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, July 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,

We need more cybersecurity experts with background in biology and life sciences. No, it is not a joke.

According to Randall Murch, *cyberbiosecurity* involves the understanding, protection, mitigation, investigation, and attribution of unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life and medical sciences, that affect security, competitiveness, and resilience.

Areas of concern include the privacy of patient data, the security of public health databases, the integrity of diagnostic test data, the integrity of public biological databases, the security implications of automated laboratory systems, disease surveillance and outbreak management data, and the security of proprietary *biological engineering* advances.

Biological information is measured, monitored, altered, and converted to digital information. Digital information can be used to manipulate biological systems.

Cybersecurity is always important when digital information is propagated and stored through networks of connected electronic devices.

Biosecurity refers to the threat to humans, living organisms and the environment, as the result of the exposures to biological agents, such as pathogens, that occur naturally or intentionally.

Securing the information flow in systems, and providing cyberbiosecurity training to persons having authorized access, is critical for public health, economic security, and national security for every country.

Pathogen detection, identification, and tracking is shifting to methods relying on whole genomes. We increasingly rely on genome databases, and these databases are increasingly becoming the targets for cyberattacks from state sponsored but independent groups and the organized crime.

The protection of the privacy of individuals, growers, and retailers is another major cyberbiosecurity challenge, as we need to collect pathogen genomic data from infected individuals or agricultural and food products during disease outbreaks to improve disease modeling and forecast.

The fact that genome databases are most utilized by the research community increases the risks, as the research community is not always following cybersecurity standards and best practices. The culture of trust and the willingness to share without considering information security rules is becoming a major vulnerability.

The access to pathogen sequences will lead to malicious use. Many genomes of animal and plant pathogens are accessible to all users of pathogen genome databases. We even had recommendations that open access to pathogen genomes should be promoted (Committee on Genomics Databases for Bioterrorism Threat Agents, 2004). The reduced cost of synthetic DNA technology and the advancement in synthetic biology reversed this approach, but many databases are still not properly secured.

Most security measures are designed to protect from external attacks. Insiders pose substantial threats, as they already have authorized access to critical systems. Insiders include employees of the organization, employees of trusted business partners, suppliers and service providers.

The threats posed by insiders can be unintentional or intentional, both of which should be accounted for in cyberbiosecurity assessments and training programs. Unintentional incidents include phishing or social engineering attacks from outside parties. They can be the results of negligence or misjudgement, and cyberbiosecurity training can dramatically reduce them.

Intentional incidents include insiders that commit fraud for financial gain, or seek to sabotage the organization. It can be the result of bribery or blackmail from foreign governments, competing organizations, or the organized crime. Employees must be trained to recognize the *modus operandi* of such persons.

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 7 (Page 26)

Solvency II - striking the balance

Sam Woods, Deputy Governor for Prudential Regulation of the Bank of England and Chief Executive of the Prudential Regulation Authority (PRA).

Number 8 (Page 31)

FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts

Number 9 (Page 33)

NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

Federal agency reveals the first group of winners from its six-year competition.

Number 10 (Page 37)

AI Improves Robotic Performance in DARPA's Machine Common Sense Program

New algorithms, simulated training prepare robots for real-world scenarios

Number 1

European Union Agency for Cybersecurity (ENISA)

ENISA Cybersecurity Threat Landscape Methodology

Policy makers, risk managers and information security practitioners need up to date and accurate information on the current threat landscape, supported by threat intelligence. The EU Agency for Cybersecurity (ENISA) Threat Landscape report has been published on an annual basis since 2013.

The report uses publicly available data and provides an independent view on observed threats agents, trends and attack vectors.

ENISA aims at building on its expertise and enhancing this activity so that its stakeholders receive relevant and timely information for policy-creation, decision-making and applying security measures, as well as in increasing knowledge and information for specialised cybersecurity communities or for establishing a solid understanding of the cybersecurity challenges related to new technologies.

The added value of ENISA cyberthreat intelligence efforts lies in offering updated information on the dynamically changing cyberthreat landscape. These efforts support risk mitigation, promote situational awareness and proactively respond to future challenges.

Following the revised form of the ENISA Threat Landscape Report 2021, ENISA continues to further improve this flagship initiative.

ENISA seeks to provide targeted as well as general reports, recommendations, analyses and other actions on future cybersecurity scenarios and threat landscapes, supported through a clear and publicly available methodology.

By establishing the ENISA Cybersecurity Threat Landscape (CTL) methodology, the Agency aims to set a baseline for the transparent and systematic delivery of horizontal, thematic, and sectorial cybersecurity threat landscapes. The following threat landscapes could be considered as examples.

- Horizontal threat landscapes, such as the overarching ENISA Threat Landscape (ETL), a product which aims to cover holistically a wide-range of sectors and industries.

- Thematic threat landscapes, such as the ENISA Supply Chain Threat Landscape, a product which focuses on a specific theme, but covers many sectors.

- Sectorial threat landscape, such as the ENISA 5G Threat Landscape, focuses on a specific sector. A sectorial threat landscape provides more focused information for a particular constituent or target group.

Recognising the significance of systematically and methodologically reporting on the threat landscape, ENISA has set up an ad hoc Working Group on Cybersecurity Threat Landscapes2 (CTL WG) consisting of experts from European and international public and private sector entities.

The scope of the CTL WG is to advise ENISA in designing, updating and reviewing the methodology for creating threat landscapes, including the annual ENISA Threat Landscape (ETL) Report.

The WG enables ENISA to interact with a broad range of stakeholders for the purpose of collecting input on a number of relevant aspects.

The overall focus of the methodological framework involves the identification and definition of the process, methods, stakeholders and tools as well as the various elements that, content-wise, constitute the cyberthreat Landscape (CTL).

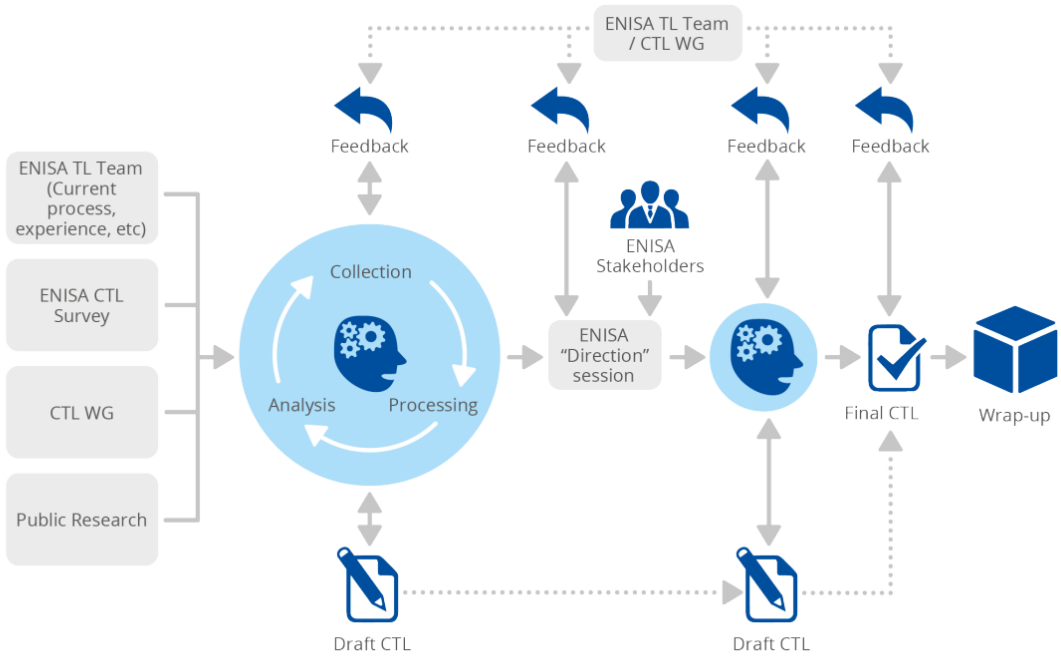


Figure 1: High level overview of ENISA CTL methodology

ETL Intelligence collection requirements:

- Vendor Cyberthreat Intelligence (CTI)
- Member States shared CTI
- Open-source intelligence (OSINT)
- Internal monitoring systems and tools (e.g. Open Cyber Situational Awareness Machine (CSAM))

To read more:
https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

Number 2

Financial Stability Institute (FSI), Insights on policy implementation No 44

Big tech interdependencies – a key policy blind spot

Juan Carlos Crisanto, Johannes Ehrentraud, Marcos Fabian, Amélie Monteil

BANK FOR INTERNATIONAL SETTLEMENTS

Executive summary

The increasingly prominent role of large technology firms (big techs) in the financial sector has raised questions about their inner workings and regulation.

Big techs have already gained a substantial footprint in parts of financial services; and the trend towards more digitalisation, which the Covid-19 pandemic has accelerated, has allowed them to fortify their market positions even further.

While big tech business models vary across markets and jurisdictions, they also share characteristics that could represent a major source of disruption to the financial system and give rise to a range of policy concerns.

One attribute of big techs' business model that has so far received less attention, and is therefore less well understood, are the implications of their internal and external interdependencies on the financial system.

Big tech activities underpin closely connected digital platform ecosystems.

Such an ecosystem, which has a digital platform at its centre, is run by financial and non-financial entities that form part of a big tech group.

Other participants in the ecosystem are third-party entities that offer products and services on the platform as well as individuals and businesses that use them.

By using cutting-edge technology, big tech entities take advantage of users' personal data as an input to create further user activity and generate more data.

This ability to enable active interaction among different participants in their ecosystem is a key element underpinning the business models of big techs. It may not be surprising therefore that significant intragroup dependencies and external interconnections are integral parts of the big tech business model.

The objective of this paper is to explore the interdependencies inherent in big tech's business models.

This assessment is based on the business models of six big techs around the world (Alibaba, Amazon, Grab, Jumia, Mercado Libre and Rakuten).

Due to the lack of a comprehensive source of information on their organisational structure, activities and the risks involved, this paper has pieced together a view of their business models using a variety of publicly available information such as securities prospectuses, annual reports, expert press reports and other investor resources.

The analysis of individual big tech business models points to several common features.

Their core activity is usually complemented by a wide array of services, particularly financial and technology ones. Another common feature relates to the integration of different big tech activities into the same platform using "ecosystem binders".

These are applications and tools that facilitate and promote the use of the entire ecosystem such as super apps and loyalty schemes. Big techs also commonly show a drive to grow and expand to new markets.

Finally, big tech business models rely on a strongly connected digital platform ecosystem that generates strong intragroup and external interdependencies.

Big techs' drive to grow is reflected in different stages of their development, generating both regional and global big techs.

The more services a big tech platform offers, the more attractive it could be for its users. The continuous expansion of big techs into new markets can be observed through various indicators related to their operations such as number of jurisdictions and clients, level of revenues and business areas.

These indicators show that Alibaba and Amazon operate globally in a wide number of business areas and have a large customer base. Other big techs such as Grab, Jumia, Mercado Libre and Rakuten have a regional focus, serve a relatively smaller customer base and operate in a limited number of business segments. They are, however, expanding towards new markets.

Intragroup dependencies help big techs achieve economies of scale but raise risks.

Financial and non-financial entities that form part of the big tech group use common payment systems to facilitate transactions across the entire ecosystem. In addition, they use the same technological infrastructures, computer applications and analytical tools to process information relevant for the group.

They also rely on a common credit scoring system to evaluate clients and share their data to make the ecosystem work.

These intragroup dependencies raise the potential for difficulties regarding one or more parts of big tech activities to spill over across the entire group, which may have a negative impact on their provision of regulated financial services.

The activities of big techs and financial institutions are increasingly intertwined and have the potential to give rise to meaningful external interdependencies.

Both offer financial products and services through a variety of partnerships, including:

(i) strategic alliances to facilitate payments in the big tech ecosystem;

(ii) white labelling arrangements through which big techs perform customer interface functions;

(iii) banking-as-a-service partnerships that allow big techs to integrate financial products from different providers into their platform;

(iv) pre-screening services by big techs to identify whether customers are eligible for certain financial products; and

(v) arrangements to originate and/or distribute lending and insurance products. The lack of transparency around these arrangements makes it complex to assess the type and level of risks to which financial institutions are exposed.

To read more: https://www.bis.org/fsi/publ/insights44.pdf

Number 3

EBA updates the list of Other Systemically Important Institutions

The European Banking Authority (EBA) updated today the list of Other Systemically Important Institutions (O-SIIs) in the EU, which, together with Global Systemically Important Institutions (G-SIIs), are identified as systemically important by the relevant authorities according to harmonised criteria laid down in the EBA Guidelines. This list is based on end-2020 data and also reflects the O-SII score and the capital buffers that the relevant authorities have set for the identified O-SIIs. The list is available also in a user-friendly visualisation tool.

A	B	C	D	E	F
Country	LEI	Name of institution identified as O-SII (at country's highest consolidation level)	Final O-SII buffer [1]	Identified through supervisory judgement	O-SII score
AT	529900ICA8XQYGIKR372	BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft	0.50%		564
AT	PQOH26KWDF7CG10L6792	Erste Group Bank AG	1.00%		2512
AT	9ZHRYM6F437SQJ6OUG95	Raiffeisen Bank International AG	1.00%		1835
AT	529900SXEWPJ1MRRX537	RAIFFEISEN-HOLDING NIEDERÖSTERREICH-WIEN registrierte Genossenschaft mit beschränkter Haftung	0.50%		293
AT	I6S527Q1Q3385V753S50	Raiffeisenlandesbank Oberösterreich Aktiengesellschaft	0.50%		522
AT	D1HEB8VEU6D9M8ZUXG17	UniCredit Bank Austria AG	1.00%		1172
AT	529900D4CD6DIB3CI904	Volksbank Wien AG (on consolidated basis of Volksbanken Verbund pursuant to Article 30a Austrian Banking Act)	0.50%	Y	199
BE	LSGM84136ACA92XCN876	Axa Bank Belgium	0.75%	Y	220
BE	A5GWLFH3KM7YV2SFQL8	Belfius Banque SA/NV	1.50%		1361
BE	KGCEPHLVVKVRZYO1T647	BNP Paribas Fortis SA/NV	1.50%		2671
BE	549300CBNW05DILT6870	Euroclear SA/NV	0.75%		789
BE	JLS56RAMYQZECFUF2G44	ING België NV	1.50%		1410
BE	5493008QOCP58OLEN998	Investeringsmaatschappij Argenta	0.75%	Y	330
BE	213800X3Q9LSAKRUWY91	KBC Groep	1.50%		2414
BE	MMYX0N4ZEZ13Z4XCG897	The Bank of New York Mellon SA/NV	0.75%		464
BG	549300615CPXQO52J309	Bulgarian Development Bank EAD	0.50%		426
BG	5299002142DS5ONT5540	Central Cooperative Bank AD	0.50%		392
BG	529900GEH0DAUTAXUA94	DSK Bank AD	1.00%		1661
BG	549300IRGNL8Q3O8Y413	Eurobank Bulgaria AD	0.75%		831
BG	549300UY81ESCZJ0GR95	First Investment Bank AD	1.00%		1168
BG	5299009KAL4KO7584196	Raiffeisenbank (Bulgaria) EAD [2]	0.75%		722
BG	549300Z7V2WOFIMUEK50	UniCredit Bulbank AD	1.00%		1991
BG	5299000PCY1EP8QJFV48	United Bulgarian Bank AD	0.75%		872
CY	549300VB6UM9TUOCYW67	Astrobank Ltd	0.25%		508
CY	PQ0RAP85KK9Z75ONZW93	Bank of Cyprus Public Company Ltd	1.50%		3197
CY	5493004KSNEM4U7L8714	Eurobank Cyprus Ltd	0.75%		1473
CY	CXUHEGU3MADZ2CEV7C11	Hellenic Bank Public Company Ltd	1.00%		2552
CY	253400EBCBBVB9TUHN50	RCB Bank Ltd	0.50%		1029
CY	529900VS0F7BA91P4I60	Alpha Bank Cyprus Ltd	0.25%	Y	342
CZ	9KOGW2C2FCIOIQ7FF485	Česká spořitelna, a.s.	2.00%		1564
CZ	Q5BP2UEQ48R75BOTCB92	Československá obchodní banka, a.s.	2.50%		2250

The EBA Guidelines define the size, importance, complexity and interconnectedness as the criteria to identify O-SIIs.

They also provide flexibility to relevant authorities to apply their supervisory judgment when deciding to include other institutions, which might have not been automatically identified as O-SIIs.

This approach ensures a comparable assessment of all financial institutions across the EU, whilst still not excluding those firms that may be deemed systemically important for one jurisdiction on the basis of certain specificities.

The EBA acts as the single point of disclosure for the list of O-SIIs across the EU, while each relevant authority discloses information for its respective jurisdiction, along with further details on the underlying rationale and identification process.

This additional information is relevant to understanding the specific features of each O-SII and get some insight in terms of supervisory judgment, optional indicators used, buffer decisions and phase-in implementation dates.

The list of O-SIIs is disclosed on an annual basis, along with any Common Equity Tier 1 (CET1) capital buffer requirements. Higher capital requirements will become applicable once relevant authorities decide to set institution-specific buffer requirements following the O-SII identification.

For each O-SII, the list includes the overall score in terms of basis points resulting from the EBA scoring methodology.

You may visit:
https://www.eba.europa.eu/eba-updates-list-other-systemically-important-institutions-0

https://www.eba.europa.eu/risk-analysis-and-data/global-systemically-important-institutions

Number 4

FSB proposes key performance indicators for measuring progress toward the G20 cross-border payments targets

The Financial Stability Board (FSB) published for public feedback an interim report on the approach for monitoring progress toward meeting the targets for the G20 Roadmap for Enhancing Cross-border Payments.

The report provides preliminary recommendations about key performance indicators (KPIs) that could be used to monitor progress over time and identifies existing and potential sources of data for calculating those KPIs.

In October 2021, the FSB set quantitative global targets for addressing the four challenges faced by cross-border payments (cost, speed, access, transparency) as a key foundational step in the G20 Roadmap.

These targets were set for each of the three main segments of the market (wholesale, retail and remittances). The targets define the Roadmap's ambition and create accountability. However, measuring progress toward these targets will not be straightforward because no comprehensive data sources currently exist.

For the wholesale segment, the FSB views private-sector network providers as the most promising data sources for monitoring speed and access, while the use of surveys and proxies are being evaluated for monitoring progress towards meeting the transparency target.

The retail payments segment is highly varied in terms of end-users, service providers, and payment mechanisms. The FSB proposes differentiated KPIs for the various use-cases, which would allow a better understanding of how progress toward meeting the targets differs among those use-cases.

The enormous variety of end-users and payment service providers in this segment make collecting comprehensive data infeasible. The FSB is, therefore, evaluating the feasibility of collecting representative samples, for instance from private-sector data aggregators.

For the remittances segment, the public sector's long-standing goal of improving conditions in this segment has led to the establishment of multiple high-quality databases, most notably the World Bank's Remittance Prices Worldwide database and Global Findex database. The FSB is proposing to leverage these, and similar, public-sector databases to calculate KPIs.

The FSB invites feedback from the public on the preliminary proposals in this report. In particular, feedback is appreciated on the following questions:

Has the FSB identified appropriate potential sources of data for efficiently monitoring progress toward the Roadmap's targets? What, if any, additional or alternative public or private data sources should the FSB also consider and for what KPIs?

Has the FSB defined the KPIs appropriately, such that they are closely and meaningfully tied to the relevant target? What, if any, additional considerations should inform the calculation of the KPIs so that they provide sufficiently representative measurements of progress toward the targets without being overly burdensome?

The FSB is evaluating the use of proxies for monitoring progress toward some of the targets. Are the proxies proposed appropriate? What, if any, additional or alternative proxies should the FSB consider that are sufficiently representative and simplify monitoring?

The responses will help to inform the FSB's report in October 2022 to the G20 setting out further details of the implementation approach and the KPIs. Feedback should be sent to fsb@fsb.org by 31 July 2022 with the title "Monitoring progress toward cross-border payments targets".

To read more:
https://www.fsb.org/2022/07/fsb-proposes-key-performance-indicators-for-measuring-progress-toward-the-g20-cross-border-payments-targets/

Number 5

Crypto-Assets and Decentralized Finance through a Financial Stability Lens

Vice Chair Lael Brainard, At Bank of England Conference, London, UK

Recent volatility has exposed serious vulnerabilities in the crypto financial system. While touted as a fundamental break from traditional finance, the crypto financial system turns out to be susceptible to the same risks that are all too familiar from traditional finance, such as leverage, settlement, opacity, and maturity and liquidity transformation. As we work to future-proof our financial stability agenda, it is important to ensure the regulatory perimeter encompasses crypto finance.

Distinguishing Responsible Innovation from Regulatory Evasion

New technology often holds the promise of increasing competition in the financial system, reducing transaction costs and settlement times, and channeling investment to productive new uses.

But early on, new products and platforms are often fraught with risks, including fraud and manipulation, and it is important and sometimes difficult to distinguish between hype and value.

If past innovation cycles are any guide, in order for distributed ledgers, smart contracts, programmability, and digital assets to fulfill their potential to bring competition, efficiency, and speed, it will be essential to address the basic risks that beset all forms of finance.

These risks include runs, fire sales, deleveraging, interconnectedness, and contagion, along with fraud, manipulation, and evasion. In addition, it is important to be on the lookout for the possibility of new forms of risks, since many of the technological innovations underpinning the crypto ecosystem are relatively novel.

Far from stifling innovation, strong regulatory guardrails will help enable investors and developers to build a resilient digital native financial infrastructure.

Strong regulatory guardrails will help banks, payments providers, and financial technology companies (FinTechs) improve the customer experience, make settlement faster, reduce costs, and allow for rapid product improvement and customization.

We are closely monitoring recent events where risks in the system have crystallized and many crypto investors have suffered losses.

Despite significant investor losses, the crypto financial system does not yet appear to be so large or so interconnected with the traditional financial system as to pose a systemic risk.

So this is the right time to ensure that like risks are subject to like regulatory outcomes and like disclosure so as to help investors distinguish between genuine, responsible innovation and the false allure of seemingly easy returns that obscures significant risk.

This is the right time to establish which crypto activities are permissible for regulated entities and under what constraints so that spillovers to the core financial system remain well contained.

Insights from Recent Turbulence

Several important insights have emerged from the recent turbulence in the crypto-finance ecosystem.

First, volatility in financial markets has provided important information about crypto's performance as an asset class. It was already clear that crypto-assets are volatile, and we continue to see wild swings in crypto-asset values.

The price of Bitcoin has dropped by as much as 75 percent from its all-time high over the past seven months, and it has declined almost 60 percent in the three months from April through June. Most other prominent crypto-assets have experienced even steeper declines over the same period.

Contrary to claims that crypto-assets are a hedge to inflation or an uncorrelated asset class, crypto-assets have plummeted in value and have proven to be highly correlated with riskier equities and with risk appetite more generally.

Second, the Terra crash reminds us how quickly an asset that purports to maintain a stable value relative to fiat currency can become subject to a run.

The collapse of Terra and the previous failures of several other unbacked algorithmic stablecoins are reminiscent of classic runs throughout history. New technology and financial engineering cannot by themselves convert risky assets into safe ones.

Third, crypto platforms are highly vulnerable to deleveraging, fire sales, and contagion—risks that are well known from traditional finance—as illustrated by the freeze on withdrawals at some crypto lending platforms and exchanges and the bankruptcy of a prominent crypto hedge fund. Some retail investors have found their accounts frozen and suffered large losses.

Large crypto players that used leverage to boost returns are scrambling to monetize their holdings, missing margin calls, and facing possible insolvency.

As their distress intensifies, it has become clear that the crypto ecosystem is tightly interconnected, as many smaller traders, lenders, and DeFi (decentralized finance) protocols have concentrated exposures to these big players.

Finally, we have seen how decentralized lending, which relies on overcollateralization to substitute for intermediation, can serve as a stress amplifier by creating waves of liquidations as prices fall.

Same Risk, Same Regulatory Outcome

The recent turbulence and losses among retail investors in crypto highlight the urgent need to ensure compliance with existing regulations and to fill any gaps where regulations or enforcement may need to be tailored—for instance, for decentralized protocols and platforms.

As we consider how to address the potential future financial stability risks of the evolving crypto financial system, it is important to start with strong basic regulatory foundations.

A good macroprudential framework builds on a solid foundation of microprudential regulation.

Future financial resilience will be greatly enhanced if we ensure the regulatory perimeter encompasses the crypto financial system and reflects the principle of same risk, same disclosure, same regulatory outcome.

By extending the perimeter and applying like regulatory outcomes and like transparency to like risks, it will enable regulators to more effectively

address risks within crypto markets and potential risks posed by crypto markets to the broader financial system.

Strong guardrails for safety and soundness, market integrity, and investor and consumer protection will help ensure that new digital finance products, platforms, and activities are based on genuine economic value and not on regulatory evasion, which ultimately leaves investors more exposed than they may appreciate.

Due to the cross-sectoral and cross-border scope of crypto platforms, exchanges, and activities, it is important that regulators work together domestically and internationally to maintain a stable financial system and address regulatory evasion.

The same-risk-same-regulatory-outcome principle guides the Financial Stability Board's work on stablecoins, crypto-assets, and DeFi; the Basel consultation on the prudential treatment of crypto-assets; the work by the International Organization of Securities Commissions' FinTech network; the work by federal bank regulatory agencies on the appropriate treatment of crypto activities at U.S. banks; and a host of other international and domestic work.

In implementing a same-risk-same-regulatory-outcome principle, we should start by ensuring basic protections are in place for consumers and investors.

Retail users should be protected against exploitation, undisclosed conflicts of interest, and market manipulation—risks to which they are particularly vulnerable, according to a host of research. If investors lack these basic protections, these markets will be vulnerable to runs.

Second, since trading platforms play a critical role in crypto-asset markets, it is important to address noncompliance and any gaps that may exist.

We have seen crypto-trading platforms and crypto-lending firms not only engage in activities similar to those in traditional finance without comparable regulatory compliance, but also combine activities that are required to be separated in traditional financial markets.

For example, some platforms combine market infrastructure and client facilitation with risk-taking businesses like asset creation, proprietary trading, venture capital, and lending.

Third, all financial institutions, whether in traditional finance or crypto finance, must comply with the rules designed to combat money laundering and financing of terrorism and to support economic sanctions.

Platforms and exchanges should be designed in a manner that facilitates and supports compliance with these laws.

The permissionless exchange of assets and tools that obscure the source of funds not only facilitate evasion, but also increase the risk of theft, hacks, and ransom attacks.

These risks are particularly prominent in decentralized exchanges that are designed to avoid the use of intermediaries responsible for know-your-customer identification and that may require adaptations to ensure compliance at this most foundational layer.

Finally, it is important to address any regulatory gaps and to adapt existing approaches to novel technologies. While regulatory frameworks clearly apply to DeFi activities no less than to centralized crypto activities and traditional finance, DeFi protocols may present novel challenges that may require adapting existing approaches.

The peer-to-peer nature of these activities, their automated nature, the immutability of code once deployed to the blockchain, the exercise of governance functions through tokens in decentralized autonomous organizations, the absence of validated identities, and the dispersion or obfuscation of control may make it challenging to hold intermediaries accountable.

It is not yet clear that digital native approaches, such as building in automated incentives for undertaking governance responsibilities, are adequate alternatives.

Connections to the Core Financial Institutions

There are two specific areas that merit heightened attention because of heightened risks of spillovers to the core financial system: bank involvement in crypto activities and stablecoins.

To date, crypto has not become sufficiently interconnected with the core financial system to pose broad systemic risk. But it is likely regulators will continue to face calls for supervised banking institutions to play a role in these markets.

Bank regulators will need to weigh competing considerations in assessing bank involvement in crypto activities ranging from custody to issuance to customer facilitation.

Bank involvement provides an interface where regulators have strong sightlines and can help ensure strong protections. Similarly, regulators are drawn to approaches that effectively subject the crypto intermediaries that resemble complex bank organizations to bank-like regulation.

But bringing risks from crypto into the heart of the financial system without the appropriate guardrails could increase the potential for spillovers and has uncertain implications for the stability of the system.

It is important for banks to engage with beneficial innovation and upgrade capabilities in digital finance, but until there is a strong regulatory framework for crypto finance, bank involvement might further entrench a riskier and less compliant ecosystem.

Private Digital Currencies and Central Bank Digital Currencies

Stablecoins represent a second area with a heightened risk of spillovers. Currently, stablecoins are positioned as the digital native asset that bridges from the crypto financial system to fiat. This role is important because fiat currency is referenced as the unit of account for the crypto financial system.

Stablecoins are currently the settlement asset of choice on and across crypto platforms, often serving as collateral for lending and trading activity. As highlighted by large recent outflows from the largest stablecoin, stablecoins pegged to fiat currency are highly vulnerable to runs.

For these reasons, it is vital that stablecoins that purport to be redeemable at par in fiat currency on demand are subject to the types of prudential regulation that limit the risk of runs and payment system vulnerabilities that such private monies have exhibited historically.

Well-regulated stablecoins might bring additional competition to payments, but they introduce other risks. There is a risk of fragmentation of stablecoin networks into walled gardens.

Conversely, there is a risk that a single dominant stablecoin might emerge, given the winner-takes-all dynamics in such activities.
Indeed, the market is currently highly concentrated among three dominant stablecoins, and it risks becoming even more concentrated in the future.

The top three stablecoins account for almost 90 percent of transactions, and the top two of these account for 80 percent of market capitalization.

Given the foundational role of fiat currency, there may be an advantage for future financial stability to having a digital native form of safe central bank money—a central bank digital currency. A digital native form of safe central bank money could enhance stability by providing the neutral trusted settlement layer in the future crypto financial system.

A settlement layer with a digital native central bank money could, for instance, facilitate interoperability among well-regulated stablecoins designed for a variety of use cases and enable private-sector provision of decentralized, customized, and automated financial products.

This development would be a natural evolution of the complementarity between the public and private sectors in payments, ensuring strong public trust in the one-for-one redeemability of commercial bank money and stablecoins for safe central bank money.

Building in Risk Management and Compliance

Crypto and fintech have introduced competition and put the focus on how innovation can help increase inclusion and address other vexing problems in finance today.

Slow and costly payments particularly affect lower-income households with precarious cash flows who rely on remittances or miss bills waiting on paychecks. Many hard-working individuals cannot obtain credit to start businesses or to respond to an emergency.

But while innovation and competition can reduce costs in finance, some costs are necessary to keep the system safe.

Intermediaries earn revenues in exchange for safely providing important services. Someone must bear the costs of evaluating risk, maintaining resources to support those risks through good times and bad, complying with laws that prevent crime and terrorism, and serving less sophisticated customers fairly and without exploitation.

In the current crypto ecosystem, often no one is bearing these costs. So when a service appears cheaper or more efficient, it is important to understand whether this benefit is due to genuine innovation or regulatory noncompliance.

So as these activities evolve, it is worth considering whether there are new ways to achieve regulatory objectives in the context of new technology. Distributed ledgers, smart contracts, and digital identities may allow new forms of risk management that shift the distribution of costs.

Perhaps in a more decentralized financial system, new approaches can be designed to make protocol developers and transaction validators accountable for ensuring financial products are safe and compliant.

Conclusion

Innovation has the potential to make financial services faster, cheaper, and more inclusive and to do so in ways that are native to the digital ecosystem.

Enabling responsible innovation to flourish will require that the regulatory perimeter encompass the crypto financial system according to the principle of like risk, like regulatory outcome, and that novel risks associated with the new technologies be appropriately addressed.

It is important that the foundations for sound regulation of the crypto financial system be established now before the crypto ecosystem becomes so large or interconnected that it might pose risks to the stability of the broader financial system.

To read more:
https://www.federalreserve.gov/newsevents/speech/brainard20220708a.htm

Number 6

Staff paper, an overview of the proposal for an Insurance Recovery and Resolution Directive (IRRD)

The disorderly failure of an insurer or a group of insurers may pose risks to financial stability and to policyholders.

Insurance undertakings provide important services to other actors in the financial system, policyholders and companies. Studies document that the insurance sector contribution to overall systemic risk has been increasing.

Due to their interconnectedness, a failure of a large insurer or the simultaneous failure of several insurers, may have negative repercussions on other parts of the financial system.

Equally, it is key to ensure that at the moment of failure the insurer continues to function as good as is possible in order to prevent policyholder detriment e.g. by continuing to pay out claims and pensions.

A regular insolvency procedure might be cumbersome and unable to manage a failure of an insurer in an orderly fashion.

For example, the settlement of policyholders' claims could be considerably delayed possibly by several years, undermining the wider public's trust in the insurance sector as whole.

Therefore, an authority that is specialised in the insurance business, is familiar with the challenges of resolution, and is equipped with a set of specific tools, would be best placed to deal with situations of distress and default of insurers.

Finally, an important objective of a recovery and resolution regime is to prevent the use of public funds i.e. taxpayers' money.

The ultimate goal is therefore to prevent failure - and if this is not possible - facilitate an orderly market exit.

The proposal put forward by the European Commission (COM) in September 2021, which will be briefly explained in the following paragraphs, is very much welcomed by EIOPA. This goes, in particular, with regard to the focus on the preventive approach, the fact that it addresses all relevant building blocks of a recovery and resolution

framework, and the focus on cooperation and coordination among authorities.

Although there are several technical issues that could be subject to debate (e.g. on how the tools will work in practice), EIOPA is generally in agreement with the proposal, which is fully aligned with the international standards. From that point of view, EIOPA believes that the approach and the main elements should broadly remain as they are.

Resolution tools. One of the fundamental elements of the proposed Directive are the set of resolution powers it includes. It goes from the more traditional ones, like the run-off or the portfolio transfer (where there is a lot of experience by authorities), to others that are newer.

Bail-in	• Write-down of liabilities or conversion to shares – policyholders cannot receive shares
Solvent run-off	• Withdrawal of authorisation and run-off
Sale of all or part of the business	• To third party / parties
Bridge undertaking	• Public controlled entity where assets and liability are temporarily managed
Asset and liability separation	• Impaired or problem assets and/or liabilities can be transferred to a management vehicle
Additional national tools and powers	• If consistent with framework

To read more:
https://www.eiopa.europa.eu/document-library/other-documents/eiopa-staff-paper-proposal-insurance-recovery-and-resolution_en

Number 7

Solvency II - striking the balance

Sam Woods, Deputy Governor for Prudential Regulation of the Bank of England and Chief Executive of the Prudential Regulation Authority (PRA).

Introduction

The UK's post-Brexit review of insurance regulation is entering a critical phase, with important decisions shortly to come for us, government and Parliament.

With that in mind I thought it would be useful to highlight some of the key points from the Prudential Regulation Authority's (PRA's) perspective, while HM Treasury's current consultation on Solvency II is ongoing, with a particular focus on the main point of contention between us and parts of the industry.

My main message is this. Following Brexit we have a once-in-a-generation opportunity to reshape insurance regulation to work better for the UK.

We can do this while loosening parts of the regime which were over-calibrated by the EU and making it easier for insurers to invest in a wider range of assets, but we also need to strengthen it in one area in order to avoid risks to the millions of current and future pensioners who rely on insurers for their retirement income.

The combined effect of these changes should support the government's objectives for competitiveness, growth and investment in the economy.

Overview

Following our exit from the EU, we have been examining the main bit of prudential insurance regulation (Solvency II) to see how it can be tailored to work better for the UK, working with the Treasury.

The Treasury has set three objectives for the review, which we support: a competitive insurance sector, investment to support growth and policyholder protection.

While the details of the review can appear technical and abstract, the stakes are real. A stable insurance sector backstops the livelihoods of millions of policyholders, in particular current and future pensioners who rely on insurers for their retirement incomes.

The insurance sector is also a major part of the wider financial sector, and an important source of finance for the real economy including productive and green investment.

Brexit gives us an opportunity to rewrite the insurance regulations we inherited from the EU – and in doing so help drive further investment in the economy. But we need to be clear that this is not a free lunch.

If changes simply loosen regulations which were over-cooked by the EU, without tackling other areas where regulations are too weak, then we are putting policyholders at risk.

The interests of pensioners and other insurance policyholders can get lost in these debates, but Parliament has given the PRA a primary objective to protect policyholders, and it is a central part of our job to highlight risks and propose ways to deal with them.

While pursuing our primary objectives of safety and soundness and policyholder protection, we also have regard to a number of important considerations, including the competitiveness of the sector and the contribution it can make to long-term economic growth.

We are also mindful that as part of its review of the Future Regulatory Framework, the Government has proposed to give the PRA a new secondary objective to promote long-term economic growth and international competitiveness, alongside our existing secondary competition objective.

With all of those factors in mind, we think we can deal with the risks we are worried about while also supporting the government's wider objectives.

Specifically, some in the insurance industry have the impression that we are opposed to any release of capital requirements for insurers.

I want to be very clear that that is not the PRA's position – indeed, following a lot of work and examination of the evidence over the last year or so we think that a substantial capital release should be possible while continuing to protect policyholders adequately.

This could occur as part of a reform package comprising three main components:

- first, a large cut to the "Risk Margin", which is an extra liability that firms have to carry in order to make it more likely that another firm will agree to take on their insurance policies if the firm gets into trouble, to ensure policyholders are still protected in that scenario;

- second, a package of measures to remove unnecessary bureaucracy from the regime and enable insurers to invest in a wider set of assets; and

- third, measures to put one part of the regime (the "Matching Adjustment") onto a more sustainable footing.

While there are important issues to debate on the first two elements, it's on the third of these that there is the main current difference of view between the PRA and parts of the life insurance sector and I will focus mainly on that element in my remarks today.

What is the "Matching Adjustment" and why does it matter?

The main point of contention in the review is what, if anything, to change about the calibration of a part of the regime called the "Matching Adjustment" (or "MA" for short).

It's usually at this point in any speech about insurance regulation that most people switch off, but bear with me while I try to bring the issue to life.

First, what is this "MA" and what does it do? It allows insurance companies to recognise as capital up-front a part of the income they expect to earn on their assets in the future, but only as long as they can show that the cashflows they expect to receive from those assets closely match the payments they have undertaken to make to their insurance policyholders (hence "matching" adjustment).

This is therefore most relevant for the annuity business, where insurance companies promise to pay individuals' pensions far into the future.

You might ask why the regulator favours such an arrangement, which is not common in other bits of regulation, when perhaps it would be more prudent to make insurance companies wait until those returns (for instance, interest payments on corporate bonds) are actually paid to them before recognising them as capital which could be paid out to shareholders.

The reason is that we think it protects policyholders if insurance companies are incentivised to invest in assets which will produce cash at the right time, so that insurance companies are not scrabbling around for the right assets when they have to make payments to pensioners in the future.

However, you would be right to think that if we allow such an arrangement we must operate it with a very high degree of confidence that those future returns will in fact materialise – in other words that insurance companies do not recognise up-front returns which then later don't show up.

Second, why does the MA matter?

For me there are two reasons.

First, the nature of the business for which it is primarily used: pensions provided by insurance companies.

When an individual puts their life savings into an insurance company in return for a promise that the company will pay their pension right up until their death (potentially decades later), we need to be very confident that the company is going to be able to make good on that promise.

The same is true when companies of all sorts pass their pension liabilities over to an insurance company, which is happening in very high volumes – for those pensioners too we need take care that the foundations of that insurer are robust. We estimate that over 8 million policyholders are served by this sector.

And second, the MA is a vital part of those foundations simply because it is so large – on the most recent figures, the total assets in MA portfolios amount to around £380 billion, and the MA confers a capital benefit on insurers of around £80 billion – up from around £60 billion when the regime was introduced.

To put that £80 billion figure in context, the entire capital base of the life insurance industry is around £112 billion, and for a number of insurers the MA by itself makes up the bulk of their capital.

In short, millions of pensioners rely on their insurer for their livelihood, and in turn those insurers rely very heavily on the MA.

It is true that people who get their pension from an insurance company which fails should have some protection from a compensation scheme which spreads the cost of failures across the industry, but we should not underestimate the risks to them, the industry and the public purse of a

major failure – we need to be sure that the basis on which pension promises are made is solid.

To read more:
https://www.bankofengland.co.uk/speech/2022/july/sam-woods-speech-given-at-the-bank-of-england-solvency-ii-striking-the-balance

Number 8

FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts

The Financial Crimes Enforcement Network (FinCEN) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) are issuing a joint alert urging financial institutions to be vigilant against efforts by individuals or entities to evade BIS export controls implemented in connection with the Russian Federation's (Russia) further invasion of Ukraine.

This joint alert provides financial institutions with an overview of BIS's current export restrictions; a list of commodities of concern for possible export control evasion; and select transactional and behavioral red flags to assist financial institutions in identifying suspicious transactions relating to possible export control evasion.

This alert further reminds financial institutions of their Bank Secrecy Act (BSA) reporting obligations and details how suspected export control evasion activity may also be reported to BIS enforcement authorities.

Overview of Recent BIS Actions in Response to the Invasion of Ukraine

Since February 24, 2022, BIS has implemented a series of stringent export controls that restrict Russia's access to specific technologies and other items that it needs to sustain its military activity in Ukraine.

These controls primarily target Russia's defense, aerospace, and maritime sectors. They also include other targets such as Russia's energy production sector as well as luxury goods used by Russian elites.

These controls are aligned with export controls implemented by 37 U.S. allies and partners and represent the most comprehensive application of Commerce's export authorities targeting a single country.

The United States has also applied restrictions to Belarus in response to its substantial enabling of Russia's war effort.

These actions are part of a coordinated international endeavor to apply economic pressure on Russia and Belarus to degrade the military

capabilities that Russia uses to wage its war, and to restrict Russia's access to items that can support the country's defense industrial base and military and intelligence services.

They also increase the costs on Russian and Belarusian persons who support the government of Russia and its invasion of Ukraine.

These recent BIS actions also build on export restrictions that the United States previously established following Russia's occupation of Crimea in 2014, and in response to other malign Russian activities. Some of these prior restrictions remain in effect, while others have been expanded in scope through BIS's recent regulatory actions.

These actions have imposed controls on a range of items subject to the Export Administration Regulations (EAR) that had not previously required export licenses when destined for Russia or Belarus.

The new controls place significant restrictions on:

(i) U.S. exports, reexports, and in-country transfers to Russia, and

(ii) products destined for Russia and manufactured abroad with certain U.S. technology, software, or tooling. BIS imposed similar controls on items subject to the EAR and destined for Belarus, including broad in-country transfer controls.

With this joint alert, FinCEN is partnering with BIS to assist U.S. financial institutions in identifying customers and transactions that may pose elevated risks of attempted export control evasion.

To read more:
https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

Number 9

NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

Federal agency reveals the first group of winners from its six-year competition.

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

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has chosen the first group of encryption tools that are designed to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on every day — such as online banking and email software.

The four selected encryption algorithms will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years.

"Today's announcement is an important milestone in securing our sensitive data against the possibility of future cyberattacks from quantum computers," said Secretary of Commerce Gina M. Raimondo. "Thanks to NIST's expertise and commitment to cutting-edge technology, we are able to take the necessary steps to secure electronic information so U.S. businesses can continue innovating while maintaining the trust and confidence of their customers."

The announcement follows a six-year effort managed by NIST, which in 2016 called upon the world's cryptographers to devise and then vet encryption methods that could resist an attack from a future quantum computer that is more powerful than the comparatively limited machines available today. The selection constitutes the beginning of the finale of the agency's post-quantum cryptography standardization project.

"NIST constantly looks to the future to anticipate the needs of U.S. industry and society as a whole, and when they are built, quantum computers powerful enough to break present-day encryption will pose a serious threat to our information systems," said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. "Our post-quantum cryptography program has leveraged the top minds in cryptography — worldwide — to produce this first group of quantum-resistant algorithms that will lead to a standard and significantly increase the security of our digital information."

Four additional algorithms are under consideration for inclusion in the standard, and NIST plans to announce the finalists from that round at a future date. NIST is announcing its choices in two stages because of the need for a robust variety of defense tools.

As cryptographers have recognized from the beginning of NIST's effort, there are different systems and tasks that use encryption, and a useful standard would offer solutions designed for different situations, use varied approaches for encryption, and offer more than one algorithm for each use case in the event one proves vulnerable.

Encryption uses math to protect sensitive electronic information, including the secure websites we surf and the emails we send. Widely used public-key encryption systems, which rely on math problems that even the fastest conventional computers find intractable, ensure these websites and messages are inaccessible to unwelcome third parties.

However, a sufficiently capable quantum computer, which would be based on different technology than the conventional computers we have today, could solve these math problems quickly, defeating encryption systems. To counter this threat, the four quantum-resistant algorithms rely on math problems that both conventional and quantum computers should have difficulty solving, thereby defending privacy both now and down the road.

The algorithms are designed for two main tasks for which encryption is typically used: general encryption, used to protect information exchanged across a public network; and digital signatures, used for identity authentication. All four of the algorithms were created by experts collaborating from multiple countries and institutions.

For general encryption, used when we access secure websites, NIST has selected the CRYSTALS-Kyber algorithm. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation.

For digital signatures, often used when we need to verify identities during a digital transaction or to sign a document remotely, NIST has selected the three algorithms CRYSTALS-Dilithium, FALCON and SPHINCS+ (read as "Sphincs plus").

Reviewers noted the high efficiency of the first two, and NIST recommends CRYSTALS-Dilithium as the primary algorithm, with FALCON for applications that need smaller signatures than Dilithium can provide. The third, SPHINCS+, is somewhat larger and slower than the other two, but it

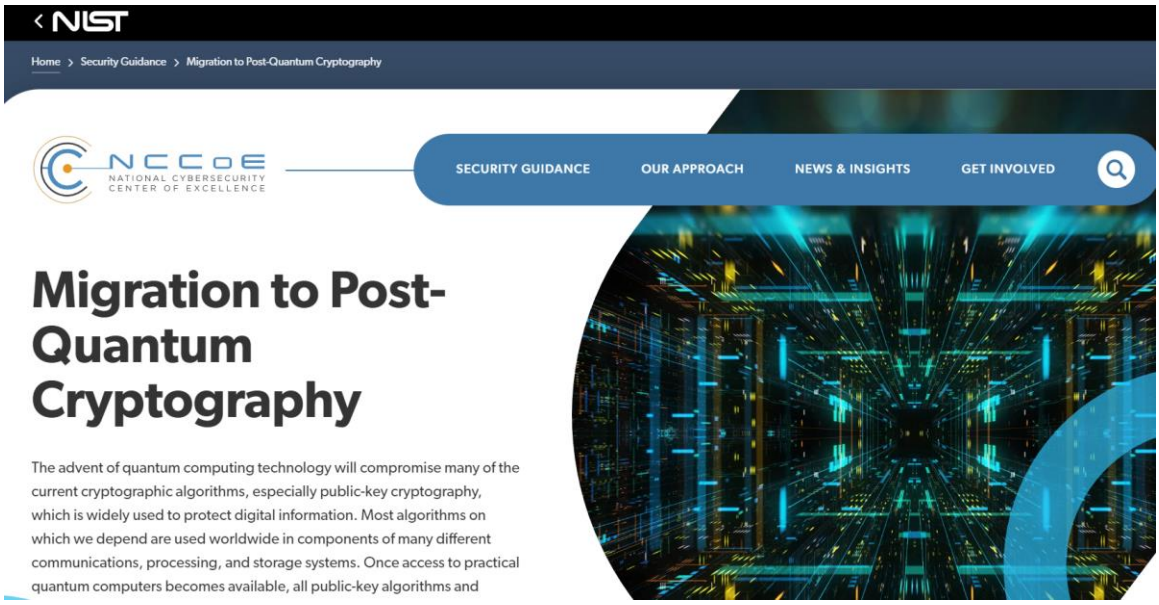
is valuable as a backup for one chief reason: It is based on a different math approach than all three of NIST's other selections.

Three of the selected algorithms are based on a family of math problems called structured lattices, while SPHINCS+ uses hash functions. The additional four algorithms still under consideration are designed for general encryption and do not use structured lattices or hash functions in their approaches.

While the standard is in development, NIST encourages security experts to explore the new algorithms and consider how their applications will use them, but not to bake them into their systems yet, as the algorithms could change slightly before the standard is finalized.

To prepare, users can inventory their systems for applications that use public-key cryptography, which will need to be replaced before cryptographically relevant quantum computers appear.

They can also alert their IT departments and vendors about the upcoming change. To get involved in developing guidance for migrating to post-quantum cryptography, see NIST's National Cybersecurity Center of Excellence project page at: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms



All of the algorithms are available on the NIST website at: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

PROJECTS | POST-QUANTUM CRYPTOGRAPHY | POST-QUANTUM CRYPTOGRAPHY STANDARDIZATION

Post-Quantum Cryptography PQC

Round 3 Submissions

Official comments on the Third Round Candidate Algorithms should be submitted using the "Submit Comment" link for the appropriate algorithm. Comments from the pqc-forum Google group subscribers will also be forwarded to the pqc-forum Google group list. We will periodically post and update the comments received to the appropriate algorithm.

All relevant comments will be posted in their entirety and should not include PII information in the body of the email message.

Please refrain from using OFFICIAL COMMENT to ask administrative questions, which should be sent to pqc-comments@nist.gov

Guidelines for Submitting Tweaks for Third Round Finalists and Candidates (pdf)

To read more:
https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Number 10

AI Improves Robotic Performance in DARPA's Machine Common Sense Program

New algorithms, simulated training prepare robots for real-world scenarios

Researchers with DARPA's Machine Common Sense (MCS) program demonstrated a series of improvements to robotic system performance over the course of multiple experiments.

Just as infants must learn from experience, MCS seeks to construct computational models that mimic the core domains of child cognition for objects (intuitive physics), agents (intentional actors), and places (spatial navigation).

Using only simulated training, recent MCS experiments demonstrated advancements in systems' abilities – ranging from understanding how to grasp objects and adapting to obstacles, to changing speed/gait for various goals.

"These experiments are important milestones that get us closer to building and fielding robust robotic systems with generalized movement capabilities," said Dr. Howard Shrobe, MCS program manager in DARPA's Information Innovation Office. "The prototype systems don't need large sensor suites to deal with unexpected situations likely to occur in the real world."

Rapidly Adapting to Changing Terrain

In one experiment, researchers at the University of California, Berkeley developed a rapid motor adaption (RMA) algorithm that allows quadruped robots to adapt rapidly to changing terrain.

Using the RMA algorithm and proprioceptive feedback (the sense of self-movement and body position), the robots successfully navigated through a range of both real-world and simulated terrain.

The algorithm is trained completely in simulation without using any domain knowledge-like reference trajectories or predefined foot trajectory generators and is deployed without any fine-tuning.

Real-time terrain adaption is essential for quadruped robots to help military units with load carrying and sensing.

Carrying Dynamic Loads

Oregon State researchers demonstrated the ability for a bipedal robot to learn how to carry dynamic loads with only proprioceptive feedback.

The robot, known as Cassie, learned commonsense behaviors in a simulated-to-real learning environment.

Cassie adapted its gait to account for changes in load dynamics, such as sloshing liquids or balancing weights.

After training in simulation, Cassie was able to walk on a treadmill for several minutes with four different types of dynamic loads. In contrast, before the learned commonsense training, Cassie fell immediately.

Understanding How to Grasp Objects

In natural environments, humans encounter a vast variety of possible tools, tool variations, and objects. This variety presents a challenge for robots.

They must foresee all possibilities to function, which is why it's important that they're equipped with a general grasping capability rather than a specialized capability, for a predefined set of objects.

University of Utah researchers as part of the Oregon State University MCS team developed an active, grasp-learning algorithm that allows robots with multi-fingered hands to dexterously grasp previously unseen objects when trained entirely in simulation.

The new approach enabled the robot to grasp with higher than 93% real-world success on novel objects compared to 78% of existing passive learning approaches.

Additional Research

Another technical area within MCS seeks to develop computational tools that learn from reading the web, like a research librarian, to construct a commonsense knowledge repository capable of answering natural language and image-based questions about commonsense phenomena.

MCS researchers from the University of Washington and two teams from the University of Southern California, Information Sciences Institute are currently using a variety of approaches, including hyperbolic learning.

This technique learns the commonsense structure of human behavior and physics from large collections of videos to forecast human actions up to 30 seconds in the future.

The researchers are also building a scalable, machine-authored, symbolic knowledge base that will provide a higher quality, larger, and more diverse representation of the world.

“By focusing on commonsense, we are creating the possibility for systems to have the flexibility of human learning and the breadth of human knowledge,” Shrobe said. “Fusing this knowledge with advanced robotics could result in highly capable, mission-critical systems that humans will want to have as partners.”

To read more: https://www.darpa.mil/news-events/2022-22-06

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

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

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

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

3. *Training and Certification* – Become:

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

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

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

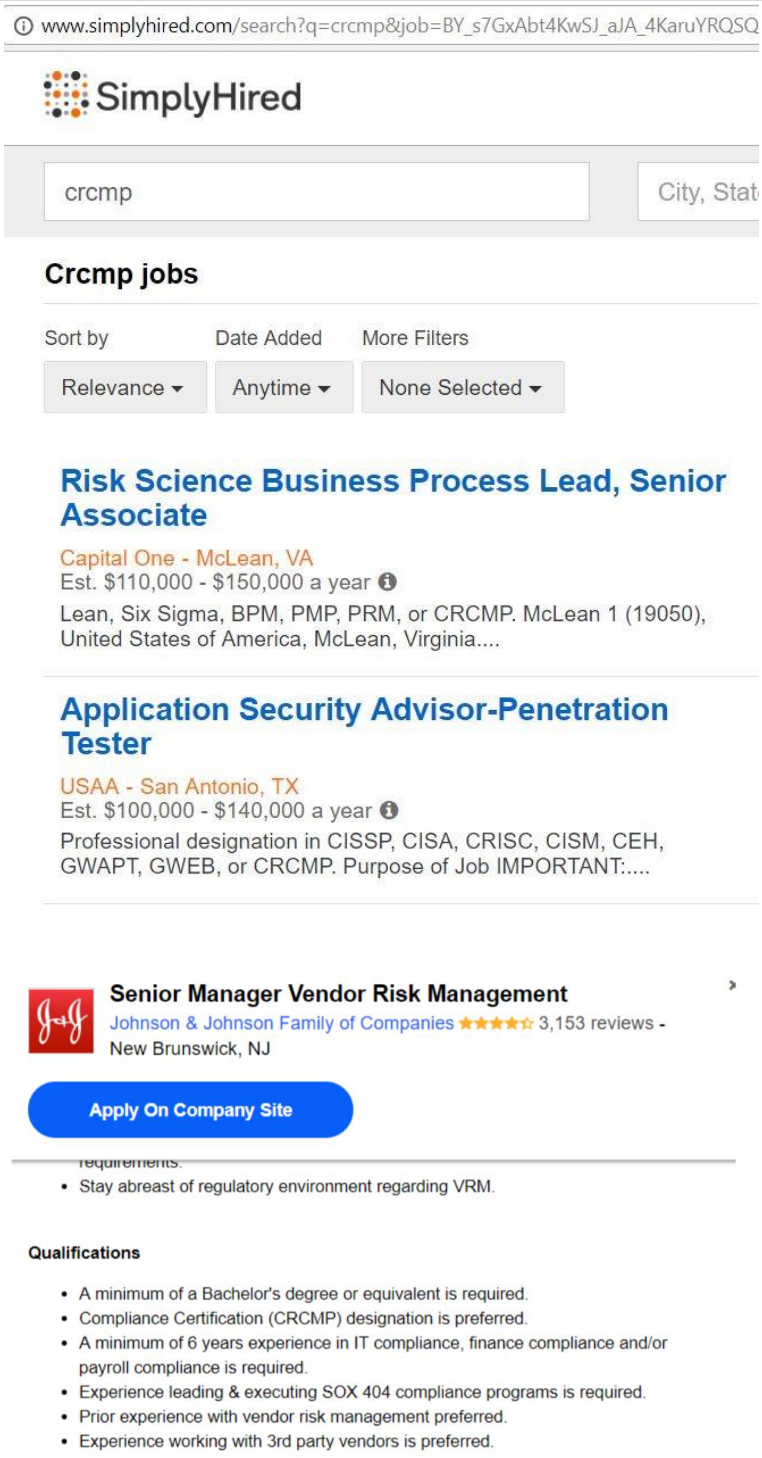
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

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

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

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



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

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

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

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

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

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

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

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

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