International Association of Hedge Funds Professionals (IAHFP)
1200 G Street NW Suite 800 Washington DC 20005-6705 USA
Tel: 202-449-9750 Web: www.hedge-funds-association.com

Hedge Funds News, October 2022

Dear members and friends,

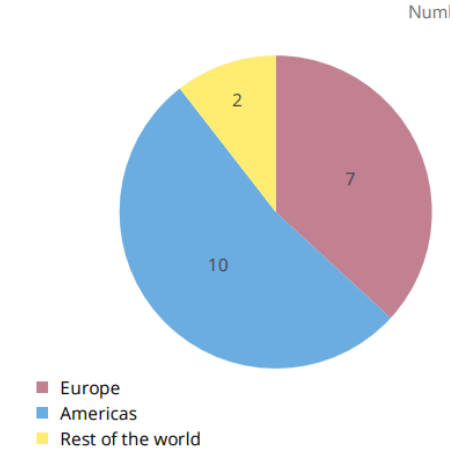
Since 2018, the Basel Committee has been pursuing a multi-pronged set of analytical, supervisory and policy initiatives related to *cryptoassets*.

As part of this work, a new cryptoasset data collection template was introduced starting with the current Basel III monitoring exercise based on end-2021 data. The template was specifically designed to support the Committee's two consultative documents on the prudential treatment of banks' cryptoasset exposures, which were published on 10 June 2021 and 30 June 2022.

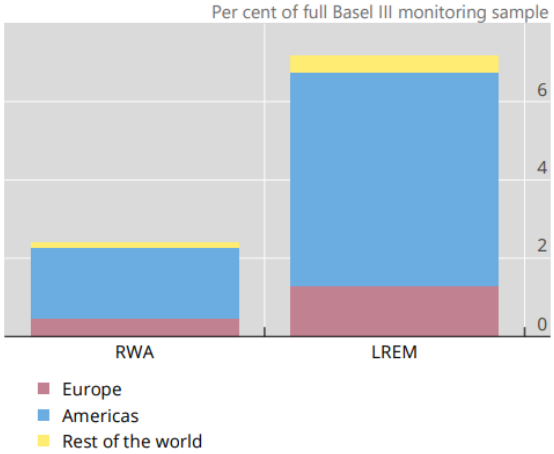
It collects granular information on banks' holdings of cryptoassets, including information at the level of individual cryptoassets. This special feature provides some analysis on banks' exposures to cryptoassets based on the data collected. Overall, 19 banks submitted cryptoasset data – 10 from the Americas, seven from Europe and two from the rest of the world (Graph , left panel).

A small proportion of banks reported crypto exposures at end-2021 Graph 1

Number of banks reporting cryptoasset exposures[1]



Proportion of banks reporting crypto exposures[2]

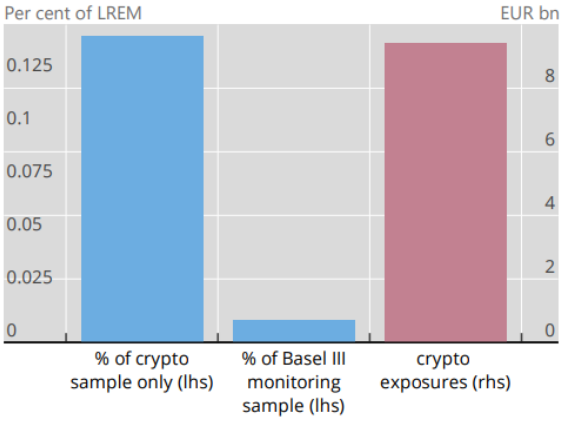


[1] All reporting banks are Group 1 banks, except for three Group 2 banks. Two Group 2 banks participated only in the crypto exercise and did not participate in the wider Basel III monitoring exercise. [2] The denominators used also account for the amounts of the two Group 2 banks which only participate in the crypto exercise and are not included in the general analysis of the Basel III monitoring exercise.

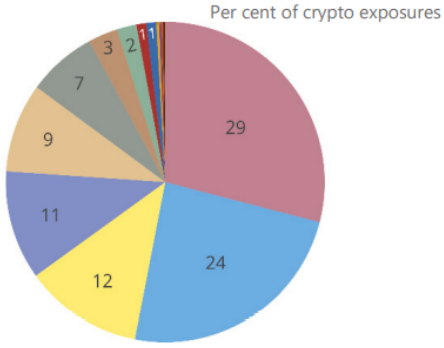
Source: BCBS end-2021 data collection and Secretariat calculations.

Crypto exposures are relatively small and unevenly distributed across banks Graph 2

Reported crypto exposures



Distribution of total crypto exposures across banks[1]



[1] Each slice represents one of the banks which reported crypto exposures.

Source: BCBS end-2021 data collection and Secretariat calculations.

All reporting banks are Group 1 banks, except for three Group 2 banks (of these, two Group 2 banks do not participate in the wider Basel III monitoring exercise and appear to specialise in cryptoassets).

These banks make up a relatively small part of the wider sample of 182 banks considered in the Basel III monitoring exercise – 2.4% of total RWA, and 7.2% of overall leverage ratio exposure measure (LREM) (Graph 1, right panel), with banks from the Americas contributing to approximately three quarters of these amounts.

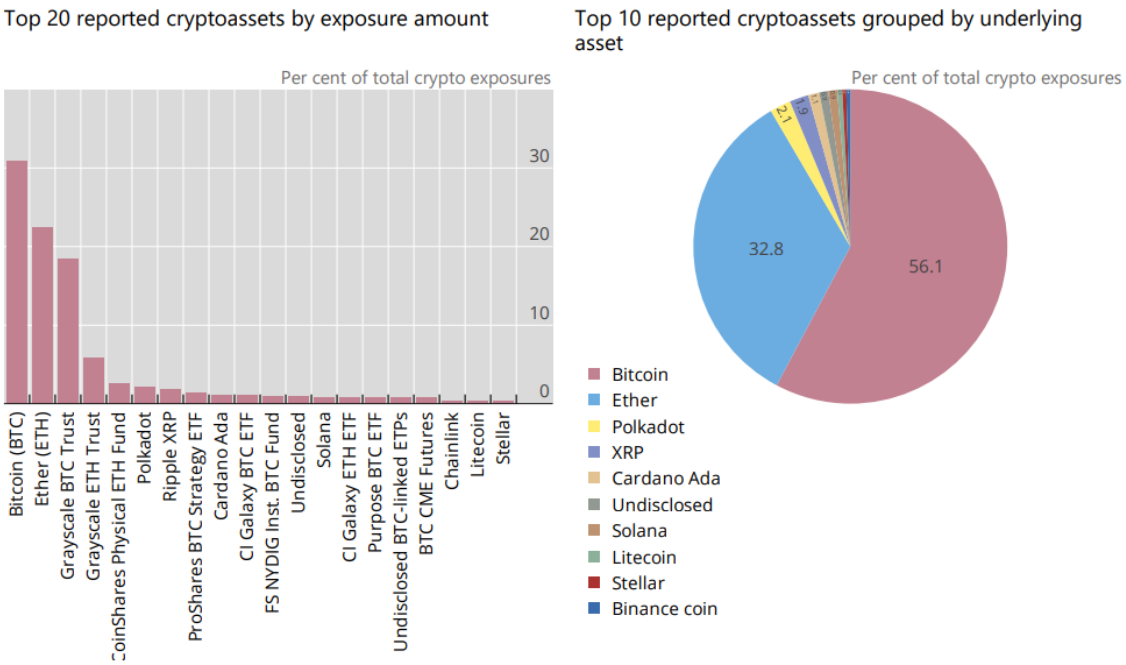
As this is the first data collection using the new template, the results in this special feature are subject to a number of data quality caveats and potential biases.

As the cryptoasset market is fast evolving, it is difficult to ascertain whether some banks have under- or over-reported their exposures to cryptoassets, and the extent to which they have consistently applied the same approach to classifying any exposures.

As such, while they are helpful in providing a broad indication of banks' cryptoasset activity, they should interpreted with a degree of caution.

Bitcoin, Ether and related cryptoassets make up the vast majority of crypto exposures

Graph 3



Source: BCBS end-2021 data collection and Secretariat calculations.

Overall amounts

Total cryptoasset exposures reported by banks amount to approximately €9.4 billion. In relative terms, these exposures make up only 0.14% of total exposures on a weighted average basis across the sample of banks reporting cryptoasset exposures.

When considering the whole sample of banks included in the Basel III monitoring exercise (ie also those that do not report cryptoasset exposures), the amount shrinks to 0.01% of total exposures (Graph 2, left panel).

Cryptoasset exposures are distributed unevenly across reporting banks, with two banks making up more than half of overall cryptoasset exposures, and four more banks making up just below 40% of the remaining exposures (Graph 2, right panel).

Composition across cryptoassets

Reported cryptoasset exposures are primarily composed of Bitcoin (31%), Ether (22%) and a multitude of instruments with either Bitcoin or Ether as the underlying cryptoassets (25% and 10% respectively).

Together, these make up almost 90% of reported exposures (Graph 3).

Focusing on the top 20 reported cryptoassets by exposure amount, other relatively significant reported cryptoassets include Polkadot (2% of reported exposures), Ripple XRP (2%), Cardano Ada (1%), Solana (1%), Litecoin (0.4%) and Stellar (0.4%).

These exposures would likely be classified as Group 2 cryptoassets under the current consultative proposal of the Basel Committee.

Banks also reported, in smaller amounts, a stablecoin (USD coin) and tokenised assets (not shown).

To read more: https://www.bis.org/bcbs/publ/d541_crypto.pdf

Federal Reserve Board announces that six of the largest banks will participate in a pilot climate scenario analysis exercise

The Federal Reserve Board has announced that six of the nation's largest banks will participate in a pilot climate scenario analysis exercise designed to enhance the ability of supervisors and firms to measure and manage climate-related financial risks.

Scenario analysis—in which the resilience of financial institutions is assessed under different hypothetical climate scenarios—is an emerging tool to assess climate-related financial risks, and there will be no capital or supervisory implications from the pilot.

The pilot exercise will be launched in early 2023 and is expected to conclude around the end of the year.

At the beginning of the exercise, the Board will publish details of the climate, economic, and financial variables that make up the climate scenario narratives.

Over the course of the pilot, participating firms will analyze the impact of the scenarios on specific portfolios and business strategies.

The Board will then review firm analysis and engage with those firms to build capacity to manage climate-related financial risks.

The Board anticipates publishing insights gained from the pilot at an aggregate level, reflecting what has been learned about climate risk management practices and how insights from scenario analysis will help identify potential risks and promote risk management practices.
No firm-specific information will be released.

Climate scenario analysis is distinct and separate from bank stress tests. The Board's stress tests are designed to assess whether large banks have enough capital to continue lending to households and businesses during a severe recession.

The climate scenario analysis exercise, on the other hand, is exploratory in nature and does not have capital consequences.
By considering a range of possible future climate pathways and associated economic and financial developments, scenario analysis can assist firms

and supervisors in understanding how climate-related financial risks may manifest and differ from historical experience.

The banks in the pilot exercise are:

- Bank of America,
- Citigroup,
- Goldman Sachs,
- JPMorgan Chase,
- Morgan Stanley,
- Wells Fargo.

In coming months, the Board will provide additional details on how the exercise will be conducted and the scenarios that will be used in the pilot.

The Financial Stability Oversight Council Releases Report on Digital Asset Financial Stability Risks and Regulation

FSOC

Note: The Financial Stability Oversight Council (FSOC or Council) was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). The purposes of the Council under the Dodd-Frank Act are:

(1) to identify risks to the financial stability of the United States that could arise from the material financial distress or failure, or ongoing activities, of large, interconnected bank holding companies or nonbank financial companies, or that could arise outside the financial services marketplace;

(2) to promote market discipline by eliminating expectations on the part of shareholders, creditors, and counterparties of such companies, that the Government will shield them from losses in the event of failure; and

(3) to respond to emerging threats to the stability of the United States (U.S.) financial system.

Executive Summary

Crypto-asset activities could pose risks to the stability of the U.S. financial system if their interconnections with the traditional financial system or their overall scale were to grow without adherence to or being paired with appropriate regulation, including enforcement of the existing regulatory structure.

The scale of crypto-asset activities has increased significantly in recent years. Although interconnections with the traditional financial system are currently relatively limited, they could potentially increase rapidly.

Participants in the cryptoasset ecosystem and the traditional financial system have explored or created a variety of interconnections. Notable sources of potential interconnections include traditional assets held as part of stablecoin activities.

Crypto-asset trading platforms may also have the potential for greater interconnections by providing a wide variety of services, including leveraged trading and asset custody, to a range of retail investors and traditional financial institutions. Consumers can also increasingly access crypto-asset activities, including through certain traditional money services

businesses. Some characteristics of crypto-asset activities have acutely amplified instability within the crypto-asset ecosystem.

Many crypto-asset activities lack basic risk controls to protect against run risk or to help ensure that leverage is not excessive.

Crypto-asset prices appear to be primarily driven by speculation rather than grounded in current fundamental economic use cases, and prices have repeatedly recorded significant and broad declines.

Many crypto-asset firms or activities have sizable interconnections with crypto-asset entities that have risky business profiles and opaque capital and liquidity positions.

In addition, despite the distributed nature of crypto-asset systems, operational risks may arise from the concentration of key services or from vulnerabilities related to distributed ledger technology.

These vulnerabilities are partly attributable to the choices made by market participants, including crypto-asset issuers and platforms, to not implement or refuse to implement appropriate risk controls, arrange for effective governance, or take other available steps that would address the financial stability risks of their activities.

Many nonbank firms in the crypto-asset ecosystem have advertised themselves as regulated.

Firms often emphasize money services business regulation, though such regulation is largely focused on anti-money laundering controls or consumer protection requirements and does not provide a comprehensive framework for mitigating financial stability vulnerabilities arising from other activities that may be undertaken, for example, by a trading platform or stablecoin issuer.

While some firms in the crypto-asset ecosystem have attempted to avoid the existing regulatory system, other firms have engaged with the existing regulatory system by obtaining trust charters or special state-level crypto-asset-specific charters or licenses.

Compliance with and enforcement of the existing regulatory structure is a key step in addressing financial stability risks. For example, certain crypto-asset platforms may be listing securities but are not in compliance with exchange or broker-dealer registration requirements.
In addition, certain crypto-asset issuers have offered and sold crypto-assets in violation of federal and state securities laws, because the offering and sale were not registered or conducted pursuant to an available exemption.

Regulators have taken enforcement actions over the past several years to address many additional instances of non-compliance with existing rules and regulations, including illegally offered crypto-asset derivatives products, false statements about stablecoin assets, and many episodes of fraud and market manipulation.

In addition, false and misleading statements, made directly or by implication, concerning availability of federal deposit insurance for a given product, are violations of the law, and have given customers the impression that they are protected by the government safety net when they are not.

Further, misrepresentations by crypto-asset firms about how they are regulated have also confused consumers and investors regarding whether a given crypto-asset product is regulated to the same extent as other financial products.

Though the existing regulatory system covers large parts of the crypto-asset ecosystem, this report identifies three gaps in the regulation of crypto-asset activities in the United States.

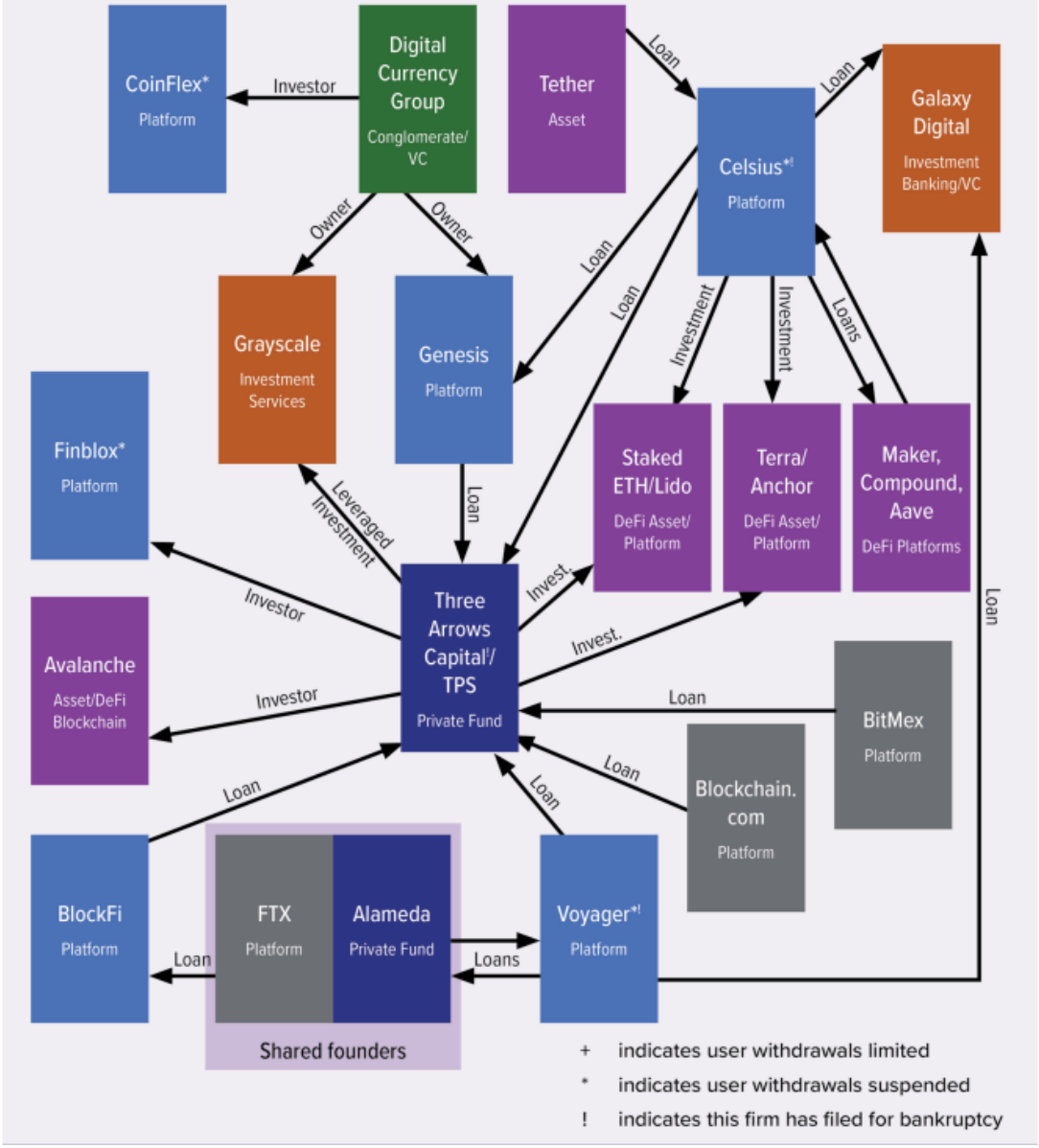
First, the spot markets for crypto-assets that are not securities are subject to limited direct federal regulation. As a result, those markets may not feature robust rules and regulations designed to ensure orderly and transparent trading, prevent conflicts of interest and market manipulation, and protect investors and the economy more broadly.

Second, crypto-asset businesses do not have a consistent or comprehensive regulatory framework and can engage in regulatory arbitrage. Some crypto-asset businesses may have affiliates or subsidiaries operating under different regulatory frameworks, and no single regulator may have visibility into the risks across the entire business.

Third, a number of crypto-asset trading platforms have proposed offering retail customers direct access to markets by vertically integrating the services provided by intermediaries such as broker-dealers or futures commission merchants. Financial stability and investor protection implications may arise from retail investors' exposure to certain practices commonly proposed by vertically integrated trading platforms, such as automated liquidation.

To ensure appropriate regulation of crypto-asset activities, the Council is making several recommendations in part 5 of this report, including the consideration of regulatory principles, continued enforcement of the existing regulatory structure, steps to address each regulatory gap, and bolstering member agencies' capacities related to crypto-asset data and expertise.

Figure B-1: Reported Interconnections of Three Arrows Capital



FSOC

FINANCIAL STABILITY OVERSIGHT COUNCIL

Report on Digital Asset Financial Stability Risks and Regulation

2022

The report: https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf

ESAs warn of rising risks amid a deteriorating economic outlook

The three European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) issued today their Autumn 2022 joint risk report.

JOINT COMMITTEE REPORT ON
RISKS AND VULNERABILITIES IN THE EU FINANCIAL SYSTEM
SEPTEMBER 2022

The report highlights that the deteriorating economic outlook, high inflation and rising energy prices have increased vulnerabilities across the financial sectors.

The ESAs advise national supervisors, financial institutions and market participants to prepare for challenges ahead.

The post-pandemic economic recovery in Europe has dwindled as a result of the Russian invasion of Ukraine.

Russia's war on Ukraine and the disruptions in trade caused a rapid deterioration of the economic outlook.

It adds to pre-existing inflationary pressures by strongly raising energy- and commodity prices, exacerbates imbalances in supply and demand, and weakens the purchasing power of households.

The risk of persistent inflation and stagflation has risen.

These factors, coupled with the deteriorated economic outlook, have significantly impacted the risk environment of the financial sector. Financial market volatility has increased across the board given high uncertainties.

After a long period of low interest rates, central banks are tightening monetary policy.

The combination of higher financing costs and lower economic output may put pressure on government, corporate and household debt refinancing while also negatively impacting the credit quality of financial institutions' loan portfolios.

The reduction of real returns through higher inflation could lead investors to higher risk-taking at a time when rate rises are setting in motion a far-reaching rebalancing of portfolios.

Financial institutions also face increased operational challenges associated with heightened cyber risks and the implementation of sanctions against Russia.

The financial system has to date been resilient despite the increasing political and economic uncertainty.

In light of the above risks and vulnerabilities, the Joint Committee of the ESAs advises national competent authorities, financial institutions and market participants to take the following policy actions:

Financial institutions and supervisors should continue to be prepared for a deterioration in asset quality in the financial sector and monitor developments including in assets that benefitted from temporary measures related to the pandemic and those that are particularly vulnerable to a deteriorating economic environment, to inflation as well as to high energy and commodity prices.

The impact of further increases in policy rates and of potential sudden increases in risk premia on financial institutions and market participants at large should be closely monitored.

Financial institutions and supervisors should closely monitor the impact of inflation risks.

Supervisors should continue to monitor risks to retail investors, in particular with regard to products where consumers may not fully realise the extent of the risks involved, such as crypto-assets.

Financial institutions and supervisors should continue to carefully manage environmental risks and cyber risks to address threats to information security and business continuity.

The report: https://www.eiopa.europa.eu/document-library/report/joint-committee-report-risks-and-vulnerabilities-eu-financial-system-1_en

BIS Working Paper No 1039

Cyber risk in central banking

by Sebastian Doerr, Leonardo Gambacorta, Thomas Leach, Bertrand Legros and David Whyte - Monetary and Economic Department

The rising number of cyber attacks in the financial sector poses a threat to financial stability and makes cyber risk a key concern for policy makers.

This paper presents the results of a survey among members of the Global Cyber Resilience Group on cyber risk and its challenges for central banks.

The survey reveals that central banks have notably increased their cyber security-related investments since 2020, giving technical security control and resiliency priority.

Central banks see phishing and social engineering as the most common methods of attack, and the potential losses from a systemically relevant cyber attack are deemed to be large, especially if the target is a big tech providing critical cloud infrastructures.

Generally, respondents judge the preparedness of the financial sector for cyber attacks to be inadequate. While central banks in most emerging market economies provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in advanced economies do.

Cooperation among public authorities, especially in the international context, could improve central banks' ability to respond to cyber attacks.

The survey reveals four main insights.

First, central banks from AEs and EMEs differ in their assessment of the frequency and cost of different cyber attacks. All central banks deem phishing and other forms of social engineering as the most likely type of attack vectors. AE central banks are significantly more worried about supply chain attacks than their EME counterparts.

When it comes to the costs resulting from an attack, advanced persistent malware and ransomware attacks rank highest. Turning to the who of these attacks, AE central banks deem organised crime and state-sponsored entities to be the main perpetrators. Among EME central banks, it is organised crime and individuals or activists.

Second, central banks actively discuss and develop policy responses to cyber attacks and have increased their cyber security-related investments notably since 2020.

Technical security control and resiliency feature high on the priority list in terms of areas for investment in cyber security.

Training existing staff on cyber security or hiring new staff with the relevant skills are also considered important, especially among EME central banks. Beyond investments, central banks focus on developing concrete policy responses.

All central banks put a high focus on developing an incident response plan in case their own institution is attacked, and several central banks are also developing a formal strategy for responding to an attack on the financial system at large.

All central banks run internal exercises to simulate cyber attacks, and the most frequently modelled scenarios are an attack on the system of the central bank itself, as well as an outage of the payments system or other critical FMI.

While supervisory authorities in most EMEs provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in AEs do.

Similarly, while supervised firms are mandated to report losses related to cyber attacks to the central bank in almost all EMEs, only two-thirds of AE respondents report that such disclosure is required.

No jurisdiction requires firms to disclose such losses publicly, however.

Third, central banks deem the potential losses from a systemically relevant cyber attack to be large, and think that losses from cyber attacks in the financial sector have increased over the past year.

Only a few central banks fully agree that the financial sector is adequately prepared for cyber attacks, and over half of the respondents think that investment in cyber security has been inadequate over the past year.

Beyond traditional financial institutions, respondents reported that they see fintechs to be more at risk from a cyber attack than big techs, even though most respondents agree that a successful attack on a big tech would lead to materially higher aggregate costs than an attack on a fintech.

And **fourth,** central banks in AEs and EMEs already cooperate widely on a range of topics. Bilateral cooperation among central banks, as well as cooperation in bodies at the regional and global levels, is the norm.

When it comes to specific topics related to cooperation, information sharing, simulations and policy formulations to improve cyber resilience stand out in AEs. Among EMEs, central banks frequently cooperate in the realms of information sharing and policy formations.

In addition, over two-thirds of respondents develop common standards and protocols for the financial sector.

The BIS supports central banks' cyber security work, as well as global cooperation in this domain, in several ways – for example, through its Cyber Resilience Coordination Centre or projects of the BIS Innovation Hub.

To read more: https://www.bis.org/publ/work1039.pdf

The Economic Outlook: Time to Let the Data Do the Talking

Governor Christopher J. Waller, Board of Governors of the Federal Reserve System, 17th Annual Vienna Macroeconomics Workshop, Vienna, Austria

Thank you, Klaus, and thank you for the invitation to speak at this workshop, which I have been attending since its very beginning in 2004.

Something that I love about this conference that has kept me coming back almost every year is its tradition of open inquiry and even some fun, on the one hand, combined with rigorous, critical analysis, on the other.

I am a supporter, and I guess a practitioner, of rigorous criticism, because, as you may have heard, the conference award given each year for "outstanding critic" was named for me.

Based on the standard I set, the person who wins the award is also known as the "most annoying participant." I suppose it was only karma that a guy like me who likes to dish out the criticism would end up in a job that receives plenty of it.

Kidding aside, I do consider being the namesake for this award a great honor, and just to make sure I don't get too much of a swelled head, by tradition the conference organizers purposefully misspell my name.

My subject today is the outlook for the U.S. economy and the Federal Reserve's ongoing campaign to bring down inflation and achieve our 2 percent objective.

There are three takeaways from my speech today. First, inflation is far too high, and it is too soon to say whether inflation is moving meaningfully and persistently downward.

The Federal Open Market Committee (FOMC) is committed to undertake actions to bring inflation back down to our 2 percent target. This is a fight we cannot, and will not, walk away from.

The second takeaway is that the fears of a recession starting in the first half of this year have faded away and the robust U.S. labor market is giving us the flexibility to be aggressive in our fight against inflation.

For that reason, I support continued increases in the FOMC's policy rate and, based on what I know today, I support a significant increase at our next meeting on September 20 and 21 to get the policy rate to a setting that is clearly restricting demand.

The final takeaway is that I believe forward guidance is becoming less useful at this stage of the tightening cycle.

Future decisions on the size of additional rate increases and the destination for the policy rate in this cycle should be solely determined by the incoming data and their implications for economic activity, employment, and inflation.

Based on all of the data that we have received since the FOMC's last meeting, I believe the policy decision at our next meeting will be straightforward.

Because of the strong labor market, right now there is no tradeoff between the Fed's employment and inflation objectives, so we will continue to aggressively fight inflation.

Inflation is widespread, driven by strong demand that has only begun to moderate, by an ongoing lag in labor force participation, and by supply chain problems that may be improving in some areas but are still considerable.

For these reasons, I expect it will take some time before inflation moves back to our 2 percent goal, and that the FOMC will be tightening policy into 2023. But the answers to questions of "how high?" and "for how long?" will depend solely on incoming data.

Since I last spoke in July, I think the argument that we entered a recession in the first half of 2022 has pretty much ended—we didn't. With each passing week, the absence of any indication of a recession in spending or employment data buries that recession argument a little deeper.

We understand some of the factors that lowered the gross domestic product (GDP) numbers in the first half, and a debate continues about other possible factors, such as mismeasurement, potentially underreporting GDP.

What we can say is that after the Fed telegraphed its policy pivot to tightening in the latter months of 2021 and began raising rates in the first quarter of this year, demand and economic activity slowed in the first half of 2022 from the strong pace of 2021.

Data suggest an uptick in consumption growth in the third quarter. Meanwhile, the Atlanta Fed's GDPNow model forecasts real GDP will grow 2.6 percent this quarter, though other estimates are a touch below this prediction.

Spending data are supportive of continued expansion. Nominal retail sales overall were flat in July, but that is mainly because falling gasoline and auto prices—which is good news—held back sales in those sectors.

Excluding that, retail sales rose 0.7 percent, suggesting that discretionary spending grew solidly. Businesses also continued to expand production and spending. Total industrial production increased 0.6 percent in July, standing 3.9 percent above its level a year ago.

Forward-looking indicators of manufacturing activity, such as new orders indexes in various manufacturing surveys, are softer than earlier in the year, but most (and in particular the positive August reading from the ISM) are not suggestive of a material pullback in manufacturing activity.

Meanwhile, the non- manufacturing ISM report suggests continuing growth, with its new orders index rising to a solid level last month.

But there are signs of moderation in economic activity, which is what the FOMC is trying to achieve by tightening monetary policy. Not surprisingly, higher interest rates this year are slowing activity in the housing market.

There have been declines in construction of single-family homes for a number of months, with permits and home starts both decreasing in July.

Sales of existing and new single-family homes have also slowed. Existing home sales fell by 5.9 percent to a seasonally adjusted annual rate of 4.8 million homes in July.

While the imbalance between housing supply and demand remains significant, it has meaningfully improved. The inventory of unsold new and existing homes has more than doubled since January.

While the three months supply of existing home is still below levels before the pandemic, the eleven months of new home inventory is the highest since the spring of 2009.

This latter statistic has raised concerns by some about a significant downturn looming in the housing market, but an important caveat is that much of the current elevated inventory reflects the recent low rate of housing completion due to continued supply constraints.

Many of these new homes for sale are still under construction, and as supply constraints ease, builders will be able deliver more completed homes to a market where the supply of existing homes remains tight. All that said, the housing market is a significant channel for monetary policy, and I will be watching this sector carefully.

The FOMC's goal is that the tightening in monetary policy slows aggregate demand so that it is in better alignment with supply across all sectors of the economy.

My expectation is that strong household savings, the tight labor market, and additional availability of manufactured goods as supply chains constraints continue to resolve will allow households to make long-awaited purchases, which will provide a partial offset to tighter policy. That will support a slowing, rather than a contraction, in demand.

Turning to the very strong labor market, private payroll employment has been increasing at an average of nearly 400,000 a month over the last several months.

Unemployment rose two tenths of a percent in August to 3.7 percent, in part reflecting an increase in the labor force participation rate, but still stands at a very low level.

The increase in participation was welcome news, but this rate is still far below that achieved before the pandemic, when unemployment was roughly as low as today.

We are facing worker shortages in many sectors of the economy. Job openings have started to decline a bit but remain very elevated. These data confirm that the Fed is hitting its full employment mandate, so all my attention is on bringing inflation down.

Inflation slowed in July, which was a very encouraging development. Headline inflation for both the consumer price index and the index derived from personal consumption expenditures (PCE)—the Fed's preferred measure—slowed, largely due to continuing declines in prices for gasoline and other petroleum products.

Excluding volatile energy and food prices, core inflation for these two indexes also stepped down from the rapid increases of earlier this year, but it is still too early to say that inflation is moving meaningfully and persistently downward.

Inflation is still widespread. For both headline and core inflation, at least 60 percent of the underlying categories of different goods and services increased by 3 percent or more.

Prices for housing services are elevated and still rising. Core goods inflation continues to run well above its pre-pandemic level.

Inflation for services excluding housing has moved up this past year in part due to consumers shifting back to more normal activities outside the household as social distancing has eased.

Looking ahead, I will be focusing on a number of factors that will influence inflation. On housing services—rent and the so-called owners' equivalent rent —I expect to see sizable increases in this component of inflation for a while as the recent rise in new rentals makes its way into aggregate price measures.

In a speech in March, I noted that, based on various measures of asking rents, some analysts were predicting that the rate of rent inflation in the consumer price index could double in 2022, and so far it is on pace to more than double.

Owners-equivalent rent is similarly on pace to nearly double this year. Sometime early next year, though, I expect to see the upward pressure on inflation from these forces to ease as future increases in new or renewed leases moderate and the full effects of monetary policy tightening make their way to housing services prices.

Beyond housing, I expect goods price inflation to continue to moderate as monetary policy now and going forward slows the pace of increase in aggregate demand, supply problems ease, and supply and demand come into better balance.

There is some evidence that goods supply production and delivery problems tied to the pandemic are improving, with supplier delivery times and reports of items in short supply continuing to drop.

In terms of service price inflation, we saw a step-down in airfares and other travel-related services last month, but I am uncertain about how these services, as well as food services, and nonmarket services prices will evolve going forward.

Nominal wages have been growing quickly, and I'll be watching closely to see how wage growth evolves and feeds into inflation.

The Atlanta Fed's Wage Growth Tracker hit another record in July for its 24 years of data, a 12-month rate of 6.7 percent wage growth.

I don't expect wage increases to ease up much unless and until there is a significant softening in the labor market.

One way to anticipate future wage growth is through quit rates. Most people who quit their jobs are moving to others that pay significantly better, so I take quits as one signal about where wages are headed in the near term.

Quits are near their highest level over the 22 years that the government has tracked them, but they have come down from the start of this year, and further decreases would bring them closer to the level they were at immediately before the pandemic, when wages were growing much more slowly than today.

Another factor that I will be watching closely is longer-term inflation expectations, which I believe significantly influence inflation.

As inflation moved higher over the past year and a half, measures of short-term inflation expectations moved up notably, but measures of longer-term expectations rose only a little and generally stand near levels seen in the years before the pandemic, when inflation was low.

In fact, several measures of longer-term expectations have edged lower over the past couple of months. To me, this means that the public retains confidence that the Fed will be able to rein in inflation in the medium term.

To sum up, while I welcome promising news about inflation, I don't yet see convincing evidence that it is moving meaningfully and persistently down along a trajectory to reach our 2 percent target.

I keep in mind that a year ago we saw similarly promising evidence of inflation moderating for several months before it jumped up to a high and then very high level.

Those earlier inflation readings probably delayed our pivot to tightening monetary policy by a few months.
The consequences of being fooled by a temporary softening in inflation could be even greater now if another misjudgment damages the Fed's credibility.

So, until I see a meaningful and persistent moderation of the rise in core prices, I will support taking significant further steps to tighten monetary policy.

Now let me lay out the implications of this outlook for monetary policy. Since March, the FOMC has raised our policy target range from near zero to between 2-1/4 and 2-1/2 percent.

That puts the upper bound of the current target range at the median of FOMC participants' longer-run projection for the policy rate, as recorded in the June Summary of Economic Projections (SEP).

This long-run rate is effectively where participants think the policy rate would settle when the economy is growing at its potential and inflation is at our 2 percent target.

This is a good definition of success when employment and inflation are near our goals and no help is needed from monetary policy. But that isn't the case now; inflation is far from our goal, so more action is needed.

The policy rate will have to move meaningfully above this neutral level to further restrain aggregate demand and put more downward pressure on prices.

Looking ahead to our next meeting, I support another significant increase in the policy rate. But, looking further out, I can't tell you about the appropriate path of policy. The peak range and how fast we will move there will depend on data we will receive about the economy.

Earlier this year, when we were ending asset purchases, inflation was quite elevated, and we were lifting the target range off the effective lower bound, so it made sense to provide forward guidance to help convey the urgency the FOMC felt about tightening monetary policy.

Forward guidance was useful in helping the public understand how quickly we expected to tighten, and we saw longer-term interest rates move up quite rapidly as a result of these communications. And additional hikes should lead to further restraint in aggregate demand.

As we continue to raise rates, we need to see, month by month, how households and businesses are adjusting to the tighter financial conditions, and how that adjustment is affecting inflation. We shouldn't be estimating what the peak level of the target range will be and how quickly we will get there, because those details are much more dependent on what new economic data tell us than was the case when the only direction for the federal funds rate to go was up—and up by a lot.

This is not to suggest that I anticipate rate increases stopping very soon. I expect that getting inflation to fall meaningfully and persistently toward

our 2 percent target will require increases in the target range for the federal funds rate until at least early next year.

But don't ask me about the policy path because I truly don't know—it will depend on the data.

Six months ago, I would not have thought that we would be where we are today, with inflation so far from our target, after significantly tightening policy with a series of large rate increases and by shrinking the balance sheet.

There are a range of possibilities for how the economy will perform, however, and we can talk about the implications of that range. Say, for example, that inflation follows the path laid out in the June SEP, which has core PCE inflation falling to 4.3 percent in the fourth quarter of 2022 and then moving toward 2 percent over 2023 and 2024. In that case, I would support our policy rate peaking near 4 percent.

But based on the experience of the past year and half, it would be foolish to express great confidence that this plausible path will come to pass. Instead, it is important to consider the range of possibilities and the appropriate policy responses.

For example, if inflation does not moderate or rises further this year, then, in my view, the policy rate will probably need to move well above 4 percent. Alternatively, if inflation suddenly decelerates, then, in my view, the policy rate might peak at less than 4 percent.

One thing that is more predictable and has a significant effect on tightening policy over time is the shrinking of the Fed's holdings of assets as maturing securities run off our balance sheet. Starting this month, the Fed is shedding $60 billion a month in Treasury securities and up to $35 billion a month in agency mortgage-backed securities.

This action effectively increases the supply of securities in the hands of private investors and will thus put upward pressure on interest rates, as private investors must now be enticed to hold these assets.
All told, the FOMC has taken unprecedented and decisive policy actions this year to quickly increase the policy rate in response to high inflation. But where we stand now is not good enough. Though the labor market is strong, inflation is too elevated.

So I support another significant hike in two weeks. After that, the tightening path will continue until we see clear and convincing evidence that inflation is moving meaningfully and persistently down to our 2 percent target.

The pace of tightening is uncertain; it will depend on the data. No matter what, I am ready and willing to do what it takes to bring inflation down.

To read more:
https://www.federalreserve.gov/newsevents/speech/waller20220909a.htm

Chief Information Officers, Private Sector Practices Can Inform Government Roles

United States Government Accountability Office
Report to Congressional Committees

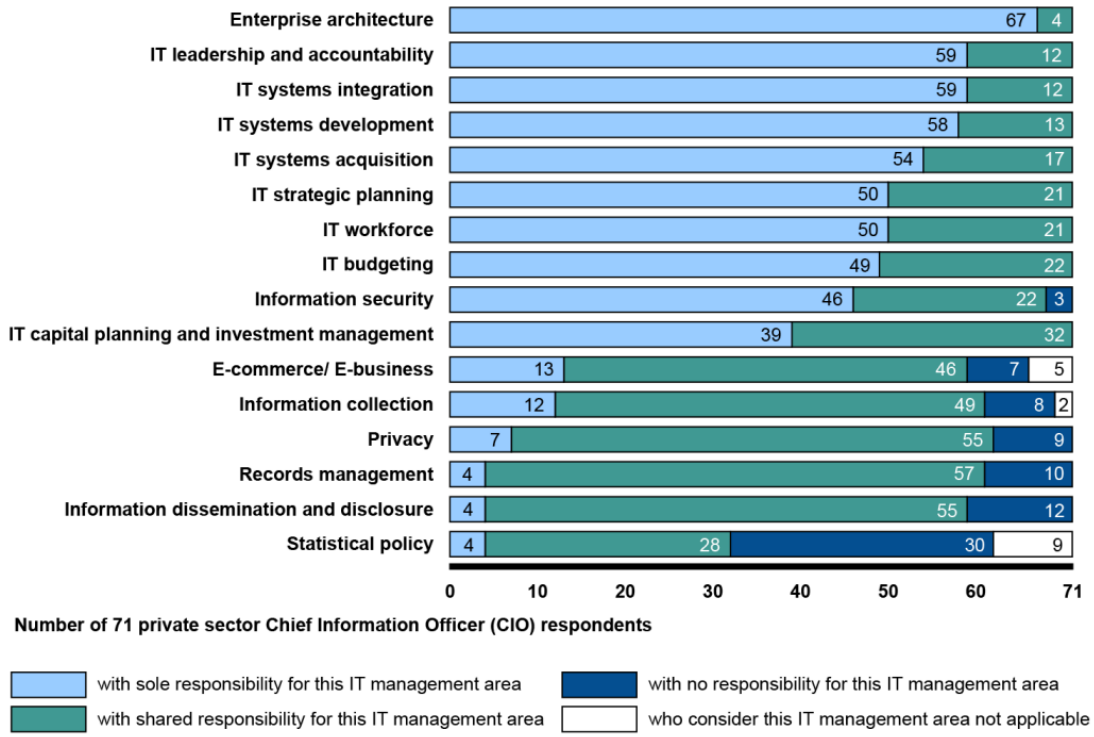
What GAO Found

A majority of the 71 private sector Chief Information Officer (CIO) survey respondents reported having responsibilities that aligned with those of agency CIOs in 13 of 14 key IT management areas.

These areas include strategic planning, investment management, and information security. One area of responsibility (the statistical policy area) was reported by more than half of respondents as being outside their scope of responsibility.

In addition, CIO respondents also reported sharing responsibility with other executives in each IT management area (see figure 1).

Figure 1: Extent of Sharing of IT Management Area Responsibilities Reported by 71 Private Sector Chief Information Officer (CIO) Respondents



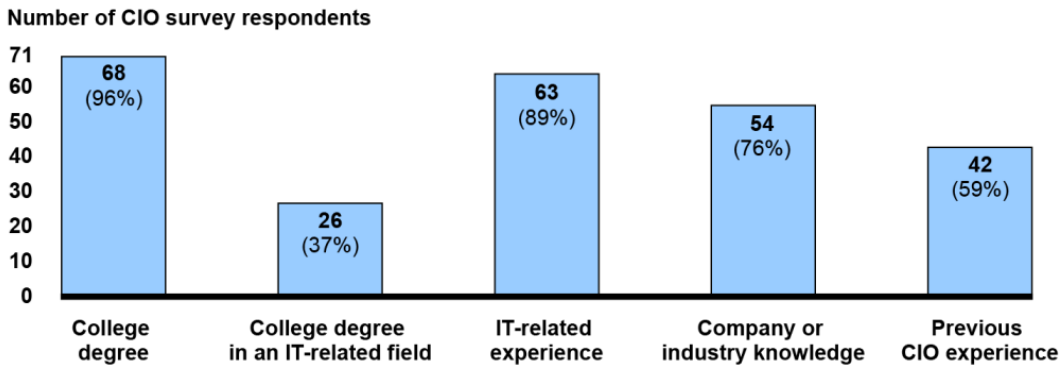
Source: GAO analysis of data from 71 private sector CIO survey respondents. | GAO-22-104603

Private sector CIO respondents were highly educated and experienced, with a majority reporting previous IT-related experience, previous CIO experience, industry knowledge, and a college degree (see figure 2).

Notably, a majority of respondents reported that their degrees were not IT-related. Respondents reported an average tenure in their current CIO role of about 6 years.

Among respondents, CIOs with more authority over technology-related decisions tended to have a higher level of previous CIO experience, as well as the longest tenures.

Figure 2: Qualifications and Experience of Private Sector Chief Information Officer (CIO) Respondents



Source: GAO analysis of data from 71 private sector CIO survey respondents. | GAO-22-104603

This graph shows selected responses from two survey questions. The variables are categorical and the numbers are not intended to add to 71 or the percentages to 100 percent.

Responsibilities currently assigned to the Federal CIO correspond to those of agency CIOs in 10 of the 14 key IT management areas.

The Federal CIO's responsibilities also correspond to those of private sector survey respondents in each of five responsibility areas directly relevant to the roles of both.

However, the Federal CIO position is not established in law, and its main legal authorities remain those established in 2002 for the OMB position from which the role was established.

As such, its responsibilities are often more limited in key CIO management areas than those of the other types of CIOs.

For example, the Federal CIO is not responsible for ensuring that cybersecurity duties are carried out. By formalizing the Federal CIO position and establishing responsibilities and authorities over government-wide IT management, the position's impact over federal IT may be more consistent over time and across administrations.

Private sector and former agency CIOs participating in panel discussions reported challenges faced by federal agency CIOs.

Specifically, private sector CIO panelists stated that collaboration between the CIO and other senior executives is essential to driving successful business outcomes.

Conversely, former federal CIO panelists reported difficulty achieving meaningful collaboration with other managers. In addition, private sector panelists stated that their companies often look for managerial skills, such as project management skills, when hiring CIOs.

By contrast, former agency CIO panelists stated that technical skills are often a primary driver in the selection of agency CIOs.

Fostering shared collaboration and increasing focus on managerial skillsets for agency CIOs could assist federal agencies and their CIOs in securing resources and implementing IT priorities.

The Level of IT Responsibilities Shared by Private Sector CIO Respondents Varied Based on Their Reporting Structure

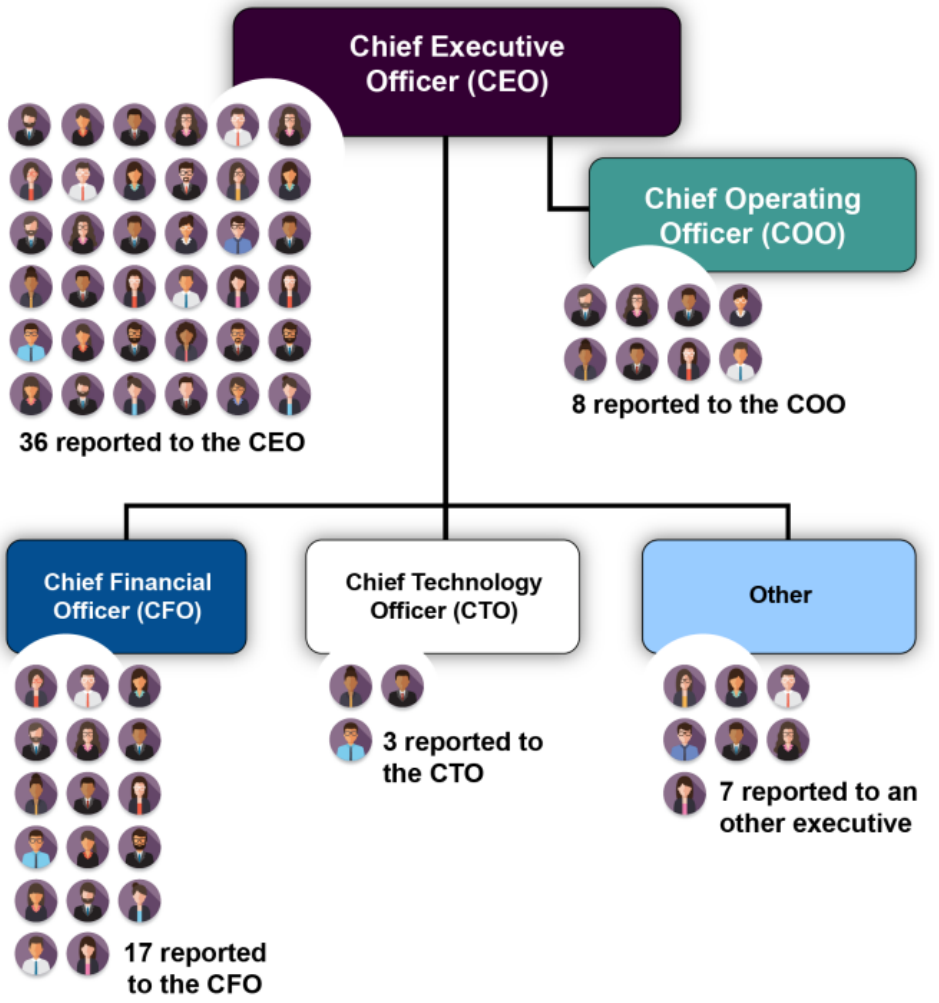
Private sector CIOs who responded to our survey had direct reporting relationships to several different senior executives at their companies.

For example, approximately half of private sector CIOs reported directly to their company's CEO, and about a quarter to their company's CFO.

The remainder of the CIO respondents reported directly to other executives, such as their COO, chief technology officer (CTO), president, chief administrative officer, chief growth officer, or the chief of corporate operations. Figure 3 shows the percent of CIO respondents directly

reporting to each of the four primary types of senior executives mentioned by CIOs, as well as those reporting to executives other than those four.

Figure 3: Reporting Structure for 71 Private Sector Chief Information Officer (CIO) Respondents



Source: GAO analysis of data from 71 private sector CIO survey respondents; images: sapannpix/stock.adobe.com. | GAO-22-104603

To read more:
https://www.gao.gov/assets/gao-22-104603.pdf

Deputy Attorney General Lisa O. Monaco Delivers Remarks on Corporate Criminal Enforcement

Good afternoon. Thank you, Dean McKenzie, for the introduction and for hosting us today. I'm happy to be back at NYU, and to see so many friends and former colleagues in the room.

Let me start by acknowledging some of my DOJ colleagues who are here. That includes the U.S. Attorneys for the Southern and Eastern Districts of New York, New Jersey, and Connecticut.

But just as importantly, we're joined in person and on the livestream by line prosecutors, agents, and investigative analysts—the career men and women who do the hard work, day in and day out, to make great cases and hold wrongdoers accountable.

I also want to recognize our federal and state partners who play a critical role in corporate enforcement. And of course, let me also thank Professor Arlen and the NYU Program on Corporate Compliance and Enforcement for arranging this event and for serving as a bridge between the worlds of policymaking and academia.

Addressing corporate crime is not a new subject for the Justice Department. In the aftermath of Watergate, Attorney General Edward Levi was tasked not only with restoring the Department's institutional credibility, but also with rebuilding its corporate enforcement program.

In a 1975 speech, he told prosecutors that there was great demand to be more aggressive against, what he called, "white collared crime." He explained his distaste for that term, saying that it suggested a distinction in law enforcement based upon social class. But, nonetheless, he acknowledged that it was an area that needed to be given "greater emphasis." These words are as true today as they were then.

But Attorney General Levi also said that efforts to fight corporate crime were hampered by a lack of resources, specially trained investigators, and other issues. He answered those complaints as all great Attorneys General do—he said his Deputy Attorney General would take care of it. For at least a half-century, therefore, it has been the responsibility of my predecessors to set corporate criminal policy for the Department, and I follow in their footsteps.

Last October, I announced immediate steps the Justice Department would take to tackle corporate crime.

I also formed the Corporate Crime Advisory Group, a group of DOJ experts tasked with a top-to-bottom review of our corporate enforcement efforts.

To get a wide range of perspectives, we met with a broad group of outside experts, including public interest groups, ethicists, academics, audit committee members, in-house attorneys, former corporate monitors, and members of the business community and defense bar. Many of these people are here today.

Our meetings sparked discussions on individual accountability and corporate responsibility; on predictability and transparency; and on the ways enforcement policies must square with the realities of the modern economy. Every meeting resulted in some idea or insight that was helpful and that we sought to incorporate into our work. Today, you will hear how these new policies reflect this diverse input.

Let me turn now to substance—and the changes the Department is implementing to further strengthen how we prioritize and prosecute corporate crime.

First, I'll reiterate that the Department's number one priority is individual accountability—something the Attorney General and I have made clear since we came back into government. Whether wrongdoers are on the trading floor or in the C-suite, we will hold those who break the law accountable, regardless of their position, status, or seniority.

Second, I'll discuss our approach to companies with a history of misconduct. I previously announced that prosecutors must consider the full range of a company's prior misconduct when determining the appropriate resolution. Today, I will outline additional guidance for evaluating corporate recidivism.

Third, I'll highlight new Department policy on voluntary self-disclosures, including the concrete and positive consequences that will flow from self-disclosure. We expect good companies to step up and own up to misconduct. Voluntary self-disclosure is an indicator of a working compliance program and a healthy corporate culture. Those companies who own up will be appropriately rewarded in the Department's approach to corporate crime.

Fourth, I'll detail when compliance monitors are appropriate and how we can select them equitably and transparently. Today, I am also directing Department prosecutors to monitor those monitors: to ensure they remain on the job, on task, and on budget.

Finally, I'll discuss how the Department will encourage companies to shape financial compensation around promoting compliance and avoiding improperly risky behavior. These steps include rewarding companies that claw back compensation from employees, managers, and executives when misconduct happens. No one should have a financial interest to look the other way or ignore red flags. Corporate wrongdoers—rather than shareholders—should bear the consequences of misconduct.

Taken together, the policies we're announcing today make clear that we won't accept business as usual. With a combination of carrots and sticks—with a mix of incentives and deterrence—we're giving general counsels and chief compliance officers the tools they need to make a business case for responsible corporate behavior. In short, we're empowering companies to do the right thing—and empowering our prosecutors to hold accountable those that don't.

Individual Accountability

Let me start with our top priority for corporate criminal enforcement: going after individuals who commit and profit from corporate crime.

In the last year, the Department of Justice has secured notable trial victories, including convictions of the founder and chief operating officer of Theranos; convictions of J.P. Morgan traders for commodities manipulation; the conviction of a managing director at Goldman Sachs for bribery; and the first-ever conviction of a pharmaceutical CEO for unlawful distribution of controlled substances.

Despite those steps forward, we cannot ignore the data showing overall decline in corporate criminal prosecutions over the last decade. We need to do more and move faster. So, starting today, we will take steps to empower our prosecutors, to clear impediments in their way, and to expedite our investigations of individuals.

To do that, we will require cooperating companies to come forward with important evidence more quickly.

Sometimes we see companies and counsel elect—for strategic reasons—to delay the disclosure of critical documents or information while they consider how to mitigate the damage or investigate on their own. Delayed disclosure undermines efforts to hold individuals accountable. It limits the Department's ability to proactively pursue leads and preserve evidence before it disappears. As time goes on, the lapse of statutes of limitations, dissipation of evidence, and the fading of memories can all undermine a successful prosecution.

In individual prosecutions, speed is of the essence.

Going forward, undue or intentional delay in producing information or documents—particularly those that show individual culpability—will result in the reduction or denial of cooperation credit. Gamesmanship with disclosures and productions will not be tolerated.

If a cooperating company discovers hot documents or evidence, its first reaction should be to notify the prosecutors. This requirement is in addition to prior guidance that corporations must provide all relevant, non-privileged facts about individual misconduct to receive any cooperation credit.

Separately, Department prosecutors will work to complete investigations and seek warranted criminal charges against individuals prior to or at the same time as entering a resolution against a corporation. Sometimes the back-and-forth of resolving with a company can bog down individual prosecutions, since our prosecutors have finite resources.

In cases where it makes sense to resolve a corporate case first, there must be a full investigative plan outlining the remaining work to do on the individual cases and a timeline for completing that work.

Collectively, this new guidance should push prosecutors and corporate counsel alike to feel they are "on the clock" to expedite investigations, particularly as to culpable individuals. While many companies and prosecutors follow these principles now, this guidance sets new expectations about the sequencing of investigations and clarifies the Department's priorities.

History of Misconduct

Now, it's safe to say that no issue garnered more commentary in our discussions than the commitment we made last year to consider the full criminal, civil, and regulatory record of any company when deciding the appropriate resolution.

That decision was driven by the fact that between 10% and 20% of large corporate criminal resolutions have involved repeat offenders.

We received many recommendations about how to contextualize historical misconduct, to develop a full and fair picture of the misconduct and corporate culture under review. We heard about the need to evaluate the regulatory environment that companies operate in, as well as the need to consider the age of the misconduct and subsequent reforms to the company's compliance culture.

In response to that feedback, today, we are releasing additional guidance about how such histories will be evaluated. Now let me emphasize a few points.

First, not all instances of prior misconduct are created equal. For these purposes, the most significant types of prior misconduct will be criminal resolutions here in the United States, as well as prior wrongdoing involving the same personnel or management as the current misconduct. But past actions may not always reflect a company's current culture and commitment to compliance. So, dated conduct will generally be accorded less weight.

And what do we mean by dated? Criminal resolutions that occurred more than 10 years before the conduct currently under investigation, and civil or regulatory resolutions that took place more than five years before the current conduct.

We will also consider the nature and circumstances of the prior misconduct, including whether it shared the same root causes as the present misconduct. Some facts might indicate broader weaknesses in the compliance culture or practices, such as wrongdoing that occurred under the same management team or executive leadership. Other facts might provide important mitigating context.

For example, if a corporation operates in a highly regulated industry, its history should be compared to others similarly situated, to determine if the company is an outlier.

Separately, we do not want to discourage acquisitions that result in reformed and improved compliance structures. We will not treat as recidivists companies with a proven track record of compliance that acquire companies with a history of compliance problems, so long as those problems are promptly and properly addressed post-acquisition.

Finally, I want to be clear that this Department will disfavor multiple, successive non-prosecution or deferred prosecution agreements with the same company. Before a prosecution team extends an offer for a successive NPA or DPA, Department leadership will scrutinize the proposal. That will ensure greater consistency across the Department and a more holistic approach to corporate recidivism.

Companies cannot assume that they are entitled to an NPA or a DPA, particularly when they are frequent flyers. We will not shy away from bringing charges or requiring guilty pleas where facts and circumstances require. If any corporation still thinks criminal resolutions can be priced in as the cost of doing business, we have a message—times have changed.

Voluntary Self-Disclosure

That said, the clearest path for a company to avoid a guilty plea or an indictment is voluntary self-disclosure. The Department is committed to providing incentives to companies that voluntarily self-disclose misconduct to the government. In many cases, voluntary self-disclosure is a sign that the company has developed a compliance program and has fostered a culture to detect misconduct and bring it forward.

Our goal is simple: to reward those companies whose historical investments in compliance enable voluntary self-disclosure and to incentivize other companies to make the same investments going forward.

Voluntary self-disclosure programs, in various Department components, have already been successful. Take, for example, the Antitrust Division's Leniency Program, the Criminal Division's voluntary disclosure program for FCPA violations, and the National Security Division's program for export control and sanctions violations. We now want to expand those policies Department-wide.

We also want to clarify the benefits of promptly coming forward to self-report, so that chief compliance officers, general counsels, and others can make the case in the boardroom that voluntary self-disclosure is a good business decision.

So, for the first time ever, every Department component that prosecutes corporate crime will have a program that incentivizes voluntary self-disclosure. If a component currently lacks a formal, documented policy, it must draft one.

Predictability is critical. These policies must provide clear expectations of what self-disclosure entails. And they must identify the concrete benefits that a self-disclosing company can expect.

I am also announcing common principles that will apply across these voluntary self-disclosure policies. Absent aggravating factors, the Department will not seek a guilty plea when a company has voluntarily self-disclosed, cooperated, and remediated misconduct. In addition, the Department will not require an independent compliance monitor for such a corporation if, at the time of resolution, it also has implemented and tested an effective compliance program.

Simply put, the math is easy: voluntary self-disclosure can save a company hundreds of millions of dollars in fines, penalties, and costs. It can avoid reputational harms that arise from pleading guilty. And it can reduce the

risk of collateral consequences like suspension and debarment in relevant industries.

If you look at recent cases, you can see the value proposition. Voluntary self-disclosure cases have resulted in declinations and non-prosecution agreements with no significant criminal penalties. By contrast, recent cases that did not involve self-disclosure have resulted in guilty pleas and billions of dollars in criminal penalties, this year alone. I expect that resolutions over the next few months will reaffirm how much better companies fare when they come forward and self-disclose.

Independent Compliance Monitors

Let me turn to monitors. Over the past year of discussions, we heard a call for more transparency to reduce suspicion and confusion about monitors. Today, we're addressing those concerns.

First, we are releasing new guidance for prosecutors about how to identify the need for a monitor, how to select a monitor, and how to oversee the monitor's work to increase the likelihood of success.

Second, going forward, all monitor selections will be made pursuant to a documented selection process that operates transparently and consistently.

Finally, Department prosecutors will ensure that the scope of every monitorship is tailored to the misconduct and related compliance deficiencies of the resolving company. They will receive regular updates to verify that the monitor stays on task and on budget. We at the Department of Justice are not regulators, nor do we aspire to be. But where we impose a monitor, we recognize our obligations to stay involved and monitor the monitor.

Corporate Culture

As everyone here knows, it all comes back to corporate culture. Having served as both outside counsel and a board member in the past, I know the difficult decisions and trade-offs companies face about how to invest corporate resources, structure compliance programs, and foster the right corporate culture.

In our discussions leading to this announcement, we identified encouraging trends and new ways in which compliance departments are being strengthened and sharpened. But resourcing a compliance department is not enough; it must also be backed by, and integrated into, a corporate culture that rejects wrongdoing for the sake of profit. And

companies can foster that culture through their leadership and the choices they make.

To promote that culture, an increasing number of companies are choosing to reflect corporate values in their compensation systems.

On the deterrence side, those companies employ clawback provisions, the escrowing of compensation, and other ways to hold financially accountable individuals who contribute to criminal misconduct. Compensation systems that clearly and effectively impose financial penalties for misconduct can deter risky behavior and foster a culture of compliance.

On the incentive side, companies are building compensation systems that use affirmative metrics and benchmarks to reward compliance-promoting behavior.

Going forward, when prosecutors evaluate the strength of a company's compliance program, they will consider whether its compensation systems reward compliance and impose financial sanctions on employees, executives, or directors whose direct or supervisory actions or omissions contributed to criminal conduct. They will evaluate what companies say and what they do, including whether, after learning of misconduct, a company actually claws back compensation or otherwise imposes financial penalties.

I have asked the Criminal Division to develop further guidance by the end of the year on how to reward corporations that employ clawback or similar arrangements. This will include how to help shift the burden of corporate financial penalties away from shareholders—who frequently play no role in misconduct—onto those more directly responsible.

Conclusion

But we're not done.

We will continue to engage and protect victims—workers, consumers, investors, and others.
We will continue to find ways to improve our approach to corporate crime, such as by enhancing the effectiveness of the federal government's system for debarment and suspension.

We will continue to seek targeted resources for corporate criminal enforcement, including the $250 million we are requesting from Congress for corporate crime initiatives next year.

Today's announcements are fundamentally about individual accountability and corporate responsibility. But they are also about ownership and choice.

Companies should feel empowered to do the right thing—to invest in compliance and culture, and to step up and own up when misconduct occurs. Companies that do so will welcome the announcements today. For those who don't, however, our department prosecutors will be empowered, too—to hold accountable those who don't follow the law.

Thank you again for having me here today. I look forward to taking some questions.

To read more: https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement

Technology and Talent - Audit Quality Challenges in the 21st Century

Christina Ho, PCAOB Board Member,
Deloitte PPD Seminar, Washington, DC

Thank you for the introduction. It is a pleasure to be here today and since you gave me the luxury of picking my own topic, I thought I would share my perspectives on audit quality challenges in the 21st century. The views that I express here are my own and do not necessarily reflect the views of other PCAOB Board members or staff.

Hindsight is 20/20

In July of this year, we celebrated the 20th anniversary of the Sarbanes-Oxley Act of 2002, affectionately known as "SOX". You may recall that the birth of SOX started with egregious corporate scandals.

The first was Enron, a corporation that appeared to be a reputable energy company at the time. The company's leadership created fictitious holdings, used special purpose entities to hide their debt and toxic assets, and falsified accounting records. Eventually, Enron filed for Bankruptcy in 2001, tumbling its share price from its height at $90.75 to a mere $.26 cents.

This scandal spurred not only the demise of the company but also its auditor, Arthur Anderson, and eradicated the life savings of numerous hardworking employees and investors who had the utmost confidence in the company's financial position.

Following suit in 2002 was another large accounting scandal, resulting in the bankruptcy of WorldCom, the 2nd largest long-distance telephone company at the time.

Both Enron and WorldCom intentionally "cooked the books," and again, Arthur Anderson turned a blind eye at WorldCom for inflating profits.

Given these extensive financial scandals, the federal government implemented sweeping reform by enacting SOX with bipartisan congressional support.

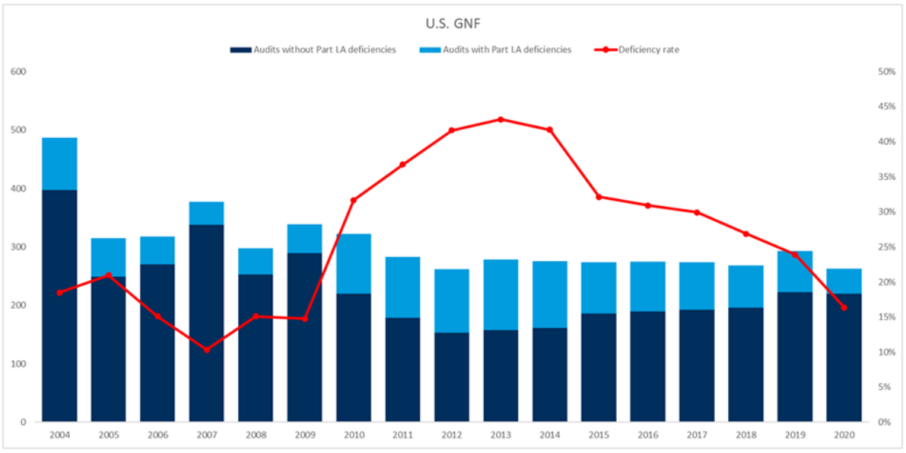
With the enactment of SOX came the beginning of the PCAOB and the end of more than 100 years of self-regulation by the accounting profession.

As a newly formed independent regulatory and oversight body, the PCAOB had its growing pains during the initial years and has evolved in maturing its programs throughout the past 20 years.

Today, the PCAOB has almost 1,700 registered firms, including U.S. and non-U.S. registered firms. In relation to foreign registered firms, most recently on August 26, 2022, PCAOB Chair Williams announced that the PCAOB had signed an agreement with People's Republic of China authorities, which is the first step toward opening access for the PCAOB to inspect and investigate completely registered public accounting firms in mainland China and Hong Kong.

Prior to her August 26, 2022 announcement, Chair Williams provided remarks on the celebration of the SOX 20th anniversary on July 28, 2022.

In that speech, Chair Williams shared that the PCAOB has completed over 4,300 firm inspections in 55 countries, including reviewing more than 15,000 audits of public companies and over 1,000 broker-dealer engagements.



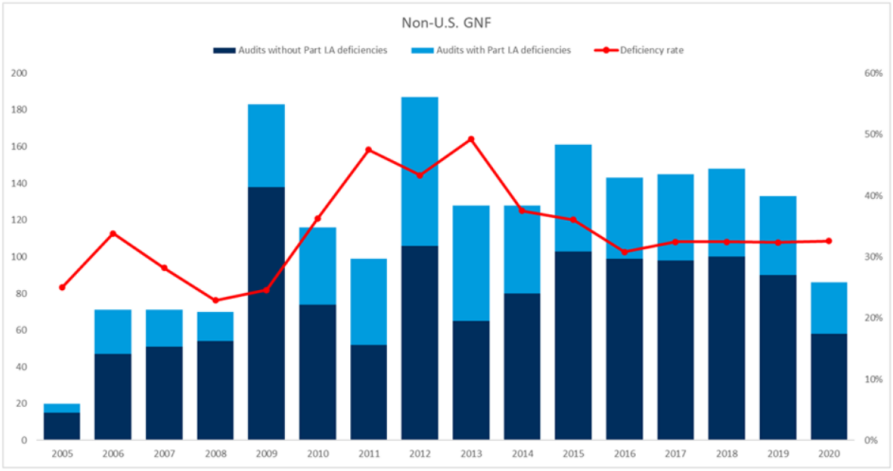
Source: PCAOB (Tables Contain Aggregated, Anonymized, and Rounded Publicly Available Data)

To provide historical context, I would like to share some high-level trends of the deficiency rates for both the U.S. and Non-U.S. Global Network Firms (GNF) since the inception of our Inspection program.

As illustrated, the Part I.A findings deficiency rate for U.S. GNFs in 2004 was about 18%, which trended downward through 2007 to about 10%, rising to over 40% at the peak in 2013, then settled back down to about 16% in 2020. The deficiency rate is the ratio of audits with findings relative

to the total number of audits (with and without findings) reviewed by the PCAOB Inspections division.

For Non-U.S. GNFs, the trending is similar, starting at about a 25% deficiency rate in 2005, slightly down to below 25% in 2008, up again to nearly 50% in 2013, then landing at about 33% in 2020.



Source: PCAOB (Tables Contain Aggregated, Anonymized, and Rounded Publicly Available Data)

To read more: https://pcaobus.org/news-events/speeches/speech-detail/ho-technology-and-talent-audit-quality-challenges-in-the-21st-century

Technical documentation of the methodology to derive EIOPA's risk-free interest rate term structures

Letter of the Executive Director

Solvency II aims at implementing an economic and risk-based supervisory framework in the field of insurance and reinsurance. The framework is built upon three pillars, all equally relevant, that provide for quantitative requirements (Pillar 1), qualitative requirements (Pillar 2) and enhanced transparency and disclosure (Pillar 3).

The starting point in Solvency II is the economic valuation of the whole balance sheet, where all assets and liabilities are valued according to market consistent principles.

The risk-free interest rate term structure (hereafter in this letter, risk-free interest rate) underpins the calculation of liabilities by insurance and reinsurance undertakings.

EIOPA is required to publish the risk-free interest rate. This technical document sets out the basis on which it will do so. It is the result of collaboration between EIOPA's members and its staff.

As a default approach, the risk-free interest rate is primarily derived from the rates at which two parties are prepared to swap fixed and floating interest rate obligations.

In the absence of financial swap markets, or where information of such transactions is not sufficiently reliable, the risk-free interest rate is based on the government bond rates of the country.

The risk-free interest rates are:

• Calculated for different time periods, reflecting that the liabilities of insurance and reinsurance undertakings stretch years and decades into the future.

• Calculated in respect of the most important currencies for the EU insurance market.

• Adjusted to reflect that a portion of the interest rate in a swap transaction (or a government bond) will reflect the risk of default of the counterparty

and hence without adjustment would not be risk-free.

• Based on data available from financial markets. For those periods in the more distant future for which data are not available, the rate is extrapolated from the point at which data are available to a macroeconomic long-term equilibrium rate.

An adjustment (the volatility adjustment) is made to the liquid part of the riskfree interest rate in order to reduce the impact of short-term market volatility on the balance sheet of undertakings.

EIOPA is required to provide, both on a currency and country basis, the size of this adjustment for volatility.

A different adjustment (the matching adjustment) is made in respect of predictable portfolios of liabilities.

An undertaking can assign to eligible portfolios assets with fixed cash flows that it intends to hold to maturity. EIOPA is required to provide an estimate of what portion of the spread of such assets above the riskfree interest rate reflects risks not faced by those who hold assets to maturity.

To read more:
https://www.eiopa.europa.eu/sites/default/files/risk_free_interest_rate/eiopa-bos-22-409-technical-documentation.pdf

Federal Reserve Board invites comment on updates to operational risk-management requirements for certain systemically important financial market utilities (FMUs) supervised by the Board

The Federal Reserve Board has invited comment on updates to operational risk-management requirements for certain systemically important financial market utilities (FMUs) supervised by the Board.

FMUs provide essential infrastructure to clear and settle payments and other financial transactions upon which the financial markets and the broader economy rely to function effectively.

The proposed updates generally provide more specificity to the existing requirements.

The broad operational risk, technology, and regulatory landscape in which FMUs operate has evolved significantly since the Board last updated its risk management requirements for FMUs in 2014.

New challenges have emerged, such as the global pandemic and cyber events, while new technological advancements may improve resilience. The proposed changes would promote effective risk management in this rapidly evolving risk environment.

"In light of the rapidly evolving risk landscape, the proposed changes will help ensure that key financial market utilities operate with a high level of resilience and remain a source of strength for the financial system," said Vice Chair Lael Brainard.

The proposal addresses four key areas: incident management and notification; business continuity management and planning; third-party risk management; and review and testing of operational risk management measures.

For example, the proposal would explicitly require FMUs to establish an incident management framework and would emphasize the need for FMUs to continue to advance their cyber resilience capabilities. The proposed updates are largely consistent with existing measures that FMUs take to comply with the current requirements.

Comments on the proposed changes must be submitted within 60 days from the date of publication in the Federal Register.

For media inquiries, email media@frb.gov or call (202) 452-2955.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/bcreg20220923a.htm

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 Hedge Funds Professionals (IAHFP)

At every stage of your career, our community provides training, certification programs, resources, updates, networking and services you can use.

You can explore what we offer to our members:

1. Membership – Become a standard, premium or lifetime member. You may visit:
https://www.hedge-funds-association.com/HowToBecomeMember.html

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

3. Training and Certification – You may visit:
https://www.hedge-funds-association.com/Distance_Learning_and_Certification.htm