International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, December 12, 2022

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

Michael S Barr, Vice Chair for Supervision of the Board of Governors of the Federal Reserve System, hit the nail on the head when he said at the American Enterprise Institute in Washington, DC:

"In an environment of ever-changing risks, stress tests can quickly lose their relevance if their assumptions and scenarios remain static."

He continued: "Stress tests are not meant to be predictions about the future. Humility suggests caution in that regard. But they should be stressful: poking and prodding at the system so we can attempt to uncover hidden risks that could become manifest under certain scenarios.

This is particularly important in today's complex and interconnected financial system, in which problems can spread and lead to unexpected losses. For instance, we recently saw how exposure to interest rate risk at a

set of leveraged pension funds in the United Kingdom, coupled with unprecedented large movements in rates, caused significant disruptions to the gilt market.

This was not a risk that anyone saw coming, but it spilled over to the U.K. financial markets in a way that required a large-scale intervention by the government.

Other recent examples, to name a few, include the messy failure of Archegos last year; Russia's war against Ukraine; tensions in and with China; the implosion of the crypto-asset exchange FTX and the resulting crypto-asset market dislocations; and volatility in the markets for fixed-income securities, affecting market liquidity."

The *attempt to uncover hidden risks* is a major challenge.

According to Ovid: "The cause is hidden; the effect is visible to all". With financial stress testing we must try to *uncover hidden risks,* the cause and the effect. This is difficult, but Lao Tzu would agree, as he has said: "Do the difficult things while they are easy and do the great things while they are small."

Read more at number 2 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 6)

Implementation monitoring of the Principles for Financial Market Infrastructures (PFMI): Level 3 assessment on Financial Market Infrastructures' Cyber Resilience

BANK FOR INTERNATIONAL SETTLEMENTS

OICV-IOSCO
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

Number 2 (Page 9)

Why bank capital matters

Michael S Barr, Vice Chair for Supervision of the Board of Governors of the Federal Reserve System, American Enterprise Institute, Washington DC

Number 3 (Page 16)

International cooperation in a world of digitalisation

Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, at the 22nd International Conference of Banking Supervisors

Number 4 (Page 19)

PCAOB Launches Technology Innovation Alliance Working Group

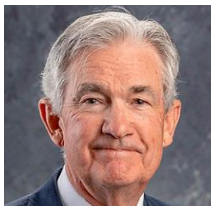
Led by Board Member Ho, expert panel will advise Board on impact of emerging technologies and provide recommendations for PCAOB oversight

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

Number 5 (Page 21)

Inflation and the labor market

Jerome H Powell, Chair of the Board of Governors of the Federal Reserve System, at the Hutchins Center on Fiscal and Monetary Policy, Brookings Institution, Washington DC.



Number 6 (Page 24)

The European Climate Law and the European Central Bank

Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, Lustrum Symposium organised by Dutch Financial Law Association

Number 7 (Page 27)

Pairing up Cybersecurity and Data Protection Efforts: EDPS and ENISA sign Memorandum of Understanding

The European Data Protection Supervisor (EDPS) and the European Union Agency for Cybersecurity (ENISA) sign a Memorandum of Understanding (MoU) which establishes a strategic cooperation framework between them.

Number 8 (Page 31)

Mega - Event Sports Diplomacy: A Strategic Communications Perspective

Una Aleksandra Bērziņa Čerenkova

Number 9 (Page 34)

NIST Finds a Sweet New Way to Print Microchip Patterns on Curvy Surfaces

Number 10 (Page 37)

U.S. Cyber Command, DARPA Initiate Rapid Cyber Capability Prototyping and Integration Pilot

Constellation aims to accelerate maturation of tactical and strategic cyber capabilities, efficiently integrate them into operational warfighting platforms

Number 1

Implementation monitoring of the Principles for Financial Market Infrastructures (PFMI): Level 3 assessment on Financial Market Infrastructures' Cyber Resilience

Executive summary

In April 2012, the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) published the Principles for financial market infrastructures (PFMI).

The PFMI set expectations for the design and operation of key financial market infrastructures (FMIs) in order to enhance their safety and efficiency and, more broadly, to limit systemic risk and foster transparency and financial stability.

The Principles apply to all systemically important payment systems (PSs), central securities depositories (CSDs), securities settlement systems (SSSs), central counterparties (CCPs) and trade repositories (TRs) (collectively, FMIs).

These FMIs collectively clear, settle and record transactions in financial markets. Following the publication of the PFMI, the CPMI and IOSCO agreed to monitor their implementation in 28 CPMI and IOSCO member jurisdictions via a dedicated standing group, the Implementation Monitoring Standing Group (IMSG).

Implementation is being monitored on three levels. Level 1 self-assessment reports on whether a jurisdiction has completed the process of adopting legislation and other policies that will enable it to implement the Principles and Responsibilities.

Level 2 assessments are peer reviews of the extent to which the content of the jurisdiction's implementation measures is complete and consistent with the PFMI.

Level 3 (L3) peer reviews examine consistency in the outcomes of implementation of the Principles by FMIs and implementation of the Responsibilities by authorities.

This report represents the fourth L3 assessment of consistency in the outcomes of FMIs' implementation of the PFMI.

It focuses on cyber resilience and was carried out during 2020–22 by the IMSG and a team of experts from CPMI and IOSCO member jurisdictions.

While Level 3 assessment reports do not include ratings, they do include key findings.

In this vein, the IMSG has identified one serious issue of concern in the area of cyber response and recovery plans to meet the two-hour recovery time objective (2hRTO) and four issues of concern in the area of cyber resilience planning and testing. The IMSG has also noted some observations.

Contents

Elements of the cyber resilience guidance — Graph 1

Source: CPMI-IOSCO Cyber Guidance (2016).

To read more: https://www.bis.org/cpmi/publ/d212.pdf

Number 2

Why bank capital matters

Michael S Barr, Vice Chair for Supervision of the Board of Governors of the Federal Reserve System, American Enterprise Institute, Washington DC

In my first speech as Vice Chair for Supervision in September, I said that the Federal Reserve Board would soon engage in a holistic review of capital standards. My argument, then and now, is that our review of regulatory policy must be a periodic feature of bank oversight.

Banking and the financial system continuously evolve, and regulation must adapt to address emerging risks. Bank capital is strong, but in doing our review, we should and are being humble about our ability—or that of bank managers—to predict how a future financial crisis might unfold, how losses might be incurred, and what the effect might be on the financial system and our broader economy.

That humility, that skepticism, will serve us well in crafting a capital framework that is enduring and effective. It will help make sure that we do not lose the hard-fought gains in resilience over the past decade and that we prepare for the future.

That review is still underway, and I have no firm conclusions to announce today. Rather, I thought it would be helpful at this early stage to offer my views on capital regulation and the role that capital standards play in helping to advance the safety and soundness of banks and the stability of the financial system.

By "holistic," I mean not looking only at each of the individual parts of capital standards, but also at how those parts may interact with each other—as well as other regulatory requirements—and what their cumulative effect is on safety and soundness and risks to the financial system.

This is not an easy task, because finance is a complex system. And to make the task even harder, we are looking not only at how capital standards are working today, but also how they may work in the future, when conditions are different.

As I mentioned, we are approaching the task with humility—not with the illusion that there is an immutable capital framework to be discovered, but rather, with the awareness that revisions we conceive of today will reflect our current understanding and will inevitably require updating as our understanding evolves.

Why Do Banks Have Capital?

Let me start by explaining why banks have capital. Banks play a critical role in the economy by connecting those seeking to borrow with those seeking to save. A bank lends to its customers, including individuals and businesses, based on its assessment of the customer's creditworthiness.

A bank's depositors benefit from having bank accounts that allow them to easily make payments to others and to maintain a balance of money in a safe and liquid form. A healthy banking sector is central to a healthy economy.

The nature of banking, however, along with the interconnectedness of the financial system, can pose vulnerabilities. Even if a bank is fundamentally sound, it can suddenly be threatened with failure if its customers lose confidence and withdraw deposits. This inherent vulnerability can pose risks to the entire economy.

In the 19th and early 20th centuries, before the creation of the Federal Reserve and the Federal Deposit Insurance Corporation (FDIC), banking panics were frequent and costly to the economy.

Based on this experience—and similar experiences around the globe—many countries employ deposit insurance and other forms of a safety net to protect depositors and banks.

But offering this protection, shielding depositors and banks from risk, can have the perverse effect of encouraging risk-taking, creating what is called "moral hazard." Supervision and regulation—including capital regulation—provides a critical counterbalance, to ensure that banks, not the taxpayers, internalize the costs to society of that risk-taking.

The impact of inadequate supervision and regulation was starkly revealed in the Global Financial Crisis, as banks and their functional substitutes in the nonbank sector borrowed too much to fund their operations.

While nearly all were "adequately capitalized" in theory, many were undercapitalized in practice, since their capital levels did not reflect future

losses that would severely weaken their capital positions. And banks lacked appropriate controls and systems to measure and manage their risks.

That crisis also exposed the extent to which banks and broader financial system had become reliant on short-term wholesale funding and prone to destabilizing dynamics.

The sudden shutdown of short-term wholesale funding posed severe liquidity challenges to large financial intermediaries, both banks and nonbanks, and caused significant dislocations in financial markets.

The cost to society was enormous, with widespread devastation to households and businesses. Even with an unprecedentedly large response by government, six million individuals and families lost their homes to foreclosure.

The crisis brought on the worst and longest recession since the Great Depression. It took six years for employment to recover, during which long-term unemployment ran for long periods at a record high, and more than 10 million people fell into poverty.

The crisis left scars on families and businesses that are evident even today, and it was in part driven by imprudent risk taking by banks and nonbank financial institutions. This experience prompted the United States and other jurisdictions to revisit how supervision and regulation, including capital regulation, could have better contained that risk in both the bank and nonbank sectors.

That is why capital levels today are strong. While we have learned from and adapted to the lessons from the Global Financial Crisis, this experience underscores the need for humility and continued vigilance about the risks we may not fully appreciate today.

What Bank Capital Is and Isn't

Capital regulation—requiring a bank to operate with what is deemed to be an adequate level of equity based on its asset size and its risks—is a useful tool to strengthen the incentives for banks to lend safely and prudently.

First, I'll begin with what capital is—essentially shareholder equity in the bank. People sometimes use the shorthand of banks "holding capital" when speaking of capital requirements; however, it's helpful to remember that capital is not an asset to be held, reserves to be set aside, or money in a vault; rather, it is the way, along with debt, that banks fund loans and other assets. Without adequate capital, banks can't lend.

Higher levels of capital mean that a bank's managers and shareholders have more "skin in the game"—and have incentives to prudently manage their risks—because they bear more of the risk of the bank's activities.

Next, let me speak to how capital and debt work together to fund a firm's operations. In theory, companies should be indifferent to the mix of equity and debt they use to fund themselves, since the creditors of a safer firm will lend to it at lower rates and shareholders of a safer firm will accept a lower return on their investment.

That may not fully hold for banks because insured depositors are made risk-insensitive through deposit insurance and other creditors may provide lower cost funding if they believe the government may bail out banks in distress.

Forcing banks to fund more of their activities with equity, instead of debt, could raise the private costs of funding to the bank, and cause banks to pass those higher costs of credit to consumers. These considerations must be balanced against the public benefits of higher capital.

Empirical research supports the social benefits of strong capital requirements at banks, particularly when economic conditions weaken. While poorly capitalized banks may be forced to shrink during bad times, better capitalized banks have the capacity to support the economy by continuing to lend to households and businesses through stressful conditions. And to the extent bank capital reduces the frequency or severity of financial crises, the public is much better off with strong capital.

Last, the highest standards should apply to the highest risk firms. Larger, more complex banks pose the greatest risk and impose greater costs on society when they fail. Higher capital requirements help to ensure that larger, more complex banks internalize this greater risk and counterbalance the greater costs to society by making these firms more resilient.

Further, matching higher capital standards with higher risk appropriately limits the regulatory burden on smaller, less complex banks whose activities pose less risk to the financial system. This helps to promote a diverse banking sector that provides consumers greater choice and access to banking services.

Interactions with the Nonbank Sector

Banks, of course, are part of a broader financial system. The share of credit intermediated outside of banks has grown considerably over the past 40 years. In fact, nonbank financial intermediaries, broadly defined, fund

nearly 60 percent of the credit to the U.S. economy today as compared to approximately 30 percent in 1980.

Nonbank financial firms include money market funds, the insurance sector, the government-sponsored enterprises (Fannie Mae, Freddie Mac, and the Federal Home Loan Bank system), hedge funds and other investment vehicles, and still other nonbank lenders.

There are lots of reasons for these trends, including technological advancements, financial innovation, regulatory arbitrage, and quirks of history. Bank capital requirements, combined with the lack of strong or sometimes any capital requirements in the nonbank sector, are part of that.

We should monitor the migration of activities from banks to the nonbank sector carefully, but we shouldn't lower bank capital requirements in a race to the bottom. In times of stress, banks serve as central sources of strength to the economy, and they need capital to do so.

We need to worry, a lot, about nonbank risks to financial stability. During the Global Financial Crisis, many nonbank financial firms had woefully inadequate capital and liquidity, engaged in high-risk activities, and were faced with devastating runs that crushed the financial system and caused enormous harm to households and businesses.

The collapse of Bear Stearns and Lehman Brothers, the failure of Fannie Mae and Freddie Mac, the implosion of the insurance conglomerate AIG, and many others, laid bare the weakness of nonbank intermediation, and the need to regulate risks outside the banking system.

Many of those risks remain today. In far too many cases, nonbanks rely on funding sources that are prone to runs and do not maintain sufficient capital to internalize their risks to society.

The answer, however, is not lower capital requirements for banks, but more attention to those very risks. Further, as stress in nonbank financial markets is often transmitted to the banking system, both directly and indirectly, it is critical that banks have enough capital to remain resilient to those stresses.

Calibration of Bank Capital Requirements

One of the threshold questions is how should we think about calibrating bank capital to a socially optimal level? There is not an easy answer to that question. In my mind, as I said at the outset, it starts with humility.

Bank capital should be sufficient to enable the bank to absorb unexpected losses and continue operations through severely stressful but plausible events. Yet translating that principle into a quantum of capital involves an estimate of what future risks will emerge and what losses banks will suffer. I'm skeptical that regulators—or bank managers—know the answers to these questions.

Despite complex regulatory risk-weights, or simple leverage ratios, or the internal models used by banks, at bottom bank capital ought to be calibrated based on that humility, that skepticism.

Capital provides a cushion against unexpected risks and unforeseen losses, those a humble and skeptical person might be careful to not try to predict with too much precision. Those a humble and skeptical person might guard against.

That is the spirit in which I am approaching the Fed's holistic review of capital standards. There is a body of empirical and theoretical research on optimal capital, which attempts to determine the level of capital that equalizes the marginal benefits of capital with the marginal costs.

While the estimates vary widely, and are highly contingent on the assumptions made, the current U.S. requirements are toward the low end of the range described in most of the research literature.

International comparisons also suggest strong capital requirements support banks and the U.S. economy. We have strong capital levels today, and generally higher bank capital requirements in the United States after the Dodd-Frank Act have corresponded with healthy economic growth and have supported the competitiveness of U.S. firms in the global economy.

Finally, some banks have asserted that the resilience of the banking system in the pandemic suggests that bank capital is already high enough. There were some positive signs from a Federal Reserve-conducted sensitivity analysis and subsequent stress test.

Banks did their part and lent strongly, based on their strong capital positions and widespread government support. But we didn't get a real test of resilience because Congress, the President, and the Federal Reserve rightly stepped in with massive assistance to avert an economic disaster.

Furthermore, I'd observe that the recent experience of the pandemic suggests that large, unexpected shocks can occur with little notice. Our inability to predict such events would argue for a higher overall capital level than one based solely on historical experience.

So let me return to where I began on this topic: figuring out the right level of capital requires one to be humble and skeptical.

To read more:
https://www.federalreserve.gov/newsevents/speech/barr20221201a.htm

Number 3

International cooperation in a world of digitalisation

Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, at the 22nd International Conference of Banking Supervisors

Introduction

Good morning, good afternoon and good evening. Welcome to the 22nd International Conference of Banking Supervisors (ICBS).

This is the second ICBS that we have held in virtual format, following the outbreak of Covid-19 in 2020. I am pleased to see that over 450 participants from about 90 jurisdictions are taking part in this year's event.

We have seen profound changes over just the past few years, and many more since the first ICBS in July 1979. The banking system is now much bigger and more interconnected. By one measure, total banking assets have grown by almost 4,000%.

Foreign bank claims have more than doubled, now totalling almost $34 trillion, which is equivalent to more than a third of world GDP.

Cross-border links between banks and other financial institutions now stand at $7.5 trillion.

We have also endured more than 50 systemic banking crises during this period, a stark reminder of the critical importance of prudent regulation and robust supervision.

Despite these changes, the ICBS – which exists to promote supervisory cooperation within the international banking supervisory community – has stood the test of time.

A common thread throughout the previous 21 conferences has been the commitment by central banks and supervisory authorities to collaborate and cooperate with the aim of strengthening the resilience of the global banking system and safeguarding financial stability.

Looking ahead, the need for global cooperation is perhaps more important than ever. We face a highly uncertain outlook, with no shortage of risks facing the global banking system. Stagflationary forces, rising interest rates, and high levels of public and private debt are keeping central banks and supervisors busy.

Geopolitical developments continue to shape the economic trajectory. Major structural changes are shaping the future of banking system, including climate-related financial risks; the growth of non-bank financial intermediation; and perhaps one of the most significant – and the theme of this year's ICBS – the digitalisation of finance.

Indeed, we are seeing profound technological advancement and innovation. Since the first ICBS, the speed of the fastest supercomputer has risen exponentially from roughly 1 million to over 400 quadrillion computations per second today.

Moore's Law is still delivering impressive improvements, with the number of transistors on microchips now exceeding 100 billion, a percentage increase of almost 4 million from 1979.

So it is fitting that we will be spending the next three days discussing financial technology and its implications for banks and banking supervision.

What are the opportunities and challenges posed by new technologies for banks and supervisors? How should supervision adapt to digital innovation and the emergence of new services and business models? And, perhaps most existentially, what does it mean to be a "bank" in 2022?

I will not try to provide a definitive answer these all of these questions – we will benefit from the views of a wide and diverse range of speakers over the coming days.

But let me provide a first approach to our debate during the next few days, I will focus my remarks on three broad financial stability implications resulting from the current wave of financial digitalisation, namely the impact on banks' business models, the risks from an ever-more pervasive use of digital services, and the emergence of new interconnections in the global financial system.

All three observations, underline the critical importance of cooperation among central banks and supervisory authorities in overseeing the structural changes brought about by technological innovations, reaping their benefits, and mitigating the risks they pose to global financial stability.

Digitalisation and financial stability: benefits and challenges

Finance and technology have a long and symbiotic relationship. Bankers have been applying technology for more than 150 years. Finance started to shift from analogue to digital as soon as the transatlantic telegraph cable was completed in 1866.

A second wave of technological innovations in financial services began with the advent of the automated teller machine in 1967. Yet the most recent technological breakthroughs in payment systems, digital banking services and data analytics stand out for their pace and scale.

So what does the current digitalisation of finance mean for global financial stability? What opportunities does it present for consumers and banks? What are the risks? And what does it mean for supervisors?

The Committee is conducting a series of thematic studies on the impact of various technological innovations for banks and supervisors to help answer these questions. This work is ongoing, but let me offer a few personal observations.

To read more: https://www.bis.org/speeches/sp221129.pdf

Number 4

PCAOB Launches Technology Innovation Alliance Working Group

Led by Board Member Ho, expert panel will advise Board on impact of emerging technologies and provide recommendations for PCAOB oversight

The Public Company Accounting Oversight Board (PCAOB) announced the formation of the Technology Innovation Alliance (TIA) Working Group, a group of external professionals with expertise in emerging technologies, including such technologies used by financial statement preparers and auditors.

TIA Working Group Members

Taka Ariga	Luciana Barbosa	Helen Brown-Liburd
Eric Cohen	Chris Danusiar	Evelyn Hayes
Renata Miskell	Vernon Richardson	John Turner
Andres Vinelli		

Chaired by Board Member Christina Ho, the TIA Working Group will serve two primary functions:

1. Advise the Board on the use of emerging technologies by auditors and preparers relevant to audits and their potential impact on audit quality; and

2. Make recommendations to the Board regarding how the Board's existing or future oversight programs might address the use of emerging technologies by auditors and preparers.

"It is critical for the PCAOB to remain current on technological advancements and their role in enhancing audit quality," said PCAOB Chair Erica Y. Williams.

"On behalf of the Board and all my PCAOB colleagues, I thank the experts who have stepped up to provide us perspective on technology by serving on the TIA Working Group and Board Member Ho for leading this talented group of individuals."

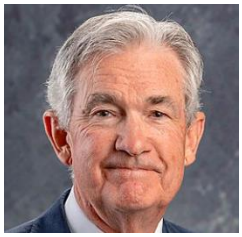
“As a regulator, we have a duty to be forward-thinking when evaluating the impact of technology and data on the future of auditing,” said Board Member Ho. “This impressive group of experts will help us look ahead from a range of perspectives.”

You may visit:
https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-launches-technology-innovation-alliance-working-group

Number 5

Inflation and the labor market

Jerome H Powell, Chair of the Board of Governors of the Federal Reserve System, at the Hutchins Center on Fiscal and Monetary Policy, Brookings Institution, Washington DC.

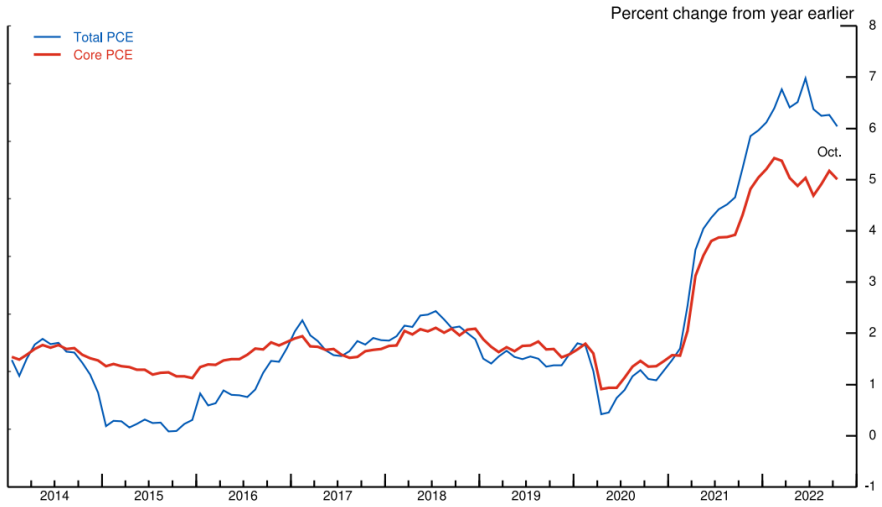


Today I will offer a progress report on the Federal Open Market Committee's (FOMC) efforts to restore price stability to the U.S. economy for the benefit of the American people.

The report must begin by acknowledging the reality that inflation remains far too high. My colleagues and I are acutely aware that high inflation is imposing significant hardship, straining budgets and shrinking what paychecks will buy. This is especially painful for those least able to meet the higher costs of essentials like food, housing, and transportation.

Price stability is the responsibility of the Federal Reserve and serves as the bedrock of our economy. Without price stability, the economy does not work for anyone. In particular, without price stability, we will not achieve a sustained period of strong labor market conditions that benefit all.

Figure 1. Total and core PCE inflation



Note: October data are estimates based on October data from the consumer price index and the producer price index. PCE is personal consumption expenditures.

Source: Bureau of Economic Analysis; Bureau of Labor Statistics; staff estimates.

We currently estimate that 12-month personal consumption expenditures (PCE) inflation through October ran at 6.0 percent (figure 1).

While October inflation data received so far showed a welcome surprise to the downside, these are a single month's data, which followed upside surprises over the previous two months.

As figure 1 makes clear, down months in the data have often been followed by renewed increases. It will take substantially more evidence to give comfort that inflation is actually declining.

By any standard, inflation remains much too high. For purposes of this discussion, I will focus my comments on core PCE inflation, which omits the food and energy inflation components, which have been lower recently but are quite volatile.

Our inflation goal is for total inflation, of course, as food and energy prices matter a great deal for household budgets. But core inflation often gives a more accurate indicator of where overall inflation is headed.

Twelve-month core PCE inflation stands at 5.0 percent in our October estimate, approximately where it stood last December when policy tightening was in its early stages. Over 2022, core inflation rose a few tenths above 5 percent and fell a few tenths below, but it mainly moved sideways. So when will inflation come down?

I could answer this question by pointing to the inflation forecasts of private-sector forecasters or of FOMC participants, which broadly show a significant decline over the next year. But forecasts have been predicting just such a decline for more than a year, while inflation has moved stubbornly sideways.

The truth is that the path ahead for inflation remains highly uncertain. For now, let's put aside the forecasts and look instead to the macroeconomic conditions we think we need to see to bring inflation down to 2 percent over time.

For starters, we need to raise interest rates to a level that is sufficiently restrictive to return inflation to 2 percent. There is considerable uncertainty about what rate will be sufficient, although there is no doubt that we have made substantial progress, raising our target range for the federal funds rate by 3.75 percentage points since March.

As our last postmeeting statement indicates, we anticipate that ongoing increases will be appropriate. It seems to me likely that the ultimate level of

rates will need to be somewhat higher than thought at the time of the September meeting and Summary of Economic Projections. I will return to policy at the end of my comments, but for now, I will simply say that we have more ground to cover.

We are tightening the stance of policy in order to slow growth in aggregate demand. Slowing demand growth should allow supply to catch up with demand and restore the balance that will yield stable prices over time. Restoring that balance is likely to require a sustained period of below-trend growth.

To read more:
https://www.federalreserve.gov/newsevents/speech/powell20221130a.htm

Number 6

The European Climate Law and the European Central Bank

Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, Lustrum Symposium organised by Dutch Financial Law Association

I am honoured to speak at this 20th anniversary dinner, with so many distinguished lawyers around me. In this setting, I feel quite comfortable dwelling on legal issues for a while.

A topic close to my heart – apart from the law – is the ongoing climate and environmental crises. I am glad that we have long since moved on from the time when only scientists and activists were concerned with this topic.

It is now high on policymakers' agendas, as we saw at the recent United Nations Conference of Parties (COP27) at Sharm el-Sheikh, at which – along with world leaders and a wide range of policymakers and interest groups – the ECB was also represented.

I was struck by one story in particular. The tiny Pacific nation of Vanuatu is badly exposed to cyclones and rising sea levels. To the inhabitants of Vanuatu, climate change is a human rights issue. And, as Vanuatu's president, Nikenike Vurobaravu, stated, "we are measuring climate change not in degrees of Celsius or tonnes of carbon, but in human lives."

Vanuatu now plans to ask the UN General Assembly to seek an opinion from the International Court of Justice on the human rights implications of the climate crisis. That opinion could determine the rights of countries most exposed to climate change. It could also touch on the obligations of those most responsible for driving the climate crisis.

Let's now focus on Europe and the possible implications of these developments in international law for my own institution, the ECB. Under the Paris Agreement adopted at COP21 in 2015, many countries committed to the long-term goal of holding the increase in the global average temperature to well below 2°C above pre-industrial levels.

To fulfil its commitment as one of parties to the Paris Agreement, the EU last year adopted the European Climate Law. The implications of the Climate Law are significant. Before going into why, let me first explain what the Climate Law does.

The Climate Law has three key elements. The first is its objective that the EU reduce its greenhouse gas emissions by at least 55% by 2030, with a new reduction target to be set for 2040. The EU should achieve climate neutrality by 2050 and aim to achieve negative emissions thereafter. The second important element is to ensure that we move towards that objective.

The European Commission has established a framework for assessing concrete progress and checking whether national and Union measures are consistent with the objective. It will issue regular reports on the conclusions of these assessments.

The third and last element is to ensure that we use the most effective instruments to achieve the objective. The introduction of a European Scientific Advisory Board on Climate Change promotes the idea that all policies should be based on up-to-date scientific insights.

It is hard to overstate the importance of the Climate Law. The EU is setting the bar high. Allow me to quote what the law says about the transition to climate neutrality.

It "requires changes across the entire policy spectrum and a collective effort of all sectors of the economy and society [...] all relevant Union legislation and policies need to be consistent with, and contribute to, the fulfilment of the climate-neutrality objective while respecting a level playing field".

We are starting to see this happen. From housing to energy and from transport to finance, the EU is introducing reforms to put Europe on track to become the first climate-neutral continent by 2050.

So how will the Climate Law affect the ECB? For me, as a member of the ECB's Executive Board and the Vice-Chair of its Supervisory Board, this question is relevant to both our monetary policy and banking supervision tasks.

This question matters because, in the field of the environment, the ECB is a policy taker, not a policymaker. So what does the ECB need to take from the policy and objectives reflected in the Climate Law? To answer this, we first need to consider whether the ECB is bound by the Climate Law. If so, the ECB would have to take measures towards achieving the climate-neutrality objective.

There is more, though. If the ECB is bound by the law, it would also have to ensure continuous progress in enhancing adaptive capacity, strengthening resilience and reducing vulnerability to climate change. Moreover, it would have to ensure that its policies on adaptation are coherent with and supportive of other such policies in the Union.

To read more:
https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp221201_1~435e6ea81a.en.html

Number 7

Pairing up Cybersecurity and Data Protection Efforts: EDPS and ENISA sign Memorandum of Understanding

The European Data Protection Supervisor (EDPS) and the European Union Agency for Cybersecurity (ENISA) sign a Memorandum of Understanding (MoU) which establishes a strategic cooperation framework between them.

Both organisations agree to consider designing, developing and delivering capacity building, awareness-raising activities, as well as cooperating on policy related matters on topics of common interest, and contributing to similar activities organised by other EU institutions, bodies, offices and agencies (EUIBAs).

Wojciech Wiewiórowski, EDPS, said: "Today's MoU formalises the EDPS and ENISA's cooperation, which has been ongoing for several years. The document establishes strategic cooperation to address issues of common concern, such as cybersecurity as a way of protecting individuals' personal data. Cybersecurity and data protection go hand in hand and are two essential allies for the protection of individuals and their rights. Privacy-enhancing technologies are a good example of this."

Juhan Lepassaar, ENISA Executive Director, said: "The Memorandum of Understanding between EDPS and ENISA will allow us to address cybersecurity and privacy challenges in a holistic manner and assist EUIBAs in improving their preparedness."

Memorandum of Understanding on increasing cooperation between the European Data Protection Supervisor and the European Union Agency for Cybersecurity

I. Preamble

1. This document is a Memorandum of Understanding setting out the principles for increased cooperation between:

• The European Data Protection Supervisor (EDPS), established by Regulation (EU) 2018/17251 of the European Parliament and of the Council , represented for the purposes of signature of this Memorandum of Understanding by the European Data Protection Supervisor, Mr Wojciech Wiewiórowski; and

• The European Union Agency for Cybersecurity (ENISA), established by Regulation (EU) 2019/8812, of the European Parliament and of the Council , represented for the purposes of signature of this Memorandum of Understanding by its Executive Director, Mr Juhan Lepassaar;

2. Under Article 52 of Regulation (EU) 2018/1725, the EDPS is the independent supervisory authority responsible, with respect to the processing of personal data, for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection are respected by the Union institutions, bodies, offices and agencies.

3. Under Title II of Regulation (EU) 2019/881, ENISA is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. The Agency acts as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders.

II. Purpose

4. This Memorandum of Understanding has been agreed in recognition of the common interest of EDPS and ENISA to cooperate more in areas of mutual interest. Building on earlier exchanges, it aims to establish, define and promote a structured cooperation in accordance with and subject to their respective statutory tasks and powers under Union law.

5. This Memorandum of Understanding does not affect in any way the tasks and powers of the EDPS as a supervisor of the processing of personal data by ENISA as an EU Agency, nor does it affect in any way the duties of ENISA as a data controller or data processor under Regulation (EU) 2018/1725 and as an independent Agency under Regulation (EU) No 2019/881. This Memorandum of Understanding does not impact activities and duties that either party carries out under Union law.

III. Strategic Cooperation

6. EDPS and ENISA agree to establish a strategic cooperation in areas of common interest with a view to addressing issues of common concern such as cybersecurity aspects of personal data protection.

7. EDPS and ENISA agree to put forward a strategic plan on promoting awareness, capacity, cyber-hygiene and privacy and data protection stand of institutions, bodies, offices and agencies of the Union.

This strategic plan will aim to promote a joint approach to cybersecurity aspects of data protection as well as to the adoption of privacy enhancing

technologies, and strengthen the capacities and skills of the aforementioned institutions, bodies, offices and agencies of the Union. Further element useful to establish the strategic plan are defined in Annex A.

8. As part of the strategic plan, EDPS and ENISA agree to consider designing, developing and delivering capacity building and awareness raising activities in areas of common interest and contributing jointly to similar activities organised by other bodies.

Within the scope of each activity, EDPS and ENISA will address aspects within their area of expertise.

9. EDPS and ENISA aim to meet at least once a year to review matters related to the strategic plan, to identify further areas of cooperation, and in order to exchange views on main current and forthcoming challenges for cybersecurity and privacy and data protection, including security of personal data processing and management of personal data breaches, data protection by design and by default and privacy by design, privacy enhancing technologies and privacy engineering and as well as analyses of emerging technologies, foresight methods and topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations.

10. EDPS and ENISA agree to appoint a single contact point responsible for coordinating their cooperation and for consulting each other on a regular basis, particularly with regard to the terms of this Memorandum of Understanding.

11. EDPS and ENISA agree to exchange the contact details of the contact points and to inform each other without undue delay in writing of any change concerning the contact points.

Memorandum of Understanding on increasing cooperation between the European Data Protection Supervisor and the European Union Agency for Cybersecurity

To read more:
https://edps.europa.eu/system/files/2022-11/22-11-30_edps_enisa_mou_en.pdf

https://www.enisa.europa.eu/news/pairing-up-cybersecurity-and-data-protection-efforts-edps-and-enisa-sign-memorandum-of-understanding

Number 8

Mega - Event Sports Diplomacy: A Strategic Communications Perspective

Una Aleksandra Bērziņa Čerenkova

Introduction and methodology description

International sports competitions have perhaps the second most widespread and normalised use of national flags and symbols after the military. Undoubtedly, sport—both in terms of athlete accomplishments and sporting events organisation—are a source of reputation for a country.

Nations use sport to tell stories of their role in fostering achievers, winners, overcomers, and even triumphant underdogs. International sporting events are drama-laden displays of national unity and purpose.

Sport is increasingly featured in national strategic documents pertaining to public diplomacy. Different in size, form, and vision, the documents nonetheless demonstrate that there is a certain strategic communications approach to sport, which might point to high soft power value.

Using both the strategies and the communication surrounding mega sports events, this report aims to analyse and compare the national strategic communications messaging—what stories nations tell, and how they position themselves externally.

This research adopts the NATO Strategic Communications Centre of Excellence definition: ‘Strategic communications encompass multiple elements of public diplomacy, political marketing, persuasion, international relations, military strategy, and many others.

Strategic communications [are] a holistic approach to communication, based on values and interests, that encompasses everything an actor does to achieve objectives, in a contested environment.’

Building on Michelsen and Woodier’s research specifically on Olympic strategic communications, the strategic communications aspect of sports diplomacy is defined here as sport-related planned interventions into the

information environment, 'with observable effects on that environment, which serve international political ends'.

Nation	Message on values	Message on athletes	Message on mega sports events	Strategic communications examples
Australia	The healthy sporting nation. Sport for regional development. Benefits for national economy.	Inclusivity and diversity.	Expertise of organising mega sports events is shared with other nations.	N/A
Japan	Improving international competition levels. Peace and development. The Olympic spirit. Health.	Talent fostering. Equality and inclusion.	Responsible legacy management (1964-2020 and beyond). Gaining recognition for Japanese sport. Hi-tech games.	Tradition plus future. Linking the 2020 Olympics with earthquake recovery. Heavy focus on commemorations.

Nation	Message on values	Message on athletes	Message on mega sports events	Strategic communications examples
China	Great rejuvenation of the Chinese nation. Shared future for mankind. Multipolarity. Friendship. Belt and Road.	N/A	Volunteering. Ecology. Olympic spirit. Welcoming, guest-loving nation.	Xi Jinping's thought ('Community with a Shared Future for Mankind'). Green and clean winter Olympics. Targeted override of #genocidegames. Praise of zero COVID19 policy.
Russia	Russian traditional values. The healthy sporting nation.	Tradition of excellence. No to bad sportsmanship. No to doping.	Ensuring the highest level of hosting. No to politics in sport. Legacy management (infrastructure, economic, social development).	#WeWillROCYou (at Beijing Winter Olympics)

In both 2021 and 2022, the world experienced the Olympic Games despite the global COVID 19 pandemic. With no lack of critical voices and opinions related to the negative benefit-to-cost ratio , two Asian cities, Tokyo and Beijing, nevertheless decided that the show must go on for these mega sports events.

How come? ‘It is precisely the reach of mega sports events, such as the Olympic Games and the World Cup, which attracts a range of actors to seek to utilise them to achieve their diplomatic goals’.

To read more:
https://stratcomcoe.org/publications/mega-event-sports-diplomacy-a-strategic-communications-perspective/254

Number 9

NIST Finds a Sweet New Way to Print Microchip Patterns on Curvy Surfaces

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST scientist Gary Zabow had never intended to use candy in his lab. It was only as a last resort that he had even tried burying microscopic magnetic dots in hardened chunks of sugar — hard candy, basically — and sending these sweet packages to colleagues in a biomedical lab. The sugar dissolves easily in water, freeing the magnetic dots for their studies without leaving any harmful plastics or chemicals behind.

By chance, Zabow had left one of these sugar pieces, embedded with arrays of micromagnetic dots, in a beaker, and it did what sugar does with time and heat — it melted, coating the bottom of the beaker in a gooey mess.

“No problem,” he thought. He would just dissolve away the sugar, as normal. Except this time when he rinsed out the beaker, the microdots were gone. But they weren’t really missing; instead of releasing into the water, they had been transferred onto the bottom of the glass where they were casting a rainbow reflection.

“It was those rainbow colors that really surprised me,” Zabow recalls. The colors indicated that the arrays of microdots had retained their unique pattern.

This sweet mess gave him an idea. Could regular table sugar be used to bring the power of microchips to new and unconventional surfaces? Zabow’s findings on this potential transfer printing process were published in Science in its Nov. 25 issue.

Semiconductor chips, micropatterned surfaces, and electronics all rely on microprinting, the process of putting precise but minuscule patterns millionths to billionths of a meter wide onto surfaces to give them new properties. Traditionally, these tiny mazes of metals and other materials are printed on flat wafers of silicon. But as the possibilities for semiconductor chips and smart materials expand, these intricate, tiny patterns need to be printed on new, unconventional, non-flat surfaces.

Directly printing these patterns on such surfaces is tricky, so scientists transfer prints. There are flexible tapes and plastics that can do the job (like using putty to pick up newsprint), but these solids can still have trouble

conforming to sharp curves and corners when the print is laid back down. They could also leave behind plastics or other chemicals that could be hard to remove or be unsafe for biomedical uses.

There are liquid techniques, where the transfer material is floated on the surface of water and the target surface is pushed through it. But that can be tricky too; with a freely flowing liquid it can be hard to place the print precisely where you want it on a new surface.

But, as Zabow discovered to his surprise, a simple combination of caramelized sugar and corn syrup can do the trick.

When dissolved in a small amount of water, this sugar mixture can be poured over micropatterns on a flat surface. Once the water evaporates, the candy hardens and can be lifted away with the pattern embedded. The candy with the print is then placed over the new surface and melted. The sugar/corn syrup combination maintains a high viscosity as it melts, letting the pattern maintain its arrangement as it flows over curves and edges. Then, using water, the sugar can be washed away, leaving just the pattern behind.

Using this technique, called REFLEX (REflow-driven FLExible Xfer), microcircuit patterns could be transferred like a stencil to allow scientists or manufacturers to etch and fill the materials they need in the right places.

Or, patterned materials could be transferred from their original chip onto fibers or microbeads for potential biomedical or microrobotics studies, or over sharp or curved surfaces within new devices.

The technique proved successful for a large range of surfaces, including printing onto the sharp point of a pin, and writing the word “NIST” in microscale gold lettering onto a single strand of human hair.

In another example, 1-micrometer-diameter magnetic disks were successfully transferred onto a floss fiber of a milkweed seed. In the presence of a magnet, the magnetically printed fiber reacted, showing the transfer had worked.

There’s still more to explore with REFLEX, but this process could open new possibilities for new materials and microstructures across fields from electronics to optics to biomedical engineering.

“The semiconductor industry has spent billions of dollars perfecting the printing techniques to create chips we rely on,” Zabow says. “Wouldn’t it be

nice if we could leverage some of those technologies, expanding the reach of those prints with something as simple and inexpensive as a piece of candy?"

You may visit:
https://www.nist.gov/news-events/news/2022/11/nist-finds-sweet-new-way-print-microchip-patterns-curvy-surfaces

Number 10

U.S. Cyber Command, DARPA Initiate Rapid Cyber Capability Prototyping and Integration Pilot

Constellation aims to accelerate maturation of tactical and strategic cyber capabilities, efficiently integrate them into operational warfighting platforms

The United States Cyber Command (CYBERCOM) and DARPA are kicking off a pilot program aimed at getting new cyber capabilities into the hands of cyber operators faster.

Known as Constellation, the pilot program will enable the flow of new cyber capabilities resulting from high-risk, high-reward cyber science and technology (S&T) research by creating a user-directed, incremental, and iterative pipeline to accelerate the creation, proving, adoption, and delivery of those capabilities into CYBERCOM's software ecosystem.

"Innovation is core to the command's strategy, which is why CYBERCOM and DARPA are working more closely than ever to mature emerging tactical and strategic cyber capabilities, and integrate them into operational warfighting platforms," said Mike Clark, Director of Cyber Acquisition & Technology at U.S. Cyber Command. "Success for Constellation means increasing the speed of transition from DARPA research and development to CYBERCOM for operational use."

In the research and development community, the "valley of death" is a metaphor commonly used to describe the most difficult phase of transitioning a prototype to an operational capability.

Fostering an agile-style pipeline from research to operations becomes essential to addressing the challenges the Department of Defense faces when developing software systems, such as rapidly evolving technology and acceptance and usability for both expert and non-expert providers.

Constellation will provide a framework and create mechanisms to provide virtual and physical infrastructure, people and contracts, sustainment of relationships required to bridge the gap between science and technology, research, development, and operational warfighting capabilities, and feedback to the S&T community regarding evolving cyber threats and mission needs.

"To have the greatest operational and strategic impact, these emergent capabilities must reach operators continuously in short timescales, much

shorter than legacy acquisition processes," said Dr. Kathleen Fisher, director of DARPA's Information Innovation Office. "We are optimistic about Constellation's potential to enable long-term sustainment for rapid cyber capability prototyping and integration. Running Constellation projects in parallel with DARPA development can help us reduce risks and transition timelines and overcome the 'valley of death.'"

To read more: https://www.darpa.mil/news-events/2022-11-28

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 individual or entity;

- should not be relied on in the 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 regarding such problems incurred because of using this site or any linked external sites.

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.

You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),

- a Certified Information Systems Risk and Compliance Professional (CISRCP),

- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,

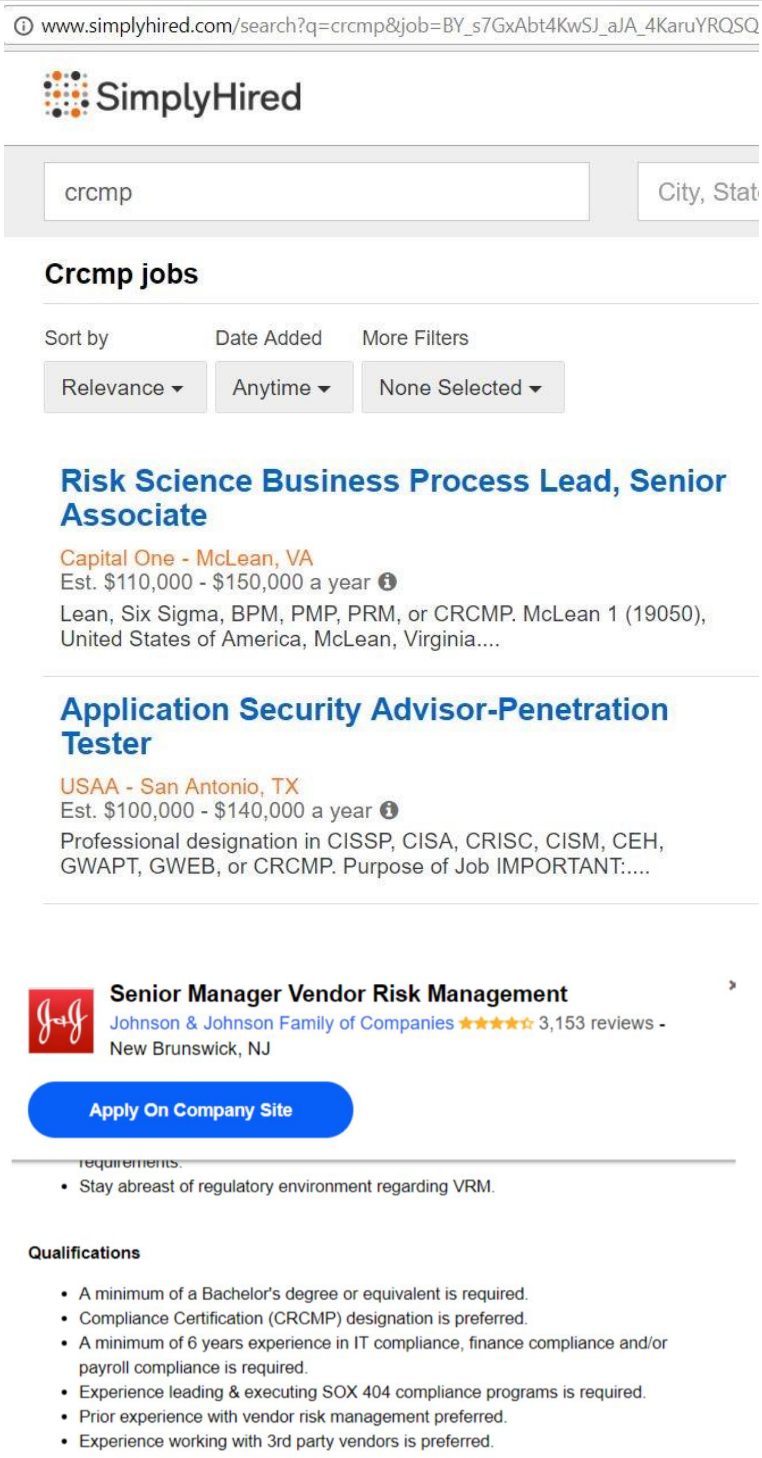
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program ($148 instead of $297).

You have a $100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for $297, and then purchase the CISRCP program for $197 (instead of $297), the CC(GRC)P program for $197 (instead of $297), the CRCMP(Re)I program for $197 (instead of $297), and the TSecTPro program for $197 (instead of $297).

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