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, April 18, 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,

Organisations take an *informal* approach to incident management, with fewer than one in five businesses having a formal incident management plan. However, a much greater proportion of organisations have a *formal* business continuity plan. This demonstrates a clear priority to ensure that business operations continue uninterrupted, while conducting proactive activity into cyber risk management is a secondary consideration.

The above scary information and conclusion is part of the very interesting *Cyber Security Breaches Survey 2022* from the UK Department for Digital, Culture, Media & Sport.

According to the paper, despite cyber security being seen as a high priority area, qualitative research found there is a *lack* of technical knowhow expertise within *smaller* organisations and at *senior level* within larger

organisations. This inhibits an organisation's cyber security for a number of reasons. These include fostering a tendency to take a reactive approach, viewing investment in cyber security *as a cost rather than an investment,* being intimidated by terminology and lacking awareness of strategic risks posed to an organisation. Many organisations remain in a reactive approach to cyber security instead of proactively driving improvements.

Also, there is a clear *lack of commercial narrative* to effectively negotiate a cyber security budget against other competing organisational priorities. For organisations that do not outsource their IT or cyber security solutions; often the cyber security profile is reliant on the colleague with cyber security responsibilities to communicate and influence board members to drive improvements.

What is really scary: Organisations are *not publicly disclosing* their cyber security profile in their *annual reports* or otherwise to best inform stakeholders.

Qualitative interviews suggested that often annual reports are produced by a colleague in a different department to IT. Additionally, *reputational concerns* around being negatively compared with peers or perceived as weak led to cyber security being limited in annual reporting to high level risks or strategy, or even omitted entirely.

On the positive side, cyber security is now seen as a high priority by a greater proportion of businesses than in any other year of the survey. It has also remained steady amongst charities compared to last year but is significantly higher than the baseline year in 2018.

In the qualitative interviews it was found that this was driven by a good high-level understanding at the senior level of the risks cyber attacks pose. This, coupled with the use of board sponsors and cyber security experts enabled organisations to practice good cyber hygiene.

Organisations have been able to maintain good cyber hygiene, with most rules, policies and controls and risk mitigation techniques remaining steady compared to last year, despite continued challenges.

More than 4 in 5 medium and large businesses have taken action for their cyber security in at least 5 areas detailed in the Government guidance; the 10 Steps to Cyber Security. This demonstrates that larger UK enterprises have a good standard of cyber security.

Additionally, several technical controls such as access management, malware, firewalls and data security are very commonplace.

Organisations have been able to implement an engaged culture around cyber security, understanding that staff vigilance is essential to protect against the threat of phishing attacks. In order to ensure staff were on board, communication put out by organisations focused on protecting customers and service users as opposed to any technical details on cyber security.

Organisations successfully implementing a good cyber security culture ensure dialogue to staff on cyber security is regular and relatively informal. They strike the right balance between changing initiatives to alter staff behaviour without making it too burdensome and disruptive for employees.

Read more at Number 6 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)

Project Ellipse
An integrated regulatory data and analytics platform

Number 2 (Page 10)

PCAOB Highlights Key Considerations for Auditors Related to the Russian Invasion of Ukraine

Number 3 (Page 17)

The return of inflation

Agustín Carstens, General Manager of the BIS at the International Center for Monetary and Banking Studies, Geneva

Number 4 (Page 19)

Is that a Fish Behind the Wheel?

SEC Commissioner Hester M. Peirce, before the University of Central Florida's Inaugural FinTech Summit

Number 5 (Page 25)

FSB Work Programme for 2022

Number 6 (Page 28)

Official Statistics

Cyber Security Breaches Survey 2022

Number 7 (Page 31)

Variation in the Inflation Experiences of Households

Governor Lael Brainard, at the Spring 2022 Institute Research Conference, Opportunity and Inclusive Growth Institute, Federal Reserve Bank of Minneapolis, Minneapolis, Minnesota

Number 8 (Page 39)

Fake WhatsApp 'voice message' emails are spreading malware

Number 9 (Page 41)

Capability Assessment for StratCom:

Using the New Risk Perspective to Inform the Development of Effective Response Capability Assessments for Countering Information Influence Operations

Number 10 (Page 44)

First Complete Human Genome Poised to Strengthen Genetic Analysis, NIST Study Shows

Number 1

Project Ellipse
An integrated regulatory data and analytics platform

Executive summary

A transformational shift in the volume, speed and variety of data is driving the innovative use of financial technology, leading to rapid changes in the financial landscape.

At the same time, regulatory authorities still rely on the collection of template-based supervisory data, which has remained largely unchanged.

Supervisors are faced with the challenge of needing to assess rapidly evolving risks to business models and technology-driven changes that may affect financial stability, with regulatory data that are infrequent and collected according to legacy frameworks.

In January 2021, the BIS Innovation Hub Singapore Centre and the Monetary Authority of Singapore (MAS) launched Project Ellipse.

With the support of the Bank of England (BoE), the International Swaps and Derivatives Association (ISDA), Financial Network Analytics (FNA) and Accenture, Project Ellipse explores how technology solutions could enable supervision to be more forward-looking, insights-based and data-driven, using an integrated regulatory data and analytics platform.

Importantly, the Ellipse prototype combines both structured and unstructured sources of data that are relevant to current events in real time.

Advanced analytics are then applied to those integrated data sources to provide supervisors with early warning indicators, analytics and prudential metrics.

Project Ellipse was undertaken in two phases. In Phase 1, the project investigated how data-driven supervision could be enabled by machine-executable digital reporting, using a cross-border common data model.

Our exploration found that regulatory reporting requirements can be expressed in unambiguous machinereadable logical reporting instructions underpinned by a consistent data model.

Programmatic specifications of the steps for generating regulatory reports can also be published alongside regulations to ensure a clear understanding of the expected data at the most granular level.

With additional logical instructions based on the same data model, supervisors could also automatically query the underlying transaction data and generate regulatory metrics referencing that standardised data.

Phase 1 illustrated the possibilities and the efficiencies that could be gained if machine-executable reporting using common data models were to be adopted.

This could also increase the volume of granular data available to supervisors, as needed to enable the use of advanced analytics.

In Phase 2, the project took existing large exposures regulatory data and integrated these with unstructured data.

Advanced analytics such as machine learning and natural language processing were applied to these data sources to make risk correlations and to analyse sentiment, alerting supervisors in real time of issues that might need further investigation.

Network analytics were also used to demonstrate how exposures could be mapped, indicating possible systemic risks to the banking system.

The Ellipse platform prototype was developed, which can extract insights from the mined data and display these via dashboards as early warnings for supervisory attention.

The second phase of Project Ellipse demonstrates how a single platform could be built so that authorities could benefit from "on demand" access to timely and integrated sources of data to help support and inform their supervisory assessments.

The BIS Innovation Hub's Project Ellipse is a prototype that authorities can test in their own environments and which may help them to explore new solutions.

It also presents an opportunity for the global regulatory community to further consider, explore and collaborate on common solutions to future-proof the data and analytical capabilities of supervisors.

To read more: https://www.bis.org/publ/othp48.pdf

Table 1 — Challenges of regulatory reporting

1 Template based, aggregated

Regulatory requirements are often template-based and call for aggregated data, meaning that data sets are fixed to a use case and hence the data received cannot be easily reused for other purposes. New reporting requirements are needed whenever additional or ad hoc information is needed.

2 Data are inconsistently described

Reporting data are often sourced from reporting firms' legacy data systems, which may not be integrated. This often results in heterogeneity of data for any given product or transaction – both within a bank and across different banks – as different systems will describe these data differently.

CHALLENGES FACED

3 Infrequent, backward looking

Regulatory reports are submitted to supervisors from reporting entities on an infrequent basis (eg every month or quarter). At times of heightened risk, the need for up-to-date data increases but, given the static nature of regulatory reports, supervisors may not have the timeliest data to make informed judgments.

4 Different sources of data are not integrated

Information contained in regulatory reports is often linked to other types of information that may point to emerging risks, but these sources of information are not connected. For instance, information sourced from market data and news often gives the first indication of emerging risks but it is difficult for supervisors to scan through the vast volumes of market and news data to assess which point to a need to take early action.

Table 2 — Possible solutions explored in Project Ellipse

1 Granular data

The collection of granular data from reporting entities could replace the need for authorities to request information using templates. It could also enable authorities to reuse those data for different use cases. Supervisory metrics could also be derived using granular data, as opposed to requiring reporting entities to aggregate the required data prior to submission.

2 Common data models

Differences in the description of data for similar products and transactions across banks can be addressed using data standards and common data models. Granular reporting requires a common understanding by authorities and financial institutions of what these data are, so that financial institutions can map their operational data to a common "input" before the required data can be reported. Supervisory metrics could then be derived using programmable rules that reference machine-readable and machine-executable common data models.

SOLUTIONS EXPLORED

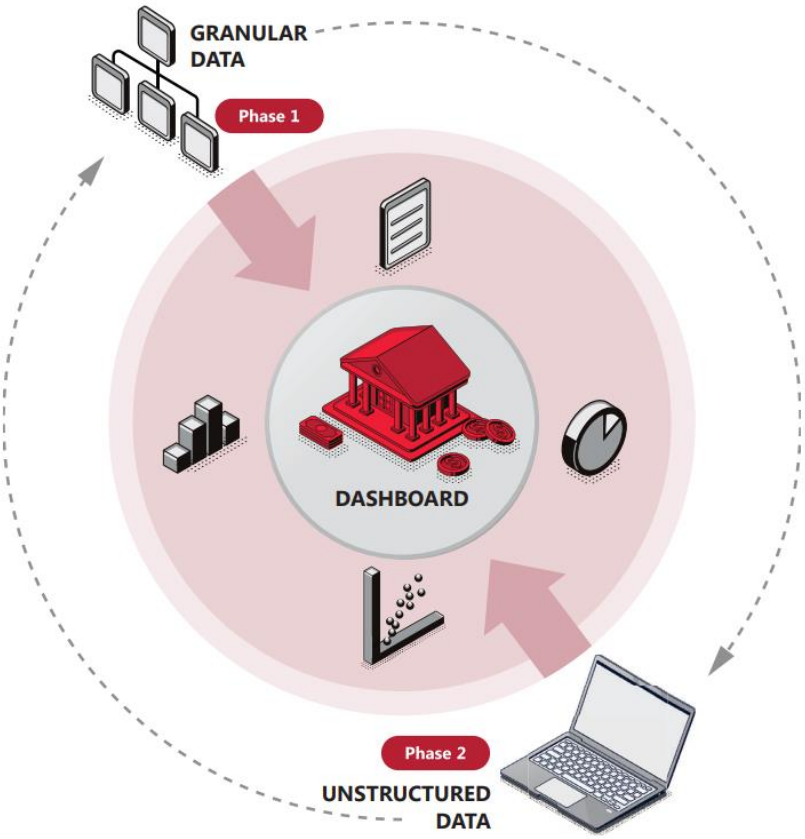
SOLUTIONS EXPLORED

3 Real-time information

Real-time insights using advanced analytics could be derived from large volumes of unstructured data that would supplement the granular reporting available. This would provide supervisors with additional indicators and early warnings of any at-risk exposures of reporting entities.

4 Integration of structured and unstructured data

Integrating granular data from reporting entities with other sources of unstructured information such as news and market data on the same platform would obviate the need for supervisors to spend time manually scanning for information. Advanced analytics such as AI and ML could be used to make risk correlations and analyse sentiment, alerting supervisors in real time of issues that may need further investigation.



Number 2

PCAOB Highlights Key Considerations for Auditors Related to the Russian Invasion of Ukraine

The Public Company Accounting Oversight Board (PCAOB) released a staff Spotlight document, "Auditing Considerations Related to the Invasion of Ukraine(PDF)." The Spotlight highlights important considerations for auditors of issuers and broker-dealers as they plan and conduct audits in this evolving environment.

"Beyond its terrible human toll, Russia's invasion of Ukraine has produced economic and market implications that are still taking shape," said PCAOB Chair Erica Y. Williams. "Our Spotlight addresses key considerations for auditors, starting with a reminder of their obligation to comply with PCAOB standards and to exercise due professional care, which may take more time or effort in highly challenging or unprecedented circumstances."

"Auditing Considerations Related to the Invasion of Ukraine" covers a range of audit-related matters, including identifying and assessing risks, planning and performing audit procedures, possible illegal acts, reviews of interim financial information, and acceptance and continuance of clients and engagements. For audits nearing completion, the Spotlight focuses on subsequent events, other information, and auditor reporting.

The Spotlight also reminds auditors to remain aware of developments that may affect the company. Knowledge obtained from past audits or interim

reviews may no longer be relevant in light of the current information environment. Therefore, it is important for the auditor to understand how changes in events, conditions, and company activities affect risks of material misstatement and whether those changes give rise to new or different risks.

Overview

The recent Russian invasion of Ukraine not only is affecting companies with operations in the region but also has the potential for farreaching economic impacts on companies operating across different jurisdictions.

We are providing this Spotlight to highlight important considerations for auditors of issuers and broker-dealers (collectively "companies") as they plan and conduct audits and reviews of interim financial information in this evolving environment.

Economic Implications

As a result of the military action, companies located (or with significant business ties) in Ukraine are experiencing major disruptions of their operations, including the loss of some or all of their physical assets and workforce.

Some companies may have idled or abandoned their production facilities and inventories in anticipation of escalating hostilities in the region.

In response to Russia's actions, many governments and international organizations have imposed various types of economic sanctions against Russia, certain Russian companies and products, and specific individuals.

Similar measures have also been imposed on Belarus for its role in the conflict.

Additionally, several major Russian banks have been removed from the network for international bank transfers (SWIFT), limiting their ability to make and receive international payments.

Further measures are also under consideration or being implemented, including US import and export restrictions of Russian goods and commodities, suspension of Russian securities from trading on US exchanges, bans of institutional investment in Russian securities, and limitations on Russian banks' ability to borrow funds.

These developments are likely to have a wide range of effects on many companies with business ties in the region, including supply and distribution chain disruptions, materials and other inventory shortages, significant increases in prices of raw materials and borrowing costs, and loss of liquidity.

Additionally, many global companies have made public statements that they would not do business in or with Russia, including intentions to close operations in Russia and boycott goods produced and sold by Russian companies.

These boycotts may continue for the foreseeable future. Some organizations, including accounting firms, have also announced that they are cutting ties with their Russian affiliates.

These events also have broader global economic implications.

Rising global inflation, driven partially by sanctions on Russia and supply chain issues, and the region's market strength in oil and other commodities markets, may lead to higher interest rates.

This in turn may increase borrowing costs for a variety of companies in various industries, whether or not they have direct business ties to the region.

Fluctuations in foreign currencies, rising oil and gas prices, and volatility in some equity and commodity markets may also negatively affect some companies.

As the potential economic impacts of the conflict continue to evolve rapidly, continuous monitoring of the situation and reassessing relevant implications remain important.

AUDIT AND INTERIM REVIEW CONSIDERATIONS

The financial statement effects from the events surrounding the Russian invasion ("current environment") are likely to vary significantly depending on a company's geographic location, industry, and other factors.

Further, the effects on some companies and industries may be longer-lasting whereas for others the effects may be only temporary.

As the situation evolves, auditors should remain aware of developments and the potential for broader economic issues that could in turn affect more companies.

Auditors may also be faced with certain challenges in completing audits of affected companies.

In some cases, obtaining sufficient appropriate audit evidence to support the auditor's opinion on the financial statements may take longer or require more audit effort.

Nonetheless, auditors are required to comply with PCAOB standards and exercise due professional care, which requires that auditors exercise professional skepticism.

Identifying and Assessing Risks

The auditor has a fundamental responsibility to identify and assess risks of material misstatement, due to error or fraud, and design and implement overall responses that address those risks.

Risks of material misstatement can arise from a variety of sources, including external factors, such as economic, legal, and political conditions in the company's industry and environment.

In times of unrest and economic uncertainty, a company's environment may change quickly.

Knowledge obtained from past audits or interim reviews may no longer be as relevant.

It is important for the auditor to understand how changes in events, conditions, and company activities affect risks of material misstatement and whether those changes give rise to new or different risks (as described in the following examples).

- Supply chain disruptions, whether from continuing to rely on Russian counterparts or from severing ties with them, may affect a company's ability to meet contractual obligations.

- A decision to boycott a key supplier, suspend sales to a key customer, or abandon investments in Russian entities may have longer-term negative effects on projected earnings.

- Companies choosing to continue doing business with certain Russian entities or individuals may have reputational risks, while companies with significant operations in Russia may experience boycotts of their products or operations.

- A company may not be able to regularly access funds through short-term borrowings and may have other liquidity issues, casting doubt about the company's ability to continue as a going concern.

- Changing circumstances may force an unplanned reallocation of resources (e.g., closure of shared service centers used by the company) or shutdown of subsidiaries or product lines.

- Heightened volatility and uncertainty may result in market and counterparty risk for some broker-dealers.

Fraud Risks

The current environment may also create opportunities, incentives, and pressures to commit fraud.

For example, company management may be motivated to downplay the effects of economic sanctions and make financial results more favorable to meet the expectations of third parties.

Fraud risks may also arise from companies potentially doing business with sanctioned entities. (See "Possible Illegal Acts" discussion below.)

Communication among engagement team members about significant matters affecting the risks of material misstatement should continue throughout the audit, including when conditions change.

Cybersecurity Risks

The economic volatility in the current environment can pose an increased risk of cybersecurity attacks.

In response to economic sanctions and boycotts, there may be increased incentive and opportunity for hackers to launch ransomware attacks or take advantage of potential weaknesses in companies' information systems. Some companies (e.g., those with multinational operations) and industries (e.g., financial institutions, utility companies) may be more likely targets of these attacks.

It is important for auditors' risk assessment procedures to include an understanding of how companies are addressing cybersecurity risks specific to the current environment with a focus on potential financial reporting impacts.

Planning and Performing Audit Procedures

The nature and extent of planning activities that are necessary depend on, among other things, changes in circumstances that occur during the audit.

Audit planning is not a discrete phase of an audit but rather a continual and iterative process.

As conditions in the company's environment evolve, auditors may need to revisit their initial assessment of risks and modify planned audit procedures.

In some cases, auditors may need to perform additional or different audit procedures to obtain sufficient appropriate audit evidence compared to those performed in prior audits.

The nature of the circumstances facing the company may pose unique challenges for the auditor. For example, audit evidence may not be available in the form originally expected (e.g., inability to obtain confirmations).

As a result, auditors may need to revise the nature, timing, and extent of audit procedures (e.g., performing new or extended procedures).

Materiality

The current environment may also cause the auditor to re-evaluate materiality and tolerable misstatement (e.g., if the auditor initially established materiality and tolerable misstatement based on estimated or preliminary financial statement amounts that differ significantly from actual amounts).

Changes in materiality can also affect the auditor's evaluation of audit results and the determination as to whether sufficient appropriate audit evidence has been obtained.

Internal Control Over Financial Reporting

Modifications to the company's operating structure and business processes may affect its flow of transactions, financial reporting processes, and related controls.

For example, control owners may no longer have access to information necessary to complete their assigned roles, which may lead to implementation of new or modified processes and controls.

In some cases, new controls may have been implemented to address evolving areas, or new control owners may be involved.

For example, controls over contracts may have been modified to include additional evaluation for compliance with laws and regulations as a result of government sanctions.

The rapidly changing environment further exacerbates the potential for disruptions to the timing and operation of certain controls, including ITrelated and review-type controls.

The auditor's procedures to understand, select, and test relevant controls may need to be modified to address the increased risk of deficiencies posed by these changes (e.g., potential lack of segregation of duties and risk of management override).

You may visit:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/documents/auditing-considerations-related-invasion-ukraine-spotlight.pdf?sfvrsn=19dc6043_3

Number 3

The return of inflation

Agustín Carstens, General Manager of the BIS at the International Center for Monetary and Banking Studies, Geneva

Thank you very much for inviting me to give this lecture. It is a pleasure and an honour to be here today.

Being the BIS's General Manager, it will not come as a surprise to you that I have decided to devote my presentation to the issue that is top of mind for policymakers around the world, namely the return of inflation.

After more than a decade of struggling to bring inflation up to target, central banks now face the opposite problem.

The shift in the inflationary environment has been remarkable.

If you had asked me a year ago to lay out the key challenges for the global economy, I could have given you a long list, but high inflation would not have made the cut.

This evening, I will describe the rise in inflation over the past year and discuss why this came as a surprise to many.

I will argue that the pandemic and the extraordinary policy response laid the groundwork for a rapid and goods-intensive bounceback in demand which supply has been unable to fully meet.

The war in Ukraine has further disrupted supply, particularly for commodities.

I will also draw some broader lessons about the inflationary process – in particular, the need to look "under the hood" of aggregate data and models to understand how the behaviour of individual firms and workers drives inflation outcomes.

A key message is that we may be on the cusp of a new inflationary era. The forces behind high inflation could persist for some time.

New pressures are emerging, not least from labour markets, as workers look to make up for inflation-induced reductions in real income.

And the structural factors that have kept inflation low in recent decades may wane as globalisation retreats.

If my thesis is correct, central banks will need to adjust, as some are already doing.

For many years now, having conquered inflation, they have had unprecedented leeway to focus on growth and employment.

Indeed, with inflation stubbornly below target, stimulating activity hit two birds with one stone.

But this is now no longer possible, since low and stable inflation must remain the priority.

If circumstances have fundamentally changed, a change in paradigm may be called for.

That change requires a broader recognition in policymaking that boosting resilient long-term growth cannot rely on repeated macroeconomic stimulus, be it monetary or fiscal.

It can only be achieved through structural policies that strengthen the productive capacity of the economy.

To read more: https://www.bis.org/speeches/sp220405.pdf

Number 4

Is that a Fish Behind the Wheel?

SEC Commissioner Hester M. Peirce, before the University of Central Florida's Inaugural FinTech Summit

Thank you, Barry [Miller]. Thank you also to Professor Ajai Singh. It is a pleasure to be part of the University of Central Florida's inaugural FinTech Summit. This morning, I would like to discuss the ways in which financial regulators ought to engage with innovation. Before I begin, I will give my standard disclaimer: the views I express are my own and not necessarily those of the Securities and Exchange Commission ("SEC") or my fellow Commissioners.

I do not think like, or have the skills of, a technologist. A recent scientific article that got picked up by the mainstream press brought that home to me. The article reported on an experiment in which the authors had created a terrestrial vehicle on wheels that could be navigated by goldfish in a tank sitting on the vehicle's chassis.

The "Fish Operated Vehicle" moved in response to the fish's movements in the tank, and the fish got a food pellet reward for reaching a target. The bottom line is that, as the researchers reported, "a fish was able to transfer its space representation and navigation skills to a wholly different terrestrial environment, thus supporting the hypothesis that the former possess a universal quality that is species-independent."

In other words, fish can drive. And they can drive well enough to put to shame my sixteen year-old self, having piloted the family van into a ditch by the side of the road.

In addition to being a lousy teenage driver, I also never would have thought to create a Fish Operated Vehicle, and, even if I had thought to create one, I could not have done so. I admire people who ask unusual and difficult questions, devise ways to get answers, and then translate those answers into something that improves society—that piece of the fish experiment may be yet to come, but I am sure that it is coming.

Sometimes the process of conceiving an idea and translating it into something useful takes a long time and involves many people, not

necessarily working together or even aware of each other. At any point along the way, an outside observer looking into the technologist's fish bowl might be asking, "Why are you doing this?" The wonderful thing about human society is that we all bring something different to the table, and the combined ingenuity of a diverse set of people enables us to achieve things none of us would on our own. Bringing together multiple disciplines, your inaugural event today embodies that spirit, which is why I am so pleased to be part of it.

FinTech too is the product of interdisciplinary efforts. Technologies developed far outside of the financial sphere turn out to be useful to investors and the people who serve them. Fish Operated Vehicle technology may not transfer into the capital markets anytime soon, but mobile technology, supercomputing, artificial intelligence, virtual reality, and cryptography, among many other technologies, already have made the leap.

Regulation influences whether, how, and when technology finds its way into the financial markets. I would like to talk today about three ways regulators should engage with innovation.

First, regulators need to approach technology with a mix of skepticism and wonder.

Second, regulators need to embrace the idea that new technology can make it easier to achieve worthy regulatory objectives.

Third, regulators need to leave space for experimentation, tinkering, and even failure.

These ideas about how regulation and technology should interact are not intended to be a complete framework for that interaction, but only themes that should inform that interaction. Let me discuss each of these ideas in turn.

Embrace both skepticism and wonder.

People are skeptical of new things, including innovations that end up transforming their lives.

The oft-replayed Bill Gates-David Letterman colloquy in 1995 about the computer and the internet is an example of how people approach innovation.

Letterman—likely giving the voice to the skepticism of most of the American public—asks "What about this internet thing?"

Gates explains that people are using the internet to publish information and send electronic mail and enthusiastically explains: "It's wild what's going on. It is the big new thing." An unimpressed Letterman, conceding that "it's easy to criticize something that you don't fully understand," pushes back on the then uses of the internet as not innovative at all:

I can remember a couple of months ago there was . . . a big breakthrough announcement that on the internet or on some computer deal they were going to broadcast a baseball game . . . and I just thought to myself, "Does radio ring a bell?"

Gates gives Letterman several other examples of how the internet might be used, but Letterman dismisses these too, although he does admit "I think one day I'll get one of these deals," by which he meant a computer. Yes, he would, and it would be hooked up to the internet too.

Matt Ridley, providing many wonderful examples of similar attitudes in his recent book on innovation, suggests that this skepticism is a perennial feature of human social and cultural life. He gives the example of the introduction of the potato to Europe five hundred years ago—a time when the calorie content of potatoes would have been a very welcome addition to people's diets.

According to Ridley, people's tuber trepidation was rooted in part in a popular theory of the day that because potatoes look like leprous fingers, they cause leprosy. Although their reasons for dismissing today's new things may sound more sophisticated, people's reluctance to embrace new things is the same as it was back then.

Regulators share this fundamental human trait. Just as other people, regulators like dealing with known quantities: a rulebook they have mastered; familiar regulated entities that know and love the rulebook almost as well as the regulators do; and time-tested technologies and business processes that fit neatly into that rulebook.

But this affection for the familiar is typically even more pronounced among regulators. For one thing, regulatory agencies draw very smart and talented, but risk-averse, employees, many of whom are lawyers, a profession not known to be entrepreneurial; I can say so in this crowd of engineers and business people.

For another, regulators generally operate under incentives that make them look skeptically at the unknown and the new: They are rarely rewarded for innovation, and any performance metrics generally measure their productivity in numbers of rules, exams, or enforcement actions.

Doing things the way they have always been done—which is probably also the way that saw the regulator's predecessors off to a happy, fulfilling retirement—seldom carries significant risk. Departure from tried-and-true methods, on the other hand, creates all sorts of risks.

These features of bureaucratic life create an environment that often is indifferent, or even hostile, to innovation. Innovations almost always disrupt existing ways of doing things.

They can render currently successful products and services obsolete or passé; even worse, from a regulator's perspective, they bring unfamiliar participants to the agency's doors, unwanted guests bearing undesirable gifts in the form of knotty problems that do not fit neatly into a regime that works just fine, thank you very much.

Moreover, the significance—or even the point—of the innovation may not be immediately clear to the regulator, or to anybody besides the innovator; in some cases, she may not even understand the full significance of her own innovation.

Consider the automobile. Although H.G. Wells and others predicted soon after the introduction of this novel method of locomotion many of the ways that this new technology would change our lives, nobody was able to foresee that the automobile would become a near-universal mode of transport, even for working men and women, in industrial societies.

As Matt Ridley notes, this inability to understand the significance of innovations, even among experts in the field, is a constant theme in the history of technological breakthroughs.

Why would a rational regulator choose to approve the introduction of a technology or product the benefits of which may seem clear only in retrospect, especially at the risk of disrupting a market that is operating to the general satisfaction of incumbent players, many of their customers, and of course the regulator herself?

If this instinctive skepticism toward innovation is so universal, how can regulators, also human but facing incentives to exercise even more skepticism than typical and acting out of a genuine concern for investors, learn to take a more positive attitude toward the possibilities of innovation?

This question is a perennial one for those concerned about the relationship between regulation and innovation and has no easy answers. But I do think that we financial regulators might benefit from recovering a sense of wonder at the history of innovation that built the financial markets that

have made possible the modern American economy. Further reflecting on the opposition that those innovators faced—and on what might have been lost had those opponents prevailed—should lead us to greater humility as we consider innovations in the markets we regulate today.

Because these markets are highly regulated—including even the trading venues themselves, whose nearly every rule we must approve—it is easy to fall into thinking that they are our creation, that the U.S. has the world's largest, most liquid markets because we crafted just the right rule set. But this just is not so.

Take the stock exchange: In the late 17th and early 18th century, this institution was just getting started in London in a big way. It was not created by an Act of Parliament or a royal edict.

In fact, as interest in trading government debt and company shares in the secondary market developed at the Royal Exchange, which had long been a venue for reputable merchants to meet and trade, the dealers in these securities—or stockjobbers, as they were called—soon found themselves unwelcome.

They were rowdy, a bit déclassé, and the quality merchants apparently did not want them making a scene where proper business was done.

The government also saw them as a threat and a nuisance and, in 1697, passed an "An Act to restraine [sic] the Number and ill Practice of Brokers and Stock-Jobbers."

The Act described stock-jobbing as "a very great abuse of the [] ancient Trade and Employment and extremely prejudicial to the public Credit of this Kingdom and to the Trade and Commerce thereof."

Indeed, the Act thundered, if this activity is not "timely prevented," it "may ruin the Credit of the Nation and endanger the Government itself."

The stockjobbers did not disappear, of course; they simply decamped to a friendlier neighborhood, just a couple blocks away where a number of coffeehouses—another recent innovation, also disfavored and briefly banned by the authorities—had set up shop.

Jonathan's Coffee House and another shop called Garraway's, in Exchange Alley, conveniently located between the Royal Exchange and the Post Office, would soon become the hub of trading in stocks and government debt.

Barriers to entry were not terribly high. Thomas Mortimer, writing in the 1760s, explained what it took to set oneself up as a broker in Jonathan's Coffee House:

Every person who enters Jonathan's to do any business there, pays 6 [pence] at the bar, for which he is entitled to firing, pen, ink, and paper, and a small cup of chocolate; and if he understands the business, is as good a Broker for that day (at least for his own affairs) as the best.

The brokers and stockjobbers continued to irritate the government and the more respectable sort of merchants. The government repeatedly sought to make many types of transactions illegal, but not only did these trades continue to occur, the brokers themselves routinely performed, and enforced performance, on these contracts that could not be enforced in a court of law.

Over time, they formalized these practices into private rules and regulations to govern their conduct.

Of course, although the accusations leveled at the stockjobbers were not the whole story, they did have some basis in fact. The innovation of a largely self-regulated market for securities led to innovations in various forms of misconduct as well. Information, then as now, was a prized commodity, and schemes to disseminate false information, or to use deception to obtain confidential information, were common. This conduct led observers like Daniel Defoe to rail against the trade:

To read more:
https://www.sec.gov/news/speech/peirce-remarks-fintech-summit-040122

Number 5

FSB Work Programme for 2022

The Financial Stability Board's (FSB) work programme for 2022 aims to maximise the value of the FSB's global and cross-sectoral approach to financial stability policy.

The FSB's work priorites reflect that financial challenges are global in nature and affect the financial system as a whole.

These challenges include digitalisation, climate change and potentially also shifts in the macroeconomic and interest rate environment.

This note summarises the ongoing and planned FSB initiatives in 2022 organised by:

(1) priority areas of work and new initiatives;

(2) work programme items that are continuing or reaching completion; and

(3) regular monitoring and reporting.

The Annex provides an indicative timeline of the FSB's publications planned for 2022.

1. Priority areas of work and new initiatives

Supporting international cooperation and coordination on current financial stability issues.

The FSB, with its broad and diverse membership of national authorities, international standard setters and international bodies, continues to promote financial stability in a rapidly evolving financial market environment.

Against the backdrop of the Russia-Ukraine conflict and its economic impacts, the FSB is reinforcing its forward-looking monitoring to identify, assess and address new and emerging risks to global financial stability.

This enhanced monitoring is informed by the FSB's new surveillance framework.

Work will also continue on policy responses to COVID-19, including: sharing information on policy responses and the timely unwinding of the temporary measures adopted in response to COVID-19, and assessing the effectiveness of those measures; and monitoring, with the standard-setting bodies (SSBs), the use of flexibility within international standards and consistency of policy responses with existing international financial standards.

- Work on the financial stability implications of current developments will continue in a flexible mode – including on specific vulnerabilities, policy issues and monitoring – and be adjusted as needed.

- FSB will work with SSBs to follow up on specific issues identified in the report on lessons learnt from COVID-19 for financial stability, including macroprudential aspects of buffer functioning.

- At the request of the Indonesian G20 Presidency, the FSB will report to the G20 on exit strategies to support equitable recovery for financial stability, and on effective practices and policy recommendations for addressing the effects of COVID-19 scarring in the financial sector.

Enhancing the resilience of the non-bank financial intermediation (NBFI) sector, while preserving its benefits.

The FSB will advance its work programme for strengthening the resilience of NBFI.

This work, set out in the FSB's holistic review of the March 2020 market turmoil, will be carried out within the FSB as well as by SSBs and international organisations.

- In 2022, remaining work on specific issues identified in the holistic review will be completed, including on open-ended funds (OEFs); margining practices; the liquidity, structure and resilience of core bond markets; and USD funding and emerging market economy (EME) vulnerabilities.

- In addition, work will focus on developing a systemic approach to NBFI. This includes enhancing the understanding of systemic risks in NBFI and strengthening their ongoing monitoring; and developing policies to address such risks.

Enhancing cross-border payments.
The FSB roadmap for enhancing cross-border payments contains a large number of actions, guided by a set of quantitative targets.

To help achieve these targets, specific proposals for material improvements to existing payments systems and arrangements are being discussed, as well as the development of new systems.

The FSB will continue to coordinate with CPMI and other SSBs and international organisations in implementing the FSB roadmap to enhance cross-border payments.

- In 2022, the FSB has committed to complete a number of actions under the roadmap, including the development of an approach to monitor progress against the quantitative targets; identification of gaps or areas for enhanced implementation in standards; and work on enhancing data sharing.

- The FSB will deliver to the G20 a progress report on the overall roadmap and the development of key performance indicators to monitor progress towards the quantitative targets.

To read more: https://www.fsb.org/wp-content/uploads/P310322.pdf

Number 6

Official Statistics

Cyber Security Breaches Survey 2022

GOV.UK

The Cyber Security Breaches Survey is an influential research study for UK cyber resilience, aligning with the National Cyber Strategy. You may visit: https://www.gov.uk/government/publications/national-cyber-strategy-2022

HM Government

National Cyber Strategy 2022

Pioneering a cyber future with the whole of the UK

It is primarily used to inform government policy on cyber security, making the UK cyber space a secure place to do business. The study explores the policies, processes, and approaches to cyber security for businesses, charities, and educational institutions. It also considers the different cyber attacks these organisations face, as well as how these organisations are impacted and respond.

Our survey results show that in the last 12 months, 39% of UK businesses identified a cyber attack, remaining consistent with previous years of the survey. However, we also find that enhanced cyber security leads to higher identification of attacks, suggesting that less cyber mature organisations in this space may be underreporting.

Of the 39% of UK businesses who identified an attack, the most common threat vector was phishing attempts (83%). Of the 39%, around one in five (21%) identified a more sophisticated attack type such as a denial of service, malware, or ransomware attack. Despite its low prevalence, organisations cited ransomware as a major threat, with 56% of businesses having a policy not to pay ransoms.

Within the group of organisations reporting cyber attacks, 31% of businesses and 26% of charities estimate they were attacked at least once a week. One in five businesses (20%) and charities (19%) say they experienced a negative outcome as a direct consequence of a cyber attack,

while one third of businesses (35%) and almost four in ten charities (38%) experienced at least one negative impact.

Looking at organisations reporting a material outcome, such as loss of money or data, gives an average estimated cost of all cyber attacks in the last 12 months of £4,200. Considering only medium and large businesses; the figure rises to £19,400. We acknowledge the lack of framework for financial impacts of cyber attacks may lead to underreporting.

Around four in five (82%) of boards or senior management within UK businesses rate cyber security as a 'very high' or 'fairly high' priority, an increase on 77% in 2021. 72% in charities rate cyber security as a 'very high' or 'fairly high' priority. Additionally, 50% of businesses and 42% of charities say they update the board on cyber security matters at least quarterly.

Figure 2.3: Percentage that have any staff using personally owned devices to carry out regular work-related activities

Change to table and accessible view

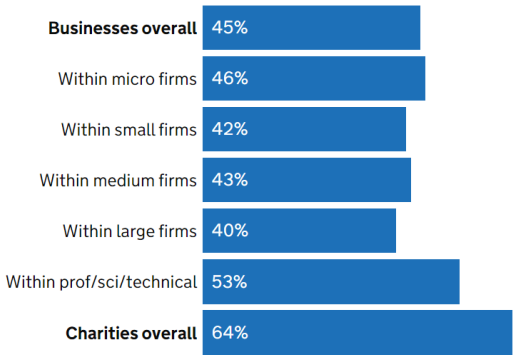


Figure 2.4: Percentage or organisations that have older versions of Windows installed

Change to table and accessible view

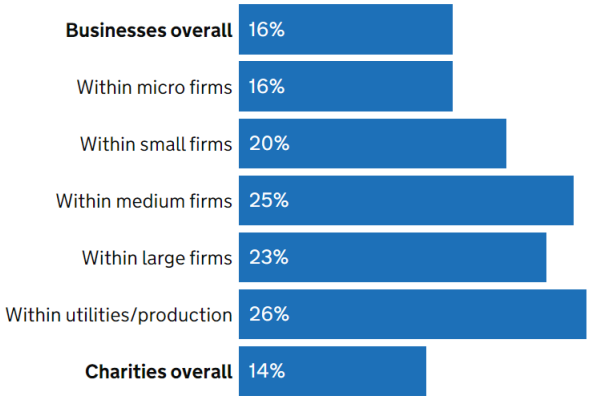


Figure 3.4: Percentage of organisations with board members or trustees that have responsibility for cyber security

Bases: 658 UK businesses; 364 micro firms; 147 small firms; 86 medium firms; 62 large firms; 71 information and communications firms; 66 health and social care; 185 charities; Only sample half A was asked.

Figure 4.2: Percentage of organisations that have carried out work to formally review the potential cyber security risks presented by the following groups of suppliers

Bases: 1,243 UK businesses; 696 micro firms; 264 small firms; 149 medium firms; 134 large firms; 82 finance or insurance firms; 424 charities

To read more:
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

Number 7

Variation in the Inflation Experiences of Households

Governor Lael Brainard, at the Spring 2022 Institute Research Conference, Opportunity and Inclusive Growth Institute, Federal Reserve Bank of Minneapolis, Minneapolis, Minnesota

It is a pleasure to join you to discuss differences in how households at different income levels experience inflation. I look forward to hearing from the panelists, who are doing important and interesting research on this topic.

By law, the Federal Reserve is assigned the responsibility to pursue price stability and maximum employment. The Federal Open Market Committee (the Committee) has long recognized the connection between stable, low inflation and maximum employment.

Forty years ago, Paul Volcker noted that the dual mandate isn't an either-or proposition and that runaway inflation "would be the greatest threat to the continuing growth of the economy… and ultimately, to employment."

Maximum employment and stable, low inflation benefit all Americans, but are particularly important for low- and moderate-income families.

The combination of good job opportunities and stable, low inflation provides purchasing power to fill up gas tanks and grocery carts and pay housing and medical costs, leaving room to build emergency cushions and invest in education; retirement; and, for some, small businesses.

Indeed, the Employment Act of 1946 called on the federal government to promote "maximum employment, production, and purchasing power."

While national data do not directly disaggregate the differential effects of inflation by household income groups, a variety of evidence suggests that lower-income households disproportionately feel the burden of high inflation.

Lower-income families expend a greater share of their income on necessities; have smaller financial cushions; and may have less ability to switch to lower-priced alternatives.

Arthur Burns noted in the late 1960s that "there can be little doubt that poor people…are the chief sufferers of inflation."

Today, inflation is very high, particularly for food and gasoline. All Americans are confronting higher prices, but the burden is particularly great for households with more limited resources.

That is why getting inflation down is our most important task, while sustaining a recovery that includes everyone. This is vital to sustaining the purchasing power of American families.

Whose Cost of Living?

In assessing inflation faced by American consumers, economists and policymakers generally rely on the change in the consumer price index (CPI) or the change in the price index for personal consumption expenditures (PCE).

Since January 2012, the Committee's price-stability goal has been specified as a longer-run goal of 2 percent in terms of annual PCE inflation.

Both CPI and PCE inflation metrics are assembled from a collection of underlying elementary price indexes for narrow subsets of goods and services.

The price changes each month for the goods and services in these subsets are combined into measures of overall inflation by calculating a weighted average of all these subindexes, where the weights are based on average aggregate consumer expenditures in each category.

Using a national average of consumer expenditures to weight the categories has intuitive appeal. This measure is particularly useful, for example, in adjusting measures of overall expenditure for changes in prices to determine how much real growth has occurred between two periods.

However, using a national average of expenditures to weight the categories has limitations when it comes to representing the true cost of living experienced by different types of households.

U.S. Households Have Different Inflation Experiences

Each household in the United States has a particular consumption bundle whose prices and quantities combine to make up that household's cost of living.

If we could start with each individual household's cost of living and aggregate across households by giving equal weight to each household, it would create an economy-wide cost-of-living index.

The change in such a cost-of-living index would represent the average inflation experienced by U.S. households.

Instead, because the CPI and PCE indexes weight every dollar of expenditure equally, these indexes implicitly weight each household's cost of living proportionally to their total expenditure.

Since lower-income households represent a relatively smaller share of overall expenditure, the inflation associated with their consumption baskets is underrepresented in the official consumer price indexes.

It would be useful to have data about consumer inflation broken out by demographic groups, similar to labor market and personal-income data, in order to assess the differential effect of inflation across different groups of households.

U.S. statistical agencies do not collect the information needed to accurately assess inflation at a household level, and it would require a large change in the way these agencies go about their work to do so.

Nonetheless, recent research has begun to assess variation in the ways different households experience inflation.

Households at different income levels could experience differential inflation effects for several reasons: Consumption shares could differ systematically for low- and high-income households; the goods and services within each consumption category could differ; the ability to substitute for lower-priced alternatives of the same item could differ; and prices paid for the same good could differ systematically due to differences in access. I will briefly touch on these four reasons.

First, low- and moderate-income households could experience inflation that diverges from the average because their consumption baskets differ systematically from the average.

Lower-income households spend 77 percent of their income on necessities — more than double the 31 percent of income spent by higher-income households on these categories.

Several studies have found that the consumption baskets of lower-income households have experienced higher-than-average inflation rates over time.

Research from the Bureau of Labor Statistics (BLS) has examined the effect of different consumption baskets by using the same elementary price indexes as used in the official CPI but assigning the weights of these components to reflect the consumption bundles of different types of households.

A 2021 working paper by BLS staff based on data from 2003 to 2018 found that a price index reflecting the consumption basket for households in the lowest-income quartile grew faster than the overall CPI, while a price index reflecting the consumption basket for households in the highest-income quartile grew more slowly than the overall CPI.

A 2015 BLS study found a similar result using data from 1982 to 2014.

Of course, the recent sharp increases in inflation may have affected the consumption bundles of lower-income households relative to the average differently than in previous cycles.

While these studies allow for differences in the weighting of price indexes across different income groups, they rely on the same elementary price indexes for subcategories of goods and services. As a result, they may miss additional sources of variation in the inflation rates experienced by households at different income levels.

This consideration brings us to the second point: Households with different levels of income may purchase significantly different items even within the same elementary index categories for goods and services.

To take an extreme example, caviar and canned tuna are both in the same elementary index. The demand and supply dynamics for those products are likely quite different, meaning that their relative price dynamics are poorly described by a single index.

Third, households at different income levels may have differing abilities to substitute for lower-priced alternatives within an elementary category.

Consider a price increase for a breakfast cereal that increases the prices of both the brand-name cereal and the corresponding lower-priced store-brand cereal but maintains a differential between them.

A household that had been purchasing brand-name cereal could save money by purchasing store-brand cereal instead, perhaps even eliminating any effect of the price increase on their actual spending while purchasing the same quantity of cereal in that narrow category.

However, a household that was already purchasing the store brand would have to either absorb the increase in cost or consume less within that category.

Finally, beyond the variation in inflation that comes from households buying different goods, research also shows that differences in inflation can result from households paying different prices for identical goods.

Using transaction-level data, researchers found that almost two-thirds of the variation in inflation across households comes from differences in prices paid for identical goods, with only about one-third coming from differences in the mix of goods within broad categories.

As a result of these differences, households with lower incomes, more household members, or older household heads experienced higher inflation on average.

Variations in the prices paid for identical goods could reflect differences in the ability of some households to stock up when prices are discounted or to buy in bulk and save—options only available to households with the means to buy in larger quantities, adequate capacity to store larger quantities, or the flexibility to delay purchases if there is an opportunity to save in the future.

In addition, evidence suggests that inflation could be lower for items purchased online rather than from brick-and-mortar stores, suggesting that households who do not have full access to online shopping options could face a higher cost of living.

One study of online transactions made between 2014 and 2017 found that online inflation averaged more than 1 percentage point per year lower than the equivalent CPI measure of the relevant product categories.

We are only beginning to understand the ways in which inflation experiences vary from household to household, how this variation correlates with income and demographic information, and how these divergent inflation experiences change over time.

This developing area of research will benefit from conferences like this one that help expand the frontier of our knowledge about the heterogeneity of experienced inflation.

Implications for the Outlook and Policy

High inflation places a burden on working families who are concerned about how far their paychecks will stretch as well as seniors living on fixed incomes. So now let me turn briefly to what we are seeing on inflation and the outlook for jobs and growth.

Headline PCE inflation for February came in at 6.4 percent on a 12-month basis. Food and energy account for an outsized one-fourth share of this high level of inflation and also constitute an outsized share of expenditure for lower-income Americans, who spend 26 percent of their income on food at home and transportation, compared with 9 percent for high-income Americans.

Core inflation is also elevated, and inflationary pressures have been broadening out. Housing contributed about one-tenth of total PCE inflation in February and is the single greatest category of expenditures by far for lower-income Americans, who spend 45 percent of their income on housing, compared to 18 percent for high-income Americans.

Durable goods inflation, particularly in autos, accounted for slightly more than one-fifth of total PCE inflation in February, representing a much greater contribution to inflation than was the case pre-pandemic.

High durable goods inflation reflects pandemic-related supply constraints as well as persistently elevated demand associated with the pandemic.

I will be carefully monitoring the extent to which demand rotates back to services and away from durable goods, where it has remained consistently above pre-pandemic levels, and the extent to which the services sector is able to absorb higher demand without generating undue inflationary pressure.

Russia's invasion of Ukraine is a human tragedy and a seismic geopolitical event. The global commodity supply shock associated with Russia's actions skews inflation risks to the upside and is expected to exacerbate high prices for gasoline and food as well as supply chain bottlenecks in goods sectors. The recent COVID lockdowns in China are also likely to extend bottlenecks.

These geopolitical events also pose downside risks to growth. That said, the U.S. economy entered this period of uncertainty with considerable momentum in demand and a strong labor market.

As of the March labor report, payroll employment has increased at a pace of 600,000 jobs per month over the past six months, and the unemployment rate has fallen by a percentage point over that period and is now close to its pre-pandemic level.

In contrast, until recently, the recovery in labor force participation was lagging far behind.

So it is particularly noteworthy to see that the pandemic constraints on labor supply are diminishing for the prime-age workforce: The prime-age participation rate jumped 0.7 percentage points for women in March, following a similar-sized jump for men in February.

An increase in labor supply associated with diminishing pandemic constraints combined with a moderation in demand associated with tightening financial conditions, slowing foreign growth, and a large decrease in fiscal support could be expected to reduce imbalances later in the year.

Against that backdrop, I will turn to policy. It is of paramount importance to get inflation down. Accordingly, the Committee will continue tightening monetary policy methodically through a series of interest rate increases and by starting to reduce the balance sheet at a rapid pace as soon as our May meeting.

Given that the recovery has been considerably stronger and faster than in the previous cycle, I expect the balance sheet to shrink considerably more rapidly than in the previous recovery, with significantly larger caps and a much shorter period to phase in the maximum caps compared with 2017–19.

The reduction in the balance sheet will contribute to monetary policy tightening over and above the expected increases in the policy rate reflected in market pricing and the Committee's Summary of Economic Projections.

I expect the combined effect of rate increases and balance sheet reduction to bring the stance of policy to a more neutral position later this year, with the full extent of additional tightening over time dependent on how the outlook for inflation and employment evolves.

Our communications have resulted in broad market expectations for an expeditious increase in the policy rate toward a neutral level and a more rapid reduction in the balance sheet compared with 2017–19.

Consistent with these expectations, we have already seen significant tightening in market financing conditions at longer maturities, which tend to be most relevant for household and business decisionmaking.

For instance, 30-year mortgage rates have increased more than 100 basis points in just a few months and are now at levels last seen in late 2018.

Looking forward, at every meeting, we will have the opportunity to calibrate the appropriate pace of firming through the policy rate to reflect what the incoming data tell us about the outlook and the balance of risks. For today, every indicator of longer-term inflation expectations lies within the range of historical values consistent with our 2 percent target.

On the other side, I am attentive to signals from the yield curve at different horizons and from other data that might suggest increased downside risks to activity. Currently, inflation is much too high and is subject to upside risks.

The Committee is prepared to take stronger action if indicators of inflation and inflation expectations indicate that such action is warranted.

We are committed to bringing inflation back down to its 2 percent target, recognizing that stable low inflation is vital to maintaining a strong economy and a labor market that works for everyone.

Number 8

Fake WhatsApp 'voice message' emails are spreading malware

A phishing campaign which impersonates WhatsApp's voice message feature has been spreading information-stealing malware.

The attack starts with an email claiming to be a notification from WhatsApp of a new private voice message. The email contains a creation date and clip duration for the supposed message, and a 'Play' button.

The identity 'Whatsapp Notifier' masks a real email address belonging to a Russian road safety organisation. As the address and organisation are real, the messages aren't flagged as spam or blocked by email security tools. Armorblox, who discovered the scam, believe the Russian organisation is playing a role without realising.

The 'Play' button will take the email recipient to a website which then asks them to click 'Allow' in an allow/block prompt to 'confirm you are not a robot'. Once 'allow' is clicked, the browser will prompt to install software that turns out to be information-stealing malware.

While there are numerous 'tells' that this is a scam, these attacks rely on people missing the signs – perhaps because they are waiting for urgent or exciting news that could well be delivered by a voice message.

The NCSC has published guidance on how to spot and report scams, including those delivered by email and messaging. You may visit: https://www.ncsc.gov.uk/collection/phishing-scams

GUIDANCE

Phishing: Spot and report scam emails, texts, websites and calls

How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you.

Our top tips for staying secure online will help you keep your devices and information secure even if you do click on a scam, and you can also learn how to recover a hacked account.

As of March 2022 the NCSC has received over:

11m reported scams

Which has resulted to:

78k scams being removed across 144,000 urls

Number 9

Capability Assessment for StratCom:

Using the New Risk Perspective to Inform the Development of Effective Response Capability Assessments for Countering Information Influence Operations

There are no established models for assessing an organisation's capability to respond to *information influence operations (IIOs)*.

While great efforts have been made to improve our knowledge and understanding of IIOs and how to counter them, and measures have been taken to strengthen democratic processes and to decrease societal vulnerabilities, few efforts have been made to measure the impact of IIOs or to assess the efficacy of the countermeasures currently in place—the response capability—to mitigate those consequences.

When facing a potential threat, we don't want to just sit and wait for something bad to happen, experience the impact, and only then consider how best to respond.

It is much better to be proactive and seek to develop a response capability that can prevent losses or effectively mitigate the negative impact of an adverse event when it occurs.

To assess whether our response capability is sufficient we must be able to:

1) clearly identify the critical assets we wish to protect, and

2) accurately describe the response we have in place for when those assets are threatened.

Traditionally, 'risk' has been defined as 'a measure of the probability and severity of adverse effects', but recent advancements in risk research have prompted a shift in thinking.

The new perspective on risk management takes into account 'the effect of uncertainty on objectives'.

While these two orientations are largely compatible, incorporating what we know about uncertainties into estimates of response effectiveness rather than relying on probability calculations results in more robust and flexible capability assessments.

Capability assessments have been a key activity within crisis and emergency management in the last decades.

The purpose of these assessments is to support proactive decision-making concerning resource allocation for response preparedness.

Traditional assessment models—the so-called indicator and index models — equate resources with capability; such assessments provide decision – makers with either a checklist of resources or a numerical representation that evaluates the resources available for a crisis response within a target range for acceptability.

While such models have proven utility in the business world, where production can be (more or less) planned, they are not well suited to crisis and emergency management where uncertainty plays a much larger role.

The new risk perspective addresses this dilemma, suggesting a way forward for an assessment model that takes uncertainties into account, identifies the most effective response tasks and, in the absence of actual feedback and the wisdom of hindsight, provides the best possible information for making decisions regarding investments in capability.

The first part of this report describes response capability assessment—what it is for, what goes into preparing one, and why incorporating the new risk perspective leads to more useful information.

The theoretical explanation will be illustrated with typical examples from the field of risk management concerning residential fires and the response capability of a local fire service.

The second part of the report offers suggestions on how these concepts and ideas might be adapted for responding to IIOs.

The report ends with concluding remarks and a glossary of terms.

To read more:
https://stratcomcoe.org/publications/capability-assessment-for-stratcom-using-the-new-risk-perspective-to-inform-the-development-of-effective-response-capability-assessments-for-countering-information-influence-operations/240

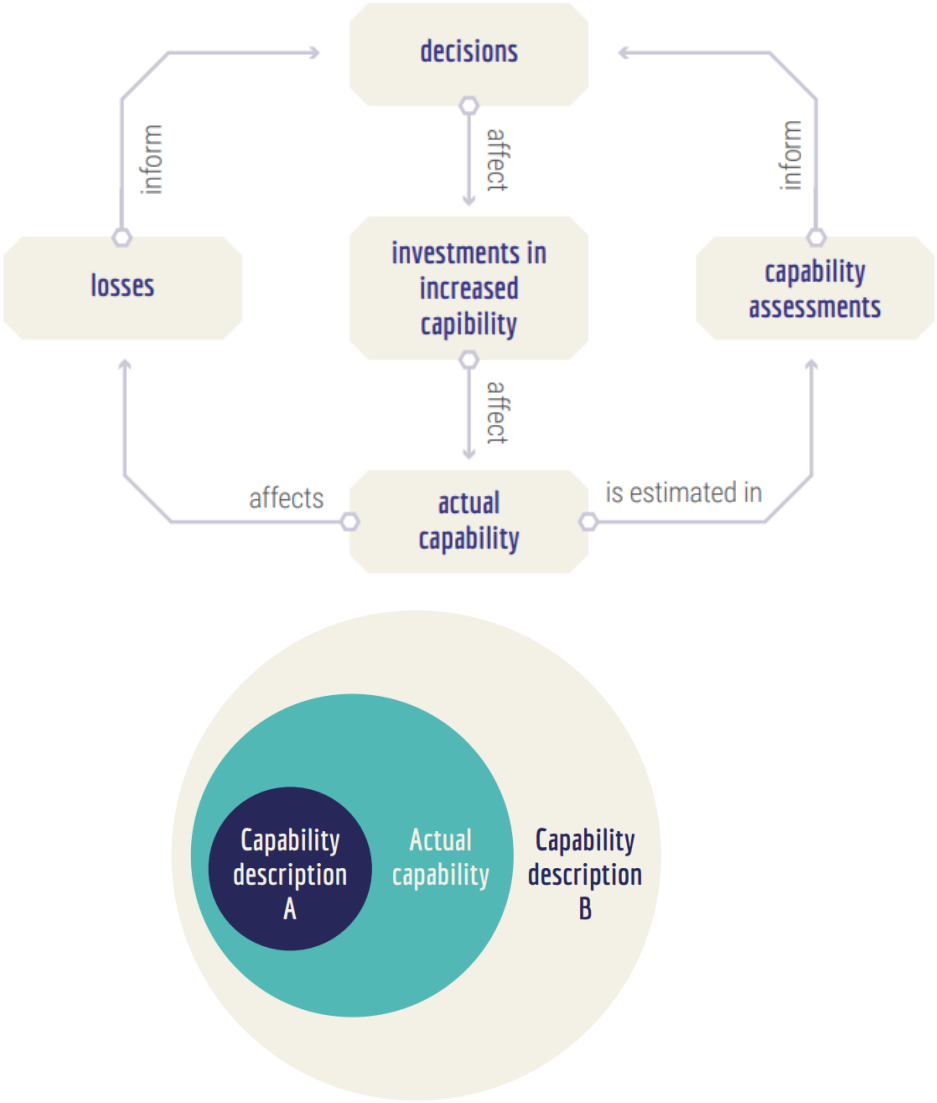


Figure 4. The difference between actual capability and possible descriptions of that capability

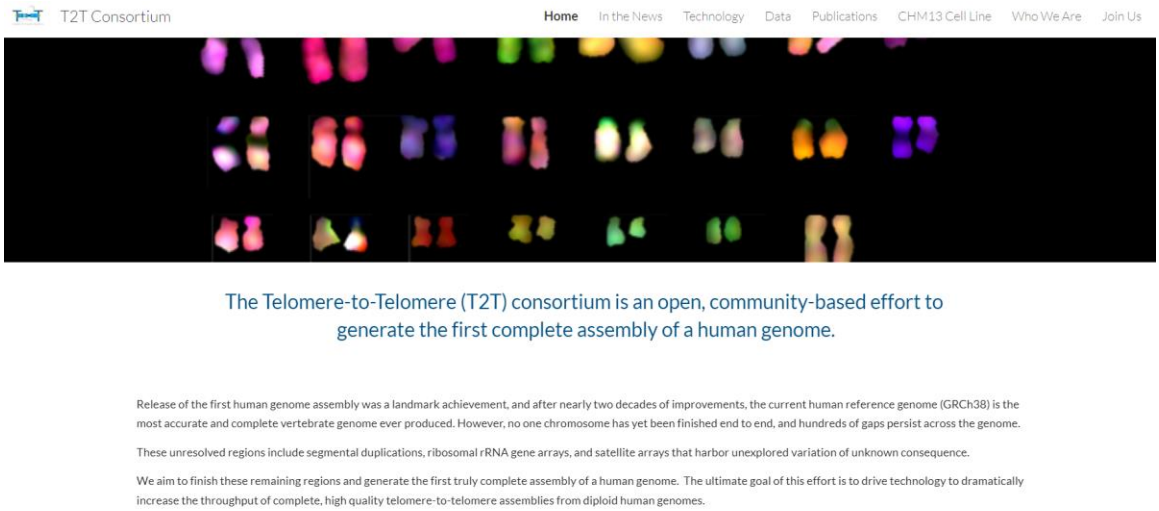
Number 10

First Complete Human Genome Poised to Strengthen Genetic Analysis, NIST Study Shows

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

Alongside the newly updated human genome, which fills in long-standing gaps to fully spell out the more than 3 billion letters that compose our genetic code, a separate companion study has shown it can serve as an accurate template that improves our DNA sequencing capabilities by leaps and bounds.

A group within the Telomere-to-Telomere (T2T) consortium — the initiative that completed the genome — led by the National Institute of Standards and Technology (NIST), Johns Hopkins University and the University of California, Davis, tested the full genome's ability to support the sequencing of DNA from thousands of people.



In a new paper published in the journal Science, the researchers found that it corrected tens of thousands of errors produced by the previous rendition of the genome and was better for the analysis of more than 200 genes of medical relevance.

The findings suggest that the T2T's genome could greatly propel research into genetic disorders, and that further in the future, patients might reap the benefits of more reliable diagnoses.

When clinicians and researchers sequence DNA to study or diagnose a genetic disorder, they use machines that produce strings of DNA, each

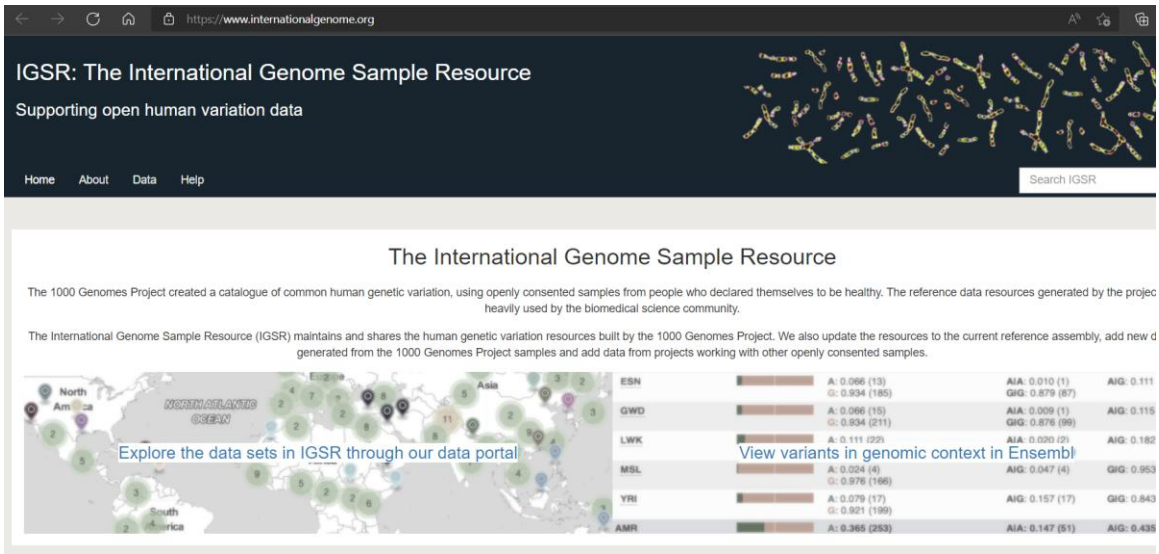
mirroring a section of a patient's or research subject's genome. Then they compare those strings to a template, called a reference genome, to get an idea of what order to place them in.

"If sequencing DNA is like putting together a puzzle, then the reference genome is like the picture of the finished puzzle on the box. It helps guide you in putting together the pieces," said NIST biomedical engineer Justin Zook, a co-author of the study.

The most advanced reference genome prior to the T2T version lacks 8% of the genome, and certain sections, which have proved difficult for sequencing technologies to decode in the past, are riddled with errors.

These imperfections made the reference akin to a puzzle box picture having blanks and showing pieces in the wrong place. But thanks to technological and scientific advances made in genomics over the past two decades, the T2T consortium was able to fill in and clean up the human reference genome.

Zook and the other study authors aimed to show just how much of a difference the finished reference would make in DNA sequencing.



The team found a proving ground for the reference in the 1000 Genomes Project (1KGP), an international effort that has amassed genetically diverse genome sequences from thousands of people from four different continents.

Rather than starting from scratch and obtaining DNA from new subjects, the researchers were able to piece together the DNA segments already laid out by 1KGP.

The authors used computer programs to analyze 3,202 genomes with the T2T reference and compared the results to published work on these genomes that was performed with the previous reference. It became clear that genomes stitched together using one of the two references differed greatly in important regions.

The T2T reference genome brought millions of genetic variations — stretches of DNA that differ from person to person — to light that the other reference did not. And it also washed away tens of thousands of blemishes in sequences, such as incorrectly located variations. In other words, the new variations filled in the blanks on the puzzle box picture and the corrections showed the right puzzle pieces where thousands were out of place before.

"What we found is that this new reference improved accuracy across the board. So, regardless of what the ancestry of the individual was, whether they were African, Caucasian or Asian, the new reference improved results for them," Zook said.

To understand the new reference's capabilities more thoroughly, the researchers attempted to use it to identify variation in 269 genes with either known or suspected connections to disease. These genes are tucked away in the regions of the genome that were previously challenging to decipher accurately.

The authors narrowed their focus to just one person characterized extensively by the NIST-led Genome in a Bottle Consortium, rather than thousands, to conduct this test. They performed a rigorous analysis of the genome of this individual, who had consented to publicizing their genetic code, using an array of powerful sequencing technologies backed by the new reference, Zook said.

For their efforts, they obtained a genomic benchmark — a highly accurate digital readout of the DNA in genes of interest — that can act as an answer key when evaluating sequencing methods.

The team paired the references with three different sequencing technologies each. But no matter the approach, T2T's genome always outperformed its predecessor, even decreasing error by as much as 12 times with one technology.

The T2T reference genome rounds out the mapping of our genetic blueprint, marking a pivotal milestone in the field of genomics. Researchers across the field will now be able to explore areas in the genome that were off limits in the past and begin to understand how scores of genes relate to

different diseases. But according to Zook, there is still more work to do before clinics put it into practice.

By all indications thus far, the T2T reference is more accurate than the current reference. However, researchers have used the current reference to analyze millions of genomes, gaining a deep well of knowledge that is essential for properly interpreting results when using it. Experts will need to grasp the ins and outs of the new reference in the same way to move forward.

“I think there'll definitely be a lot more work to understand the accuracy of DNA sequences of many individuals in regions of the genome that this reference now makes accessible,” Zook said.

To read more:
https://www.nist.gov/news-events/news/2022/03/first-complete-human-genome-poised-strengthen-genetic-analysis-nist-study

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...

www.simplyhired.com/search?q=crcmp&job=BY_s7GxAbt4KwSJ_aJA_4KaruYRQSQ

SimplyHired

crcmp

City, Stat

Crcmp jobs

Sort by | Date Added | More Filters

Relevance | Anytime | None Selected

Risk Science Business Process Lead, Senior Associate

Capital One - McLean, VA
Est. $110,000 - $150,000 a year
Lean, Six Sigma, BPM, PMP, PRM, or CRCMP. McLean 1 (19050), United States of America, McLean, Virginia....

Application Security Advisor-Penetration Tester

USAA - San Antonio, TX
Est. $100,000 - $140,000 a year
Professional designation in CISSP, CISA, CRISC, CISM, CEH, GWAPT, GWEB, or CRCMP. Purpose of Job IMPORTANT:....

Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews - New Brunswick, NJ

Apply On Company Site

- Stay abreast of regulatory environment regarding VRM.

Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

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.