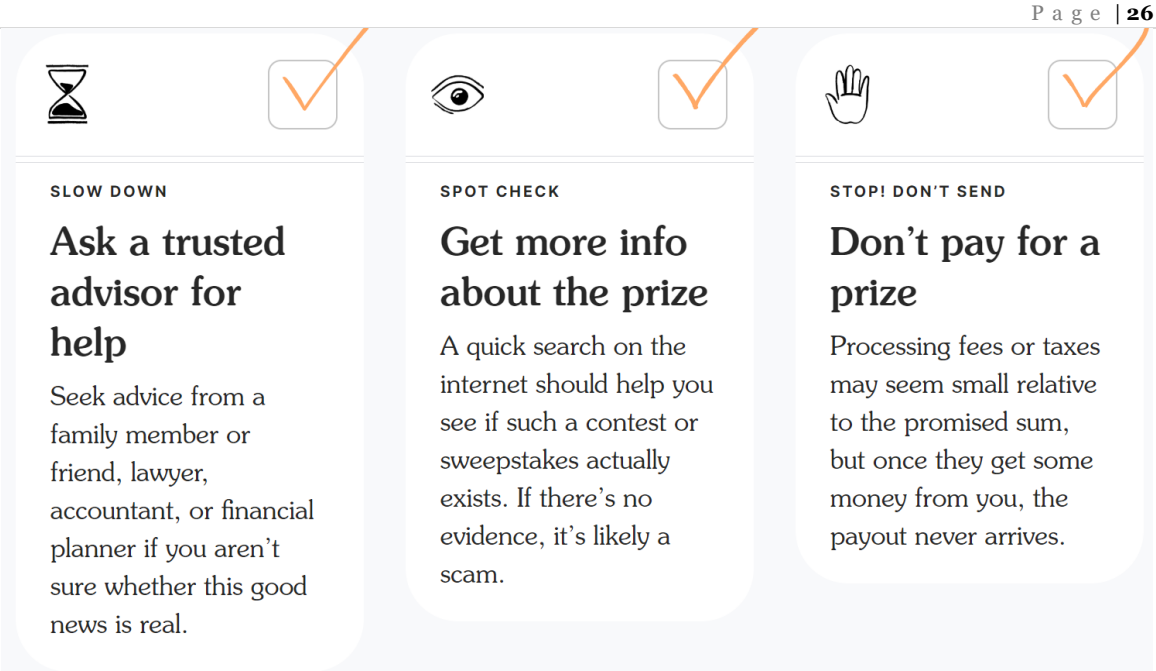
Don't use contact details provided by the caller. Do your own research to find an official number or website.

STOP! DON'T SEND

Don't agree to odd payments

You should never pay a bill with a gift card, wire transfer or Bitcoin. Any reputable organization will ask for credit card or check.

Bad news out of the blue? News too good to be true? No matter the scheme, we can apply the three golden rules to **spot the scam.**



You may visit:
https://scamspotter.org/

Countering Covid-19: The nature of central banks' policy response

Agustín Carstens, General Manager of the BIS, at the UBS High-level Discussion on the Economic and Monetary Policy Outlook, Zurich.

It is a pleasure and an honour to participate in this panel with Thomas Jordan and Axel Weber. Axel, thank you very much for the invitation.

I join Thomas in expressing my sympathy to everyone who has been affected by this pandemic and wishing all of you in the audience good health. In my opening remarks, I will briefly address the economic impact of Covid-19, to then move on to analyse the policy response of primarily the advanced economies' central banks.

No normal recession

The Covid-19 pandemic and the induced global lockdown are a truly historic event. Never before has the global economy been deliberately put into an induced coma. This is no normal recession, but one that results from explicit policy choices to avoid a large-scale public health disaster.

The unique character of this recession poses unfamiliar challenges. On the demand side, lockdowns and social distancing have made consumer spending highly insensitive to policy stimulus.

On the supply side, containment measures ordered by governments have directly hindered production, with the repercussions spreading through local and global supply chains. These disruptions could leave permanent scars on the economy if they result in large-scale layoffs and bankruptcies.

The pandemic also profoundly shook financial markets. As events unfolded, heavy sell-offs across a wide range of assets and a sharp tightening of financial conditions threatened to derail the economy even further.

The policy reaction has been unprecedented. Governments, central banks and supervisory authorities have responded boldly, decisively and imaginatively to limit the consequences of simultaneous sudden stops in spending, economic activity, funding and financial market functioning.

In particular, it took massive and unprecedented policy actions on the part of central banks and other authorities to prevent a financial collapse that would have compounded the drop in real activity.

On the fiscal side, governments have launched massive stimulus and projected fiscal deficits on a scale not seen since World War II.

A major issue will be how to finance the resulting fiscal deficits and prevent them from destabilising markets. In addition, the fiscal measures have been accompanied by far-reaching funding and credit guarantees provided by governments and/or their development banks.

The response of central banks

The sudden shock called for a speedy and massive policy response .The actions of central banks have again highlighted their central role in crisis management as they swiftly cut policy interest rates and launched large-scale balance sheet measures

This brought central banks to the forefront again as they can mobilise financial resources faster than any other authority. In this round of urgent policy mobilisation, central banks' actions concentrated on large-scale purchases of government debt as well as credit support for firms and households.

The latter encompassed funding-for lending schemes, purchases of corporate debt, and support provisions for small and medium-sized enterprises. This last set of measures is designed to travel the "last mile".

The main objective is to prevent liquidity strains that could lead to bankruptcies of solvent firms and leave long-lasting scars on growth potential. These extraordinary actions were designed precisely to flatten the mortality curve of businesses.

For their part, large-scale government bond purchases aim to lower interest rates, to provide monetary stimulus and to help the liquidity and functioning of the sovereign bond markets. This comes in the context of huge borrowing needs by governments as fiscal deficits rise and debt levels surge.

The last feature reflects the rarely employed role of the central bank as a market stabiliser and financing intermediary between the fiscal authorities and financial markets.

This should be temporary, limited by its intent and scale, and in line with the financial stability mandate of central banks. These actions are meant to

smooth the impact of a sudden ramp-up of fiscal spending induced by an extraordinary but, we hope, transient event.

These extraordinary monetary policy actions are designed exclusively to safeguard economic and financial stability, and do not amount to fiscal deficit financing. Consistent with this, the measures undertaken by central banks have contributed to an easing of financial conditions and a calming of financial turmoil.

Setting the boundaries

We could conceptualize the life cycle of a pandemic-induced crisis as having three phases: liquidity, solvency and recovery.

In many countries, we are at the end of the first stage, or at the end of the beginning, where monetary policy actions can be most effective. For the later phases, the heavy lifting should come primarily from fiscal and structural policies.

While central bank measures have been necessary and show initial success, these bring major challenges going forward in the form of a significant overlap between fiscal and monetary policy.

Central bank balance sheets are bound to grow considerably this year, in tandem with a massive increase in public debt. There is a growing nexus between fiscal and monetary policies. Against this background, how can we safeguard central bank independence and credibility going forward?

First, fiscal sustainability should be assured, otherwise perceptions may arise that debt could be inflated away. Governments can start by crafting strong intertemporal fiscal strategies, reining in future spending and developing sound revenue policies.

But the most direct route to fiscal sustainability lies in boosting growth potential. This means implementing structural reforms to lift potential growth rates, mitigating failures of healthy firms, orienting fiscal policies towards investment, preserving global supply chains and safeguarding free trade .

Second, central bank policies need to remain credibly focused on maintaining macroeconomic stability. Actions should remain in line with mandates, particularly price and financial stability.

The intention behind policy actions should be clearly articulated and overt deficit financing avoided. Proper, institutional governance should be preserved.

Wherever possible, indemnities of governments to cover potential central bank losses are extremely useful. Exit strategies should be articulated as soon as possible. Of course, an optimal exit is one that is induced by a favourable economic environment.

The bottom line is that there is a need to recognise the limits of monetary policy. Central banks cannot intervene in government debt markets on a large scale for any great length of time. Eventually, the natural boundaries between fiscal and monetary policy will need to be fully restored to preserve central bank credibility.

Finally, let me say that the aggressive measures described, crossing the traditional boundaries between fiscal and monetary policies, are only feasible for central banks in advanced economies with high credibility stemming from a long track record of stability-oriented policies. This is strong medicine and should only be taken with extreme care.

Seven Moments in Spring: Covid-19, financial markets and the Bank of England's balance sheet operations

Andrew Hauser, Executive Director, Markets - Bloomberg, London

BANK OF ENGLAND

I have always had a funny feeling about Friday the 13th – and 13 March 2020, Mark Carney's last day in the office as Governor of the Bank of England, was no exception.

Two days earlier, on Wednesday 11 March, the Bank and HM Treasury had launched an unprecedentedly comprehensive package of measures to respond to the rapidly growing economic consequences of the spread of Covid-19.

Hailed globally as a shining example of how monetary, fiscal and regulatory policies could work together to reinforce one another, the combination of interest rate cuts, government spending, cheap funding and capital easing measures seemed sure to stabilise markets and restore some much needed confidence to households and businesses.

So it cannot have been hugely welcome when, on Friday morning, with the removal vans waiting outside, I suggested the Bank's Governors needed to meet again before the weekend.

The previous day had seen disorderly conditions in the US Treasury market and the largest one-day fall in equity prices since the 1987 crash, despite major new policy announcements from the Federal Reserve and ECB.

As I ran through my gloomy update, it was clear that further action would be needed – but perhaps not at that stage quite how much more. Monday morning would be no quiet start for Andrew Bailey, the new Governor.

In my remarks today, I want to give a bird's eye's view of what happened in those extraordinary weeks, and the steps we took – either in concert with others, or using our own balance sheet – to neutralise the sudden pre-lockdown 'dash for cash' – the biggest test of core market functioning and resilience since the Great Financial Crisis (GFC) of 2008-9.

Judged solely against that narrow yardstick, central bank actions – unprecedented in scale and speed – were successful in averting a market meltdown. Commercial banks, strengthened by the post-GFC reforms, have continued to lend, supported by a range of public sector schemes. And we learned some surprisingly positive things about operating a financial system remotely – both in terms of market resilience, but also in terms of diversity and inclusion.

But this is no time for self-congratulation. The broader aspects of the Covid-19 crisis – medical, social, economic, and personal – remain hugely challenging, and involve a much wider set of actors than central banks alone.

Further financial instability cannot be ruled out. And the sheer scale of the balance sheet interventions necessary in recent months pose important longer term questions. About the extent to which the non-bank financial system may still be capable of amplifying instability – for example through sudden non-bank deleveraging, runs on money market funds, or rigidities in dealer intermediation.

And about the appropriate balance of responsibilities between the public and private sector for dealing with such vulnerabilities.

I cannot give comprehensive answers to these questions today. But, in what follows, I have tried to provide some raw material for that exercise, illustrated using seven of the most vivid 'moments' from my own experience of the past few weeks.

To read more: https://www.bankofengland.co.uk/-/media/boe/files/speech/2020/seven-moments-in-spring-covid-19-speech-by-andrew-hauser.pdf

Top ten cyber hygiene tips for SMEs during covid-19 pandemic

The EU Agency for Cybersecurity releases ten cyber hygiene tips to support SMEs in protecting their virtual assets against cyber-attacks, during the COVID-19 pandemic.

Crises like the current COVID-19 pandemic have a serious impact on the European as well as the International society and economy. Small and medium-sized enterprises (SMEs) are often coping with difficult times. Unfortunately, cybercriminals often see such crises as opportunities. Phishing and ransomware attacks are on the rise.

SMEs are also faced with a new reality where employees are working more from home. This way they become even more dependent on Information Technology (IT) than before.

It goes without saying that protecting these virtual assets is of utmost importance to almost every SME. According to ENISA, the top ten cyber hygiene topics that SMEs should address, possibly through outsourcing where needed, are presented below:

1. Management buy-in. It is important that management sees the importance of cybersecurity for the organisation and that it is informed on a regular basis.

2. Risk assessment. This answers the question: what do I have to protect and from what? Identify and prioritise the main assets and threats your organisation is facing.

3. Cybersecurity policy. Have the necessary policies in place to deal with cybersecurity and appoint someone, for example an Information Security Officer (ISO), who is responsible for overseeing the implementation of these policies.

4. Awareness. Employees should understand the risks and should be informed about how to behave online. People tend to forget such things rather rapidly, so repeating this every now and then can be valuable.

5. Updates. Keeping everything, meaning servers, workstations, smartphones, etc. up-to-date is key in your cyber hygiene. Applying security updates is part of this process. Ideally, this whole process is to a certain level automated and the updates can be tested in a testing environment.

6. Backups. Prior to doing these updates it is vital to have good backups in place. This will also protect the environment from attacks such as ransomware.

Backup the most important data often and think about the cost of losing data during a certain timespan. Keep the backups offline, test the backups and try to have duplication of the backups.

7. Access management. Have rules/policies in place for access management and enforce them. Make sure default passwords are changed for example, that passwords are not shared, etc.

8. Endpoint protection. Think about securing the endpoints through for example installing antivirus software.

9. Secure remote access. Limit remote access as much as possible and where absolutely needed, enable it but in a secure way. Make sure that communication is encrypted properly.

10. Incident management plan. There should be a plan on how to handle an incident when it occurs. Different realistic scenarios could be part of this plan. Get to know whom you could contact when things are problematic, for instance the national CSIRT.

Central banks' response to Covid-19 in advanced economies

Paolo Cavallino and Fiorella De Fiore

BIS

Key takeaways

- Central banks in advanced economies reacted swiftly and forcefully to the Covid-19 pandemic, deploying the full range of crisis tools within weeks.

  The initial response focused primarily on easing financial stress and ensuring a smooth flow of credit to the private non-financial sector.

- The pandemic triggered complementary responses from monetary and fiscal authorities.

  Fiscal backstops and loan guarantees supported central bank actions. Asset purchases, designed to achieve central banks' objectives, helped contain the costs of fiscal expansions.

- The footprint of central banks' measures will be sizeable. Across the five largest advanced economies, balance sheets are projected to grow on average by 15–23% of GDP before end2020 and to remain large in the near future.

The outbreak of Covid-19 was a shock of unprecedented size and nature. Lockdowns and containment measures on a global scale led to a generalised sudden stop in economic activity.

Workers' reduced income – particularly for precarious workers – exacerbated the fall in demand induced by distancing measures and contributed to an increase in the risk of delinquency on mortgages and consumer loans.

Businesses suffered from collapsing productive activities and reduced cash flow, which was particularly acute in sectors such as automotive, retail and travel. Concerns about household and corporate liquidity, combined with heightened uncertainty, hampered the functioning of key financial market segments.

In March 2020, corporate spreads surged globally for high-yield as well as investment grade issuers.
The markets for asset-backed and mortgage-backed securities froze in many countries. Commercial paper markets experienced strain in the United States, Canada and the euro area due to enhanced rollover risk.

Equity markets came under stress, and implied volatilities jumped for a wide range of assets. The global dash-for-cash disrupted fixed income asset markets.

The US Treasury market experienced a sharp sell-off leading to spikes in long-term yields (Schrimpf, Shin and Sushko (2020)). Pressures arose in the Japanese government bond (JGB) market, and sovereign spreads widened substantially in the euro area.

Central banks responded promptly and forcefully, consistent with their mandates, to preserve smooth market functioning and an effective transmission of monetary policy.

This Bulletin reviews the response of the central banks of the United States, the euro area, Japan, the United Kingdom and Canada.

A swift and forceful reaction

The overriding goal of central banks was to cushion the inevitable drop in economic activity by ensuring a smooth functioning of the financial system and facilitating the flow of credit to households and firms.

In doing so, central banks performed their traditional crisis role as lenders of last resort to the financial sector. They extended it further to become providers of liquidity to the private non-financial sector.

Central banks' response — Table 1

		Bank of Canada	Bank of England	Bank of Japan	Eurosystem	US Federal Reserve System
Interest rate		–1.5%	–0.65%			–1.50%
Lending operations	short-term	TROs, STLF, CTRF	CTRF, W&MF	FSOs, ROs, SLF	LTROs	ROs, PDCF, MMLF
	long-term	TROs	TFSME	SOCF, SOSME	TLTRO III, PELTROs	TALF, MSLP. PPPLF
Asset purchases	short-term	BAPF, PMMP, CPPP	CCFF	CPPs	APP, PEPP	CPFF, MLF
	long-term	CMBP, GCSPs, PBPP, CBPP	APF	JGBPs, CBPs, ETFPs, JREITPs	APP, PEPP	SOMA, PMCCF, SMCCF
Foreign exchange				YEN SL	EUR SLs	USD SLs, FIMA RF

See tables in online appendix for definition of acronyms. In some jurisdictions, central banks have macroprudential and supervisory roles, and can additionally adjust regulation. This taxonomy comprises only monetary measures.

Source: Central bank websites.

Between March and April 2020, the five central banks under review deployed the full set of crisis management policies at their disposal (Table 1). They all offered new lending operations, and either extended or inaugurated asset purchase programmes.

The Federal Reserve, the Bank of Canada and the Bank of England also cut interest rates. In addition, the Federal Reserve and, on a lesser scale, the ECB and the Bank of Japan increased the availability of their currencies abroad through swap lines.

To read more: https://www.bis.org/publ/bisbull21.pdf

Executive Order on Preventing Online Censorship

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Free speech is the bedrock of American democracy. Our Founding Fathers protected this sacred right with the First Amendment to the Constitution. The freedom to express and debate ideas is the foundation for all of our rights as a free people.

In a country that has long cherished the freedom of expression, we cannot allow a limited number of online platforms to hand pick the speech that Americans may access and convey on the internet. This practice is fundamentally un-American and anti-democratic. When large, powerful social media companies censor opinions with which they disagree, they exercise a dangerous power. They cease functioning as passive bulletin boards, and ought to be viewed and treated as content creators.

The growth of online platforms in recent years raises important questions about applying the ideals of the First Amendment to modern communications technology. Today, many Americans follow the news, stay in touch with friends and family, and share their views on current events through social media and other online platforms. As a result, these platforms function in many ways as a 21st century equivalent of the public square.

Twitter, Facebook, Instagram, and YouTube wield immense, if not unprecedented, power to shape the interpretation of public events; to censor, delete, or disappear information; and to control what people see or do not see.

As President, I have made clear my commitment to free and open debate on the internet. Such debate is just as important online as it is in our universities, our town halls, and our homes. It is essential to sustaining our democracy.

Online platforms are engaging in selective censorship that is harming our national discourse. Tens of thousands of Americans have reported, among other troubling behaviors, online platforms “flagging” content as inappropriate, even though it does not violate any stated terms of service; making unannounced and unexplained changes to company policies that have the effect of disfavoring certain viewpoints; and deleting content and entire accounts with no warning, no rationale, and no recourse.

Twitter now selectively decides to place a warning label on certain tweets in a manner that clearly reflects political bias. As has been reported, Twitter seems never to have placed such a label on another politician's tweet. As recently as last week, Representative Adam Schiff was continuing to mislead his followers by peddling the long-disproved Russian Collusion Hoax, and Twitter did not flag those tweets. Unsurprisingly, its officer in charge of so-called 'Site Integrity' has flaunted his political bias in his own tweets.

At the same time online platforms are invoking inconsistent, irrational, and groundless justifications to censor or otherwise restrict Americans' speech here at home, several online platforms are profiting from and promoting the aggression and disinformation spread by foreign governments like China. One United States company, for example, created a search engine for the Chinese Communist Party that would have blacklisted searches for "human rights," hid data unfavorable to the Chinese Communist Party, and tracked users determined appropriate for surveillance. It also established research partnerships in China that provide direct benefits to the Chinese military.

Other companies have accepted advertisements paid for by the Chinese government that spread false information about China's mass imprisonment of religious minorities, thereby enabling these abuses of human rights. They have also amplified China's propaganda abroad, including by allowing Chinese government officials to use their platforms to spread misinformation regarding the origins of the COVID-19 pandemic, and to undermine pro-democracy protests in Hong Kong.

As a Nation, we must foster and protect diverse viewpoints in today's digital communications environment where all Americans can and should have a voice. We must seek transparency and accountability from online platforms, and encourage standards and tools to protect and preserve the integrity and openness of American discourse and freedom of expression.

Sec. 2. Protections Against Online Censorship. (a) It is the policy of the United States to foster clear ground rules promoting free and open debate on the internet. Prominent among the ground rules governing that debate is the immunity from liability created by section 230(c) of the Communications Decency Act (section 230(c)). 47 U.S.C. 230(c). It is the policy of the United States that the scope of that immunity should be clarified: the immunity should not extend beyond its text and purpose to provide protection for those who purport to provide users a forum for free and open speech, but in reality use their power over a vital means of communication to engage in deceptive or pretextual actions stifling free and open debate by censoring certain viewpoints.

Section 230(c) was designed to address early court decisions holding that, if an online platform restricted access to some content posted by others, it would thereby become a "publisher" of all the content posted on its site for purposes of torts such as defamation. As the title of section 230(c) makes clear, the provision provides limited liability "protection" to a provider of an interactive computer service (such as an online platform) that engages in "'Good Samaritan' blocking" of harmful content.

In particular, the Congress sought to provide protections for online platforms that attempted to protect minors from harmful content and intended to ensure that such providers would not be discouraged from taking down harmful material. The provision was also intended to further the express vision of the Congress that the internet is a "forum for a true diversity of political discourse." 47 U.S.C. 230(a)(3). The limited protections provided by the statute should be construed with these purposes in mind.

In particular, subparagraph (c)(2) expressly addresses protections from "civil liability" and specifies that an interactive computer service provider may not be made liable "on account of" its decision in "good faith" to restrict access to content that it considers to be "obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable." It is the policy of the United States to ensure that, to the maximum extent permissible under the law, this provision is not distorted to provide liability protection for online platforms that — far from acting in "good faith" to remove objectionable content — instead engage in deceptive or pretextual actions (often contrary to their stated terms of service) to stifle viewpoints with which they disagree.

Section 230 was not intended to allow a handful of companies to grow into titans controlling vital avenues for our national discourse under the guise of promoting open forums for debate, and then to provide those behemoths blanket immunity when they use their power to censor content and silence viewpoints that they dislike. When an interactive computer service provider removes or restricts access to content and its actions do not meet the criteria of subparagraph (c)(2)(A), it is engaged in editorial conduct. It is the policy of the United States that such a provider should properly lose the limited liability shield of subparagraph (c)(2)(A) and be exposed to liability like any traditional editor and publisher that is not an online provider.

(b) To advance the policy described in subsection (a) of this section, all executive departments and agencies should ensure that their application of section 230(c) properly reflects the narrow purpose of the section and take all appropriate actions in this regard. In addition, within 60 days of the date of this order, the Secretary of Commerce (Secretary), in consultation with the Attorney General, and acting through the National

Telecommunications and Information Administration (NTIA), shall file a petition for rulemaking with the Federal Communications Commission (FCC) requesting that the FCC expeditiously propose regulations to clarify:

(i) the interaction between subparagraphs (c)(1) and (c)(2) of section 230, in particular to clarify and determine the circumstances under which a provider of an interactive computer service that restricts access to content in a manner not specifically protected by subparagraph (c)(2)(A) may also not be able to claim protection under subparagraph (c)(1), which merely states that a provider shall not be treated as a publisher or speaker for making third-party content available and does not address the provider's responsibility for its own editorial decisions;

(ii) the conditions under which an action restricting access to or availability of material is not "taken in good faith" within the meaning of subparagraph (c)(2)(A) of section 230, particularly whether actions can be "taken in good faith" if they are:

(A) deceptive, pretextual, or inconsistent with a provider's terms of service; or

(B) taken after failing to provide adequate notice, reasoned explanation, or a meaningful opportunity to be heard; and

(iii) any other proposed regulations that the NTIA concludes may be appropriate to advance the policy described in subsection (a) of this section.

Sec. 3. Protecting Federal Taxpayer Dollars from Financing Online Platforms That Restrict Free Speech. (a) The head of each executive department and agency (agency) shall review its agency's Federal spending on advertising and marketing paid to online platforms. Such review shall include the amount of money spent, the online platforms that receive Federal dollars, and the statutory authorities available to restrict their receipt of advertising dollars.

(b) Within 30 days of the date of this order, the head of each agency shall report its findings to the Director of the Office of Management and Budget.

(c) The Department of Justice shall review the viewpoint-based speech restrictions imposed by each online platform identified in the report described in subsection (b) of this section and assess whether any online platforms are problematic vehicles for government speech due to viewpoint discrimination, deception to consumers, or other bad practices.

Sec. 4. Federal Review of Unfair or Deceptive Acts or Practices. (a) It is the policy of the United States that large online platforms, such as Twitter

and Facebook, as the critical means of promoting the free flow of speech and ideas today, should not restrict protected speech.

The Supreme Court has noted that social media sites, as the modern public square, "can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard." Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017). Communication through these channels has become important for meaningful participation in American democracy, including to petition elected leaders.

These sites are providing an important forum to the public for others to engage in free expression and debate. Cf. PruneYard Shopping Center v. Robins, 447 U.S. 74, 85-89 (1980).

(b) In May of 2019, the White House launched a Tech Bias Reporting tool to allow Americans to report incidents of online censorship. In just weeks, the White House received over 16,000 complaints of online platforms censoring or otherwise taking action against users based on their political viewpoints. The White House will submit such complaints received to the Department of Justice and the Federal Trade Commission (FTC).

(c) The FTC shall consider taking action, as appropriate and consistent with applicable law, to prohibit unfair or deceptive acts or practices in or affecting commerce, pursuant to section 45 of title 15, United States Code. Such unfair or deceptive acts or practice may include practices by entities covered by section 230 that restrict speech in ways that do not align with those entities' public representations about those practices.

(d) For large online platforms that are vast arenas for public debate, including the social media platform Twitter, the FTC shall also, consistent with its legal authority, consider whether complaints allege violations of law that implicate the policies set forth in section 4(a) of this order. The FTC shall consider developing a report describing such complaints and making the report publicly available, consistent with applicable law.

Sec. 5. State Review of Unfair or Deceptive Acts or Practices and Anti-Discrimination Laws. (a) The Attorney General shall establish a working group regarding the potential enforcement of State statutes that prohibit online platforms from engaging in unfair or deceptive acts or practices. The working group shall also develop model legislation for consideration by legislatures in States where existing statutes do not protect Americans from such unfair and deceptive acts and practices. The working group shall invite State Attorneys General for discussion and consultation, as appropriate and consistent with applicable law.

(b) Complaints described in section 4(b) of this order will be shared with the working group, consistent with applicable law. The working group shall also collect publicly available information regarding the following:

(i) increased scrutiny of users based on the other users they choose to follow, or their interactions with other users;

(ii) algorithms to suppress content or users based on indications of political alignment or viewpoint;

(iii) differential policies allowing for otherwise impermissible behavior, when committed by accounts associated with the Chinese Communist Party or other anti-democratic associations or governments;

(iv) reliance on third-party entities, including contractors, media organizations, and individuals, with indicia of bias to review content; and

(v) acts that limit the ability of users with particular viewpoints to earn money on the platform compared with other users similarly situated.

Sec. 6. Legislation. The Attorney General shall develop a proposal for Federal legislation that would be useful to promote the policy objectives of this order.

Sec. 7. Definition. For purposes of this order, the term "online platform" means any website or application that allows users to create and share content or engage in social networking, or any general search engine.

Sec. 8. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

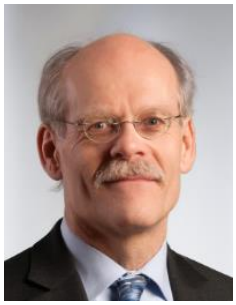
(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

The monetary policy toolbox

Stefan Ingves, Governor of the Sveriges Riksbank, at the Swedish Economics Association, Stockholm.



The spread of the coronavirus came as an unpleasant surprise to us all. It is now clear that the economic consequences of the pandemic threaten to be both serious and protracted.

Most analysts have very weak forecasts for economic developments in the coming quarters, and in some scenarios also for a longer period to come.

We are in the midst of an unforeseen economic development that needs to be met with various macroeconomic tools, and the Riksbank has an important role to play here, together with the Government, the Riksdag (Swedish parliament) and other authorities.

During the initial phase of the crisis, we Executive Board members have already taken a large number of decisions to support the Swedish economy, and thus contribute to meeting the targets for economic policy, and I will comment on what we have done in more detail later on.

We can note that many of the measures have major consequences for the Riksbank's balance sheet – something that will be a recurring theme in today's speech.

Today I intend to focus primarily on how the "monetary policy toolbox" needs to look to be able to manage future challenges.

I will take a longer perspective and discuss which tools the Riksbank may need to use, especially if the low interest rate scenario that has characterised the past 10 years becomes even more prolonged.

The fact that monetary policy measures affect a central bank's balance sheet has become increasingly common in large parts of the world. This development has been driven by the very low interest rates and the need to make monetary policy even more expansionary.
Essentially, it is nothing new – if we go back in time, there are many examples of central banks that have used variation in their asset portfolios as a means of conducting monetary policy.

The monetary policy toolbox also needs to take into account changes in the financial system; for instance, we in Sweden have, in recent years, seen a development towards a higher share of market financing for Swedish companies.

As things look now, there is considerable probability that global interest rates will remain low over a long period of time, and then monetary policy will have to find other ways of working to attain the inflation target than those we are used to, and many of the measures will have consequences for the balance sheet.

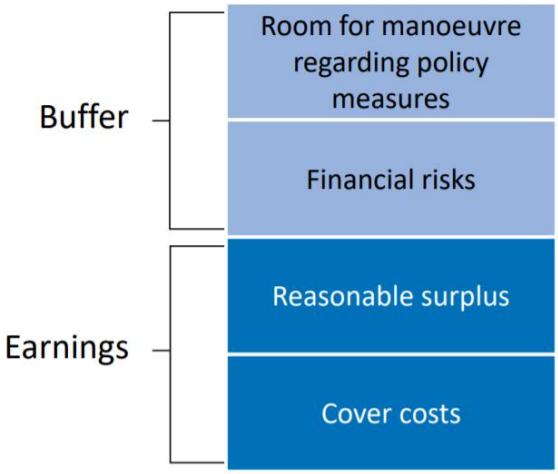
We need to endeavour to attain a better analysis of how measures that have an effect through the balance sheet affect the economy and become as clear and systematic when we talk about these as we have tried to be with regard to steering interest rates.

I intend to begin with a historical retrospective – focusing on the past 30 years – and to describe how monetary policy has developed over time.

Then I will move on to the challenges that monetary policy has faced and that have led to the use of new tools.

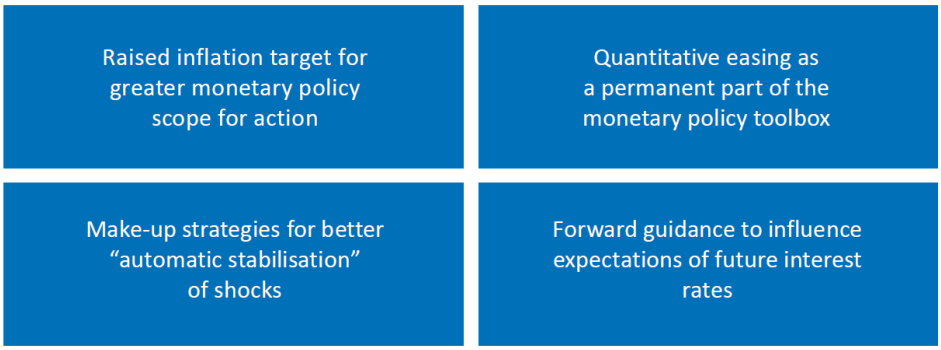
This takes me to the international discussions about the monetary policy toolbox, and, in conclusion, I would like to discuss what opportunities and limitations the Riksbank Inquiry's proposed new act entails.

Four reasons for holding equity capital



The international monetary policy discussion

Tried & tested monetary policy measures



To read more: https://www.bis.org/review/r200611c.pdf

The slides: https://www.bis.org/review/r200611c_slides.pdf

Trade credit, trade finance, and the Covid-19 Crisis

Frédéric Boissay, Nikhil Patel and Hyun Song Shin

BIS

Key takeaways

• As the Covid-19 pandemic hits economic activity, the vulnerabilities of longer and more geographically extended trade credit chains are coming to the fore, especially those related to international trade.

• While risk mitigation is available from financial intermediaries, the bulk of the exposures associated with supply chains is borne by the participating firms themselves, through inter-firm credit.

• Given the prevalence of the US dollar in trade financing, measures such as central bank swap lines that ease global dollar credit conditions may cushion the impact of the pandemic on global value chains.

The pandemic has shocked global supply chains, straining business cash flows and working capital.

For most firms, a large fraction of working capital is categorised as "accounts receivable" — the money owed by customers in the supply chain.

Accounts receivable are matched to some extent by "accounts payable" on the liabilities side of the balance sheet – the money owed to suppliers further up in the supply chain.

This interlocking chain of receivables and payables can be seen as the glue that binds supply chains together in the real economy and sustains their operation, both domestically and internationally (Carstens (2020), Kim and Shin (2012)).

Non-financial corporations may choose to finance the receivables with their own resources, in effect providing credit to customer firms. Such an arrangement is commonly referred to as "trade credit".

Alternatively, they may choose to offload the exposure to banks and other financial intermediaries.

One way to do so is via "factoring", where firms sell their accounts receivable at a discount to a third party known as the "factor", which is typically a bank, and receive immediate cash.
External financing is particularly common for importers and exporters, and the term "trade finance" is used collectively for all such arrangements facilitating international trade.

This Bulletin constructs estimates of firms' working capital and highlights some key trends by drawing on a number of data sources, including the BIS series on aggregate trade finance.

The details of the construction are reported in a separate online annex accompanying this Bulletin.

Using our estimates, we highlight the exposure of supply chains and the broader economy due to the pandemic.

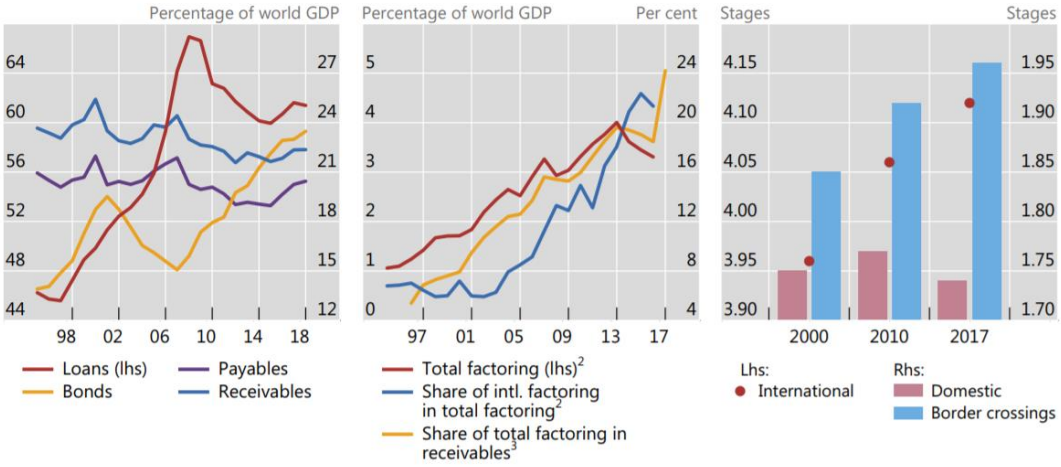
The landscape of trade credit and trade finance

In the world of interlocking payables and receivables, firms borrow from their suppliers and lend to their customers, thus creating a trade credit chain that runs parallel to the flow of goods along supply chains.

Trade credit is an important source of funding for non-financial corporations (NFCs).

The volume of trade payables is comparable with that of outstanding corporate bonds, and amounts to roughly one third of NFCs' outstanding bank loans (Graph 1, left-hand panel).

Trends in trade finance and trade credit — Graph 1



As they are intrinsically linked to the financing of inputs, trade payables are less subject to the cyclical ups and downs of corporate loans and bonds. As such, their volume has been fairly stable at around 20% of GDP over the past 25 years.

In contrast, trade finance, as proxied by the share of cross-border factoring in total factoring, has steadily increased over the past two decades (Graph 1, centre panel).

This long-term trend has gone hand in hand with the rise in international trade and, more specifically, the lengthening of global value chains (GVCs).

While the lengths of domestic production chains estimated using world input-output tables at the country-sector level have remained constant, GVCs involving multiple border crossings have lengthened significantly between 2000 and 2017 (Graph 1, right-hand panel).

Since financing needs increase with the length of supply chains (Bruno et al (2018), Bruno and Shin (2019)), trade finance has become more prominent in the context of GVCs.

To read more:
https://www.bis.org/publ/bisbull24.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.

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

The IAMBD offers standard, premium and lifetime membership, networking, training, certification programs, a monthly newsletter with alerts and updates, and services we can use.

The association develops and maintains three certification programs and many specialized tailor-made training programs for directors.

Join us. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified. Provide independent evidence that you are an expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.
You may visit:
https://www.iambd.org/HowToBecomeMember.html

2. Monthly Updates – Visit the Reading Room of the association at:
https://www.iambd.org/Reading_Room.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 may visit:
https://www.iambd.org/Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We can tailor all programs to meet specific requirements.