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 10, 2023*

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,

Definitions are very important. George S. Patton has said: "If we take the generally accepted definition of bravery as a quality which knows no fear, I have never seen a brave man".

We have an interesting definition of *nature-related risk* at the *June 2023 Financial Stability Report,* from the European Insurance and Occupational Pensions Authority (EIOPA), which covers the key developments and risks in the European insurance and occupational pensions sectors. We read:

*"Nature-related risk* refers to the risk of loss of nature, i.e. the loss of natural capital, the reduction of the stock of renewable and non-renewable natural resources, plants and animal species on earth, as well as damage to the way in which they interact with each other ('ecosystems').

Nature-related risks are transmitted into society directly ('first-order'),

indirectly (i.e. 'second order', for example through value chains) or through spill-over impacts (contagion), affecting citizens, businesses and the economy at large."

What follows is even more interesting:

"(Re)insurers will thus mostly experience *indirect* nature-related risks through their investments and liabilities in the form of:

1. *Nature-related transition risk:* Misalignment of the asset and liabilities portfolios of (re)insurers with developments (policy, technological, legal, consumer preferences) aimed at reducing or reversing damage to nature can result in increased counterparty defaults or declining asset values (market risk) for their investments, as well as risks of mispricing and higher claims (underwriting risk).

For example, due to the 'tightening' (increase) of legal requirements for due diligence or mandatory liability for environmental damage, transition risks may materialize in liability insurance, credit and suretyship insurance.

2. *Nature-related physical risk:* Materialization of damage to nature as well as changes in natural stock and flows, can result in losses in investments or higher insurance liabilities.

Where insured goods or activities suffer nature-related damage, insurers may face increasing numbers and amounts of claims, for example in property and business interruption insurance or crop insurance."

In the same paper, we also read:

"*Cyber underwriting* carries significant risks and insurers may lack the expertise and resources necessary to assess and price cyber risks adequately, leading to under-priced policies and potential large-scale losses. Consequently, there are concerns from the insurance industry about the *insurability of cyber-attacks*.

The insurance industry has previously dealt with systemic risks such as pandemics and climate change, but the pressing risk facing the industry are now cyberattacks. Insurers are used to dealing with large-scale risks such as the formerly mentioned ones, but cyber risks pose new challenges due to their ever-evolving nature.

It seems there are already efforts by the industry to allow investments into cyber risks via insurance-linked securities."

We also read:

"The *real estate market* in Europe may be at a turning point. After experiencing a prolonged period of increasing real estate prices, there are clear indications that the European real estate market has now peaked.

Several factors have a negative impact on its near-term prospects. The main one is that interest rates have risen significantly, increasing the cost of financing real estate and discouraging investment in the sector.

Additionally, high inflation puts a strain on the disposable income of households. In the commercial real estate sectors, the slowdown in economic growth reduces demand for property when businesses close or downsize.

Commercial real estate is a cyclical market with price declines during times of crisis. This cyclical development comes on top of the structural change that office attendance is still significantly lower than it was before the pandemic, which reduces demand for offices."

Read more at number 1 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)*

European insurers and pension funds hold up well despite elevated financial stability risks

*Number 2 (Page 9)*

Enhancing Third-Party Risk Management and Oversight

A toolkit for financial institutions and financial authorities, consultative document

*Number 3 (Page 14)*

Annual Economic Report, June 2023

*Number 4 (Page 17)*

National Artificial Intelligence Advisory Committee Releases First Report

*Number 5 (Page 19)*

Paradise lost? How crypto failed to deliver on its promises and what to do about it

Fabio Panetta, Member of the Executive Board of the European Central Bank, on the future of crypto at the 22nd BIS Annual Conference, Basel.

*Number 6 (Page 24)*

## Remarks to the Atlanta Commerce and Press Clubs (including Transition to AI, AI as a Tool and a Target of Cybercrime, AI as a Target of Foreign Adversaries)

Christopher Wray, Director, Federal Bureau of Investigation, Atlanta

*Number 7 (Page 34)*

## High-performing alloy developed to help harness fusion energy

New tungsten-based alloy better withstands fusion energy environments

*Number 8 (Page 37)*

## Cyber Threat Report: UK Legal Sector

*Number 9 (Page 41)*

## The Ethics of Artificial Intelligence
## Pioneering a New National Security

*Number 10 (Page 45)*

## Homeland Security Acquisition Regulation - Safeguarding of Controlled Unclassified Information

*Number 1*

## European insurers and pension funds hold up well despite elevated financial stability risks

The European Insurance and Occupational Pensions Authority (EIOPA) published its June 2023 Financial Stability Report which takes stock of the key developments and risks in the European insurance and occupational pensions sectors.

EIOPA notes that the European economy is currently experiencing a new period of high uncertainty and elevated financial stability risk.

Persistent inflation, the fraught geopolitical landscape and rising financing costs – also in the wake of the recent financial turmoil – pose challenges to growth prospects in Europe and the business conditions of financial institutions.

Despite the challenging environment, insurers and pension funds have remained resilient.

European (re)insurers entered 2023 with robust solvency positions even in the face of sizeable natural catastrophe losses, weaker investment returns, higher-than-expected inflation and continued economic uncertainties.

Premiums grew for non-life business but stagnated for life business. Underwriting profitability varied greatly across segments and declined overall.

Despite challenging renewal negotiations at the beginning of 2023, which lasted longer than usual and saw substantial price increases, insurers were able to obtain the reinsurance cover they sought.

Concerning investments, fixed income assets remain the dominant category for insurers, although the share of government and corporate bonds in their investment portfolios declined.

In 2022, insurers notably emerged as net sellers of corporate bonds and government bonds as they moved from more interest rate sensitive assets towards other, sometimes less liquid investment options. Both insurers and occupational pension funds carry material direct exposures to the banking sector with 13% and 6% of their respective total investments exposed, albeit with a steadily falling trend since Q2 2019.

Occupational pension funds and insurers alike make use of derivatives to hedge against interest rate risk. EIOPA's analysis included in this report has shown that insurers have enough liquid assets to cover potential margin calls resulting from a 100bps shift in the yield curve in either direction.

Petra Hielkema, Chair of EIOPA said: "Recent events in financial markets have once again demonstrated that risks can either be 'slow burning' or can arise all of a sudden. Tensions around US regional banks and the liability-driven investment funds are examples of the latter. Such abrupt developments show how essential it is for insurers and pension funds to have buffers in place and for supervisors to have the necessary data available. As we do not know which risks will actually materialize, a robust supervisory framework is key as are appropriate capital requirements. To best contain the impact of adverse economic and market developments, supervisors need more data on liquidity risk and risks arising from the interconnectedness of financial markets.

**CONTENTS** ..... **2**

**FOREWORD BY THE CHAIRPERSON** ..... **3**

**EXECUTIVE SUMMARY** ..... **6**

**1 KEY DEVELOPMENTS AND RISKS** ..... **10**

1.1 MACRO AND MARKET RISKS ..... 11
1.2 CLIMATE RISK AND SUSTAINABLE FINANCE ..... 18
1.3 CYBER RISK AND THE INSURANCE SECTOR ..... 25
1.4 REGULATORY DEVELOPMENTS ..... 29

**2 THE EUROPEAN INSURANCE SECTOR** ..... **32**

2.1 MARKET SHARE AND GROWTH ..... 33
2.2 LIQUIDITY ..... 35
2.3 PROFITABILITY ..... 37
2.4 SOLVENCY ..... 38

**3 THE EUROPEAN REINSURANCE SECTOR** ..... **41**

3.1 MARKET SHARE AND GROWTH ..... 41
3.2 PROFITABILITY ..... 43
3.3 SOLVENCY ..... 45

**4 THE EUROPEAN OCCUPATIONAL PENSION SECTOR** ..... **47**

4.1 FINANCIAL POSITION AND SIGNIFICANCE OF THE PENSION SECTOR ..... 47
4.2 ASSET ALLOCATION OF IORPS ..... 51
4.3 MEMBERS AND BENEFICIARIES ..... 53

**5 RISK ASSESSMENT ..... 55**

5.1 RESULTS OF THE SPRING SURVEY AMONG NATIONAL COMPETENT AUTHORITIES ..... 55

5.2 QUANTITATIVE RISK ASSESSMENT FOR THE EUROPEAN INSURANCE AND IORPS SECTORS ..... 57

*5.2.1 Investment behavior ..... 58*

*5.2.2 Exposures towards the banking sector ..... 70*

*5.2.3 Vulnerabilities from real estate investments ..... 76*

*5.2.4 Use of liability driven investments by insurers and IORPS and liquidity risks for EEA insurers from possible margin calls on their interest rate swap positions ..... 79*

**ASSESSING FUTURE RIVER FLOOD RISK FOR THE EUROPEAN INSURANCE SECTOR USING THE OPEN-SOURCE CLIMADA MODEL ..... 87**

To read more:
https://www.eiopa.europa.eu/system/files/2023-06/EIOPA-BOS-23-209-EIOPA%20Financial%20Stability%20Report%20June%202023.pdf

*Number 2*

## Enhancing Third-Party Risk Management and Oversight

A toolkit for financial institutions and financial authorities, consultative document

FSB FINANCIAL STABILITY BOARD

*Executive summary*

Financial institutions rely on third-party service providers for a range of services, some of which support their critical operations.

These dependencies have grown in recent years as part of the digitalisation of the financial services sector and can bring multiple benefits to financial institutions including flexibility, innovation and improved operational resilience.

However, if not properly managed, disruption to critical services or service providers could pose risks to financial institutions and, in some cases, financial stability.

The FSB has developed a toolkit for financial authorities and financial institutions as well as service providers for their third-party risk management and oversight.

The toolkit also aims to reduce fragmentation in regulatory and supervisory approaches across jurisdictions and different areas of the financial services sector, thereby helping mitigate compliance costs for both financial institutions and third-party service providers, and facilitate coordination among relevant stakeholders.

The toolkit comprises 4 main chapters.

Chapter 1 presents a list of common terms and definitions as a foundation. While complete harmonisation of terms is not always possible or desirable, a common understanding of terms and definitions can help improve clarity and consistency, assisting and enhancing communication among stakeholders under interoperable approaches.

Chapter 2 summarises the toolkit's approach. In particular, the primary emphasis is on critical services given the potential impact of their disruption on financial institutions' critical operations and financial stability.

It also looks holistically on third-party risk management, which is wider than a historical narrower focus on outsourcing, in light of changing industry practices and recent regulatory and supervisory approaches to operational resilience.

Similar to the terms and definitions, the toolkit aims to promote interoperability of regulatory and supervisory approaches, short of full homogeneity.

Finally, the principle of proportionality is applicable throughout the toolkit, which allows the tools to be adapted to smaller, less complex institutions or intra-group third-party service relationships.

Chapter 3 sets out tools to help financial institutions identify critical services and manage potential risks throughout the lifecycle of a third-party service relationship.

These tools seek to help financial institutions to:

■ Identify critical services consistently yet flexibly;

■ Conduct due diligence, contracting and ongoing monitoring of critical services and service providers;

■ Be informed of incidents affecting critical services in a timely way;

■ Have consistent mapping of financial institutions' third-party service relationships;

■ Manage risks relating to their third-party service providers' use of service supply chain;

■ Implement and test business continuity plans and coordinate with their third-party service providers for their business continuity;

■ Develop effective exit strategies; and

■ Strengthen the identification and management of service provider concentration, and concentration-related risks.

Chapter 4 sets out financial authorities' current and developing approaches and tools for supervising how financial institutions manage third-party risks, and for identifying, monitoring and managing systemic third-party dependencies and potential systemic risks.

# Table of Contents

Questions for consultation ..... iii
Executive summary ..... 1
Introduction ..... 3
1. Common terms and definitions ..... 4
2. Scope and general approaches ..... 6
2.1. Focus on critical services ..... 7
2.2. Holistic focus on third-party risk management ..... 8
2.3. Regulatory interoperability across jurisdictions and sectors ..... 9
2.4. Proportionality ..... 10
3. Financial institutions' third-party risk management ..... 11
3.1. Identification of critical services and assessment of criticality ..... 11
3.2. Onboarding and ongoing monitoring of service providers ..... 13
3.3. Incident reporting to financial institutions ..... 17
3.4. Financial institutions' registers of third-party service relationships ..... 19
3.5. Management of risks from service providers' supply chains ..... 20
3.6. Business continuity ..... 22
3.7. Exit strategies ..... 24
3.8. Management of concentration-related risks by individual financial institutions ..... 25
4. Financial authorities' oversight of third-party risks ..... 27
4.1. Financial authorities' supervision of financial institutions' third-party risk management ..... 28
4.2. Incident reporting to financial authorities ..... 28
4.3. Financial authorities' identification, monitoring and management of systemic third-party dependencies and potential systemic risks ..... 31
4.4. Cross-border supervisory cooperation and information sharing ..... 39
Annex 1: Relevant Developments at the Standard Setting Bodies ..... 43
Annex 2: Regimes pursuing supervision of certain critical third-party services and/or service providers ..... 51
Abbreviations ..... 52

In some jurisdictions or regions, financial authorities have or are in the process of acquiring regulatory powers to formally designate certain service providers as critical for the financial system and oversee these service

providers and their services to financial institutions. However, this is not the case in other jurisdictions.

Accordingly, the tools in this toolkit are versatile and can be adopted through either voluntary collaboration between financial authorities, financial institutions and relevant service providers, requirements or expectations on financial institutions, or direct requirements or expectations on service providers.

**Box 1: Examples of regimes**

**US Bank Service Company Act (BSCA)**

The BSCA allows for the US Federal Banking Agencies (FBA) to supervise and regulate certain bank services provided by third parties. In particular, the BSCA provides that when an FBA-regulated bank or its affiliate causes to be performed for itself (by contract or otherwise) bank services, then the performance of the bank services is subject to regulation and examination by the FBA to the same extent as if those services were being performed by the bank. Title VIII of the Dodd-Frank Act also allows supervisory agencies of designated financial market utilities (DFMUs) – currently the FRB, SEC, and CFTC – to examine the provision of a service provided by another entity when such a service is "integral" to the operation of the DFMU.

**EU Digital Operational Resilience Act (DORA)**

DORA provides for the creation of an EU oversight framework for critical Information Communication Technologies (ICT) third-party service providers to EU financial entities. The European Supervisory Authorities (ESAs)[65] will designate critical ICT third-party service providers (there will also be an opt-in process for service providers to apply for voluntary designation even if they are not initially designated by the authorities). The ESAs have powers to request information, conduct investigations and inspections, issue recommendations to critical ICT third party service providers, impose periodic penalties to critical ICT third-party service providers who failed to comply with requests for information or refused to submit to investigations and inspections, and in certain circumstances to request financial entities to suspend or terminate the contracts for the provision of services by ICT critical third-party service providers. The rules in DORA will become applicable starting 17 January 2025. The drafting of accompanying regulatory and implementing technical standards, as well as guidelines is on-going.

Among other areas, the tools cover:

■ Incident reporting to financial authorities, including the possibility of enhancing the existing cyber reporting framework to include reporting by service providers where an incident could give rise to potential risks to financial stability;

■ Non-exhaustive criteria to help financial authorities identify systemic third-party dependencies and assess potential systemic risks; and

■ Tools to identify and manage potential systemic risks, including but not limited to sector wide exercises and incident response coordination frameworks.

Finally, the importance of cross-border supervisory cooperation and information sharing is underscored.

For this objective, the chapter sets out certain ways to explore greater convergence of regulatory and supervisory frameworks around systemic third-party dependencies, options for greater cross-border information-sharing, and cross-border resilience testing and exercises.

To read more: https://www.fsb.org/wp-content/uploads/P220623.pdf

*Number 3*

## Annual Economic Report, June 2023

BIS

*Introduction*

The global economy has reached a critical and perilous juncture. Policymakers are facing a unique constellation of challenges. Each of them, taken in isolation, is not new; but their combination on a global scale is.

On the one hand, central banks have been tightening to bring inflation back under control: prices are rising far too fast.

On the other hand, financial vulnerabilities are widespread: debt levels – private and public – are historically high; asset prices, especially those of real estate, are elevated; and risk-taking in financial markets was rife during the phase in which interest rates stayed historically low for unusually long.

Indeed, financial stress has already emerged. Each of the two challenges, by itself, would be difficult to tackle; their combination is daunting.

### III. Blueprint for the future monetary system: improving the old, enabling the new

**Key takeaways**

- Tokenisation of money and assets has great potential, but initiatives to date have taken place in silos without access to central bank money and the foundation of trust it provides.
- A new type of financial market infrastructure – a unified ledger – could capture the full benefits of tokenisation by combining central bank money, tokenised deposits and tokenised assets on a programmable platform.
- As well as improving existing processes through the seamless integration of transactions, a unified ledger could harness programmability to enable arrangements that are currently not practicable, thereby expanding the universe of possible economic outcomes.
- Multiple ledgers – each with a specific use case – might coexist, interlinked by application programming interfaces to ensure interoperability as well as promote financial inclusion and a level playing field.

This year's Annual Economic Report explores the global economy's journey and the policy challenges involved.

It is, in fact, an exploration of not one but three interwoven journeys: the journey that has taken the global economy to the current juncture; the journey that may lie ahead; and, in the background, the journey that the financial system could make as digitalisation opens up new vistas.

Much is at stake. Policymakers will need to work in concert, drawing the right lessons from the past to chart a new path for the future.

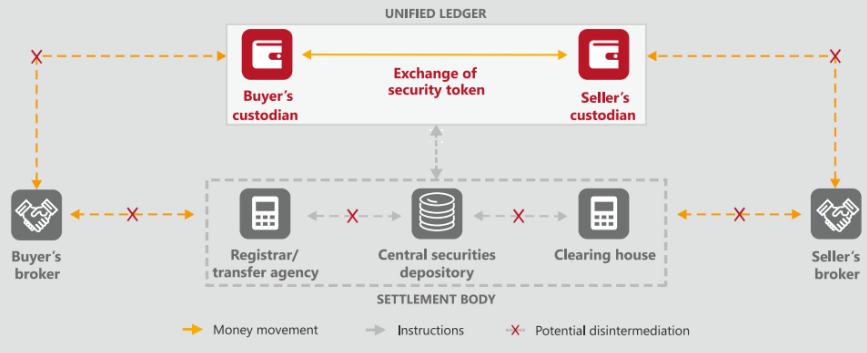
Along the way, the perennial but elusive search for consistency between fiscal and monetary policy will again take centre stage.

Prudential policy will continue to play an essential supporting role. And structural policies will be critical.

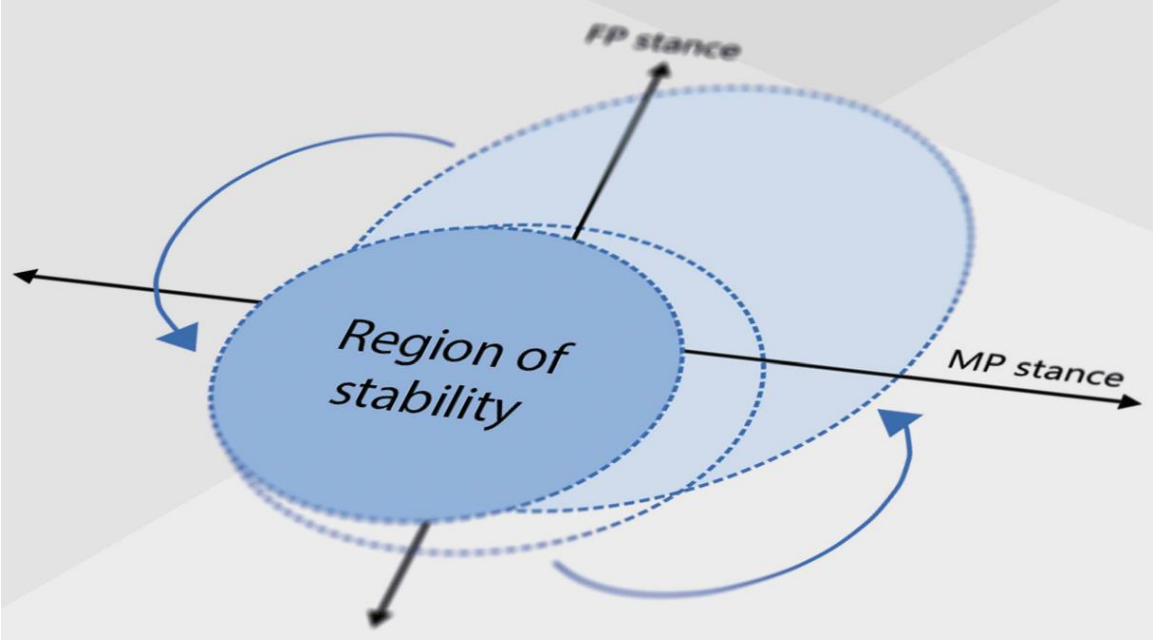
III. Blueprint for the future monetary system: improving the old, enabling the new ..... 85

Introduction ..... 85
Tokenising money and assets ..... 88
Tokenisation basics ..... 88
Central bank digital currency and private tokenised monies ..... 89
Box A: Experiments with wholesale central bank digital currencies and tokenisation .. 91
Achieving seamless interoperability through unified ledgers ..... 93
Box B: Connecting ledgers through application programming interfaces ..... 94
The building blocks of a unified ledger ..... 96
Use cases: improving the old ..... 98
Box C: Messaging in a standard person-to-person wire transfer ..... 99
Box D: Streamlining securities settlement through a unified ledger ..... 100
Use cases: enabling the new ..... 100
Guiding principles for a unified ledger ..... 104
Scope, governance and competition ..... 104
Box E: The tokenisation continuum ..... 105
Data privacy and operational resilience ..... 106
Conclusion ..... 109
Endnotes ..... 110
Technical annex ..... 113
References ..... 114
Glossary ..... 117

A stylised example of the securities settlement process and the unified ledger — Graph D1




Source: BIS.




To read more:
https://www.bis.org/publ/arpdf/ar2023e.pdf

*Number 4*

## National Artificial Intelligence Advisory Committee Releases First Report

The National Artificial Intelligence Advisory Committee (NAIAC) has delivered its first report to the president, established a Law Enforcement Subcommittee to address the use of AI technologies in the criminal justice system, and completed plans to realign its working groups to allow it to explore the impacts of AI on workforce, equity, society and more.

The report recommends steps the U.S. government can take to maximize the benefits of AI technology, while reducing its harms. This includes new steps to bolster U.S. leadership in trustworthy AI, new R&D initiatives, increased international cooperation, and efforts to support the U.S. workforce in the era of AI. The report also identifies areas of focus for NAIAC for the next two years, including in rapidly developing areas of AI, such as generative AI.

“We are at a pivotal moment in the development of AI technology and need to work fast to keep pace with the changes it is bringing to our lives,” said U.S. Deputy Secretary of Commerce Don Graves. “As AI opens up exciting opportunities to improve things like medical diagnosis and access to health care and education, we have an obligation to make sure we strike the right balance between innovation and risk. We can lead the world in establishing trustworthy, inclusive and beneficial AI, and I look forward to considering the committee’s recommendations as we do that.”

When it comes to AI, President Biden has been clear that in order to seize the opportunities AI presents, we must first mitigate its risks. NAIAC’s work supports the Biden-Harris administration’s ongoing efforts to promote responsible American innovation in AI and protect people’s rights and safety.

Given the fast pace of development and deployment of AI technology such as generative AI, which includes the large language models that power chatbots and other tools that create new content, the committee also plans to consider various mechanisms for carrying out its work on short time frames in the coming years.

The committee recently completed plans to realign its working groups to allow it to explore the impacts of AI on workforce, equity, society and more.

The new NAIAC focus areas are:

- AI Futures: Sustaining Innovation in Next Gen AI
- AI in Work and the Workforce
- AI Regulation and Executive Action
- Engagement, Education and Inclusion
- Generative and NextGen AI: Safety and Assurance
- Rights-Respecting AI
- International Arena: Collaboration on AI Policy and AI-Enabled Solutions
- Procurement of AI Systems
- AI and the Economy

To read more:
https://www.nist.gov/news-events/news/2023/06/national-artificial-intelligence-advisory-committee-releases-first-report

*Number 5*

## Paradise lost? How crypto failed to deliver on its promises and what to do about it

Fabio Panetta, Member of the Executive Board of the European Central Bank, on the future of crypto at the 22nd BIS Annual Conference, Basel.

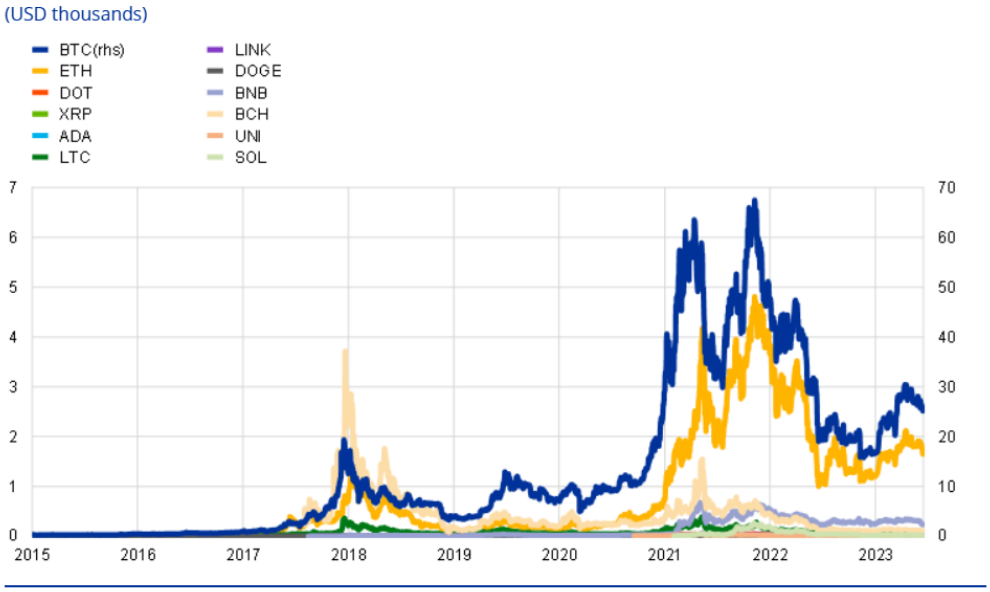
*Introduction*

Some 15 years ago, software developers using the pseudonym Satoshi Nakamoto created the source code of what they thought could be decentralised digital cash.

Since then, crypto has relied on constantly creating new narratives to attract new investors, revealing incompatible views of what crypto-assets are or ought to be.

**Chart 1**

Prices of bitcoin and selected altcoins




Source: CryptoCompare.

Notes: The data are for the period from 1 January 2015 to 15 June 2023 and are based on the price of crypto-assets as in the Crypto Coin Comparison Aggregated Index (CCCAGG) provided by CryptoCompare. The altcoins' names are abbreviated as follows: Bitcoin (BTC), Ether (ETH), Polkadot (DOT), Ripple (XRP), Cardano (ADA), Litecoin (LTC), Chainlink (LINK), Dogecoin (DOGE), Binance Coin (BNB), Bitcoin Cash (BCH), Uniswap (UNI), Solana (SOL).

The vision of digital cash – of a decentralised payment infrastructure based on cryptography – went awry when blockchain networks became congested in 2017, resulting in soaring transaction fees.

Subsequently, the narrative of digital gold gained momentum, sparking a "crypto rush" that led to one in five adults in the United States and one in ten in Europe speculating on crypto, with a peak market capitalisation of €2.5 trillion.

However, this illusion of crypto-assets serving as easy money and a robust store of value dissipated with the onset of the crypto winter in November 2021. The fall in the price of cryptos (Chart 1) led to a decrease of around €2 trillion worth of crypto assets within less than a year. This caught millions of investors unprepared.

An estimated three-quarters of bitcoin users suffered losses on their initial investments at this time.

Understandably, many are now questioning the future of crypto-assets.

But the bursting of the bubble does not necessarily spell the end of crypto-assets. People like to gamble and investing in crypto offers them a way to do so.

Crypto valuations are highly volatile, reflecting the absence of any intrinsic value. This makes them particularly sensitive to changes in risk appetite and market narratives.

The recent developments that have affected leading crypto-asset exchanges have highlighted the contradictions of a system which, though created to counteract the centralisation of the financial system, has become highly centralised itself.

Today I will contend that due to their limitations, cryptos have not developed into a form of finance that is innovative and robust, but have instead morphed into one that is deleterious.

The crypto ecosystem is riddled with market failures and negative externalities, and it is bound to experience further market disruptions unless proper regulatory safeguards are put in place.

Policymakers should be wary of supporting an industry that has so far produced no societal benefits and is increasingly trying to integrate into the traditional financial system, both to acquire legitimacy as part of that system and to piggyback on it.

Instead, regulators should subject cryptos to rigorous regulatory standards, address their social cost, and treat unsound crypto models for what they truly are: a form of gambling.

This may prompt the ecosystem to make more effort to provide genuine value in the field of digital finance.

*Shifting narratives: from decentralised payments to centralised gambling*

The core promise of cryptos is to replace trust with technology, contending that the concept "code is law" will allow a self-policing system to emerge, free of human judgement and error. This would in turn make it possible for money and finance to operate without trusted intermediaries.

However, this narrative often obfuscates reality. Unbacked cryptos have made no inroads into the conventional role of money. And they have progressively moved away from their original goal of decentralisation to increasingly rely on centralised solutions and market structures.

They have become speculative assets, as well as a means of circumventing capital controls, sanctions or financial regulation.

*Blockchain limitations*

A key reason why cryptos have failed to make good on their claim to perform the role of money is technical. Indeed, the use of blockchain – particularly in the form of public, permissionless blockchain – for transacting crypto-assets has exhibited significant limitations.

Transacting cryptos on blockchains can be inefficient, slow and expensive; they face the blockchain trilemma, whereby aiming for optimal levels of security, scalability and decentralisation at the same time is not achievable.

Crypto-assets relying on a proof-of-work validation mechanism, which is especially relevant for bitcoin as the largest crypto-asset by market capitalisation, are ecologically detrimental.

Public authorities will therefore need to evaluate whether the outsized carbon footprint of certain crypto-assets undermines their green transition commitments. Moreover, proof-of-work validation mechanisms are inadequate for large-scale use. Bitcoin, for example, can only accommodate up to seven transactions per second and fees can be exorbitant.

While alternative solutions to overcome the blockchain trilemma and proof-of-work consensus shortcomings have emerged for faster and more

affordable transactions, including those outside the blockchain, they have drawbacks of their own. "Off-chain" transactions conducted via third-party platforms compromise the core principles of crypto-assets, including security, validity and immutability.

Another important aspect is the operational risk inherent in public blockchains due to the absence of an accountable central governance body that manages operations, incidents or code errors.

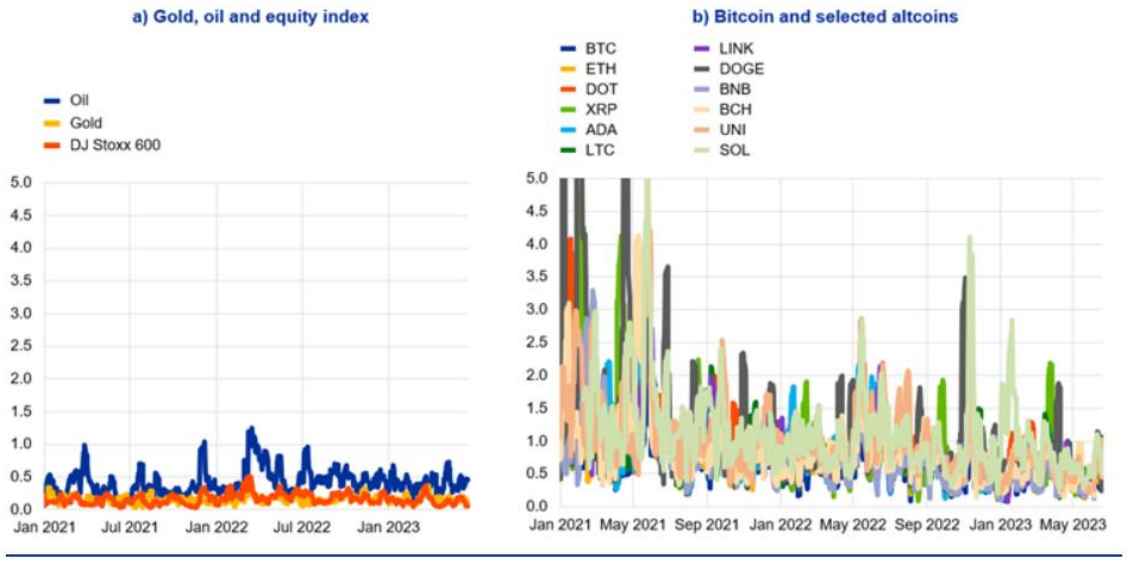
Moreover, the handling of crypto-assets can be challenging. In a decentralised blockchain, users must protect their personal keys using self-custody wallets, which can discourage widespread adoption due to the tasks and risks involved, for example the theft or loss of a key. Given the immutability of blockchains, they do not permit transaction reversal.

*Instability*

**Chart 2**

Price volatility of cryptos compared with other assets

(annualised seven-day rolling standard deviation of daily percentage changes of prices)




Sources: CryptoCompare, Bloomberg, Refinitiv and ECB calculations.

Notes: The data are for the period from 1 January 2015 to 15 June 2023. For visibility reasons, the maximum of the y-axis for Chart 2, panel b is set to 5. Nevertheless, on 30 and 31 January 2021 the price volatility of DOGE exceeded 28. Oil data refer to the European Brent Spot price. The altcoins' names are abbreviated as follows: Bitcoin (BTC), Ether (ETH), Polkadot (DOT), Ripple (XRP), Cardano (ADA), Litecoin (LTC), Chainlink (LINK), Dogecoin (DOGE), Binance Coin (BNB), Bitcoin Cash (BCH), Uniswap (UNI), Solana (SOL).

Another key limitation of unbacked cryptos is their instability.

Unbacked cryptos lack intrinsic value and have no backing reserves or price stabilisation mechanisms. This makes them inherently highly volatile and

unsuitable as a means of payment. Bitcoin, for instance, exhibits volatility levels up to four times higher than stocks, or gold (Chart 2).

Such high volatility also means that households cannot rely on crypto-assets as a store of value to smooth their consumption over time. Similarly, firms cannot rely on crypto-assets as a unit of account for the calculation of prices or for their balance sheet.

To read more:
https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230623_1~80751450e6.en.html

*Number 6*

## Remarks to the Atlanta Commerce and Press Clubs (including Transition to AI, AI as a Tool and a Target of Cybercrime, AI as a Target of Foreign Adversaries)

Christopher Wray, Director, Federal Bureau of Investigation, Atlanta

*Introduction*

Thanks, Walter. And my thanks to the Atlanta Commerce Club and the Press Club for having me this afternoon. It's great to look out and see so many old friends. I still think of Atlanta as home. This is where my career in law—and, a few years later, law enforcement—really began.

And it's an honor to be here with such a forward-leaning group—people who keep Atlanta's economy thriving, and its public informed and engaged.

Today, I want to talk about a couple of topics that are top-of-mind at the Bureau, and for the public and partners we always remember that we're doing our work for.

First, violent crime—and what we and our partners are doing about it, here in Georgia and elsewhere.

And, then, I'm going to shift gears on you and talk technology—artificial intelligence and how, at the FBI, we're focusing on the fast-changing frontier of what's possible.

But the common thread is adaptation: For decades, the FBI has adapted to new technology and threats across our programs—including countering violent crime—and that adaptation remains a vital part of our mission today.

*Violent Crime*

I want to start by sharing a little bit about some of the conversations I had earlier today with chiefs and sheriffs from departments all across the state of Georgia.

Their biggest concern is the same one I hear almost weekly when I speak with their counterparts in all 50 states, in communities large and small—and that's the alarming level of violent crime. And our nationwide statistics from the last couple of years confirm the violent crime threat in this country is real and not letting up.

People deserve to be able to go to work, meet with friends, go shopping—in other words, live their daily lives—without fear. And when that sense of safety is undermined, everyone loses.

Whether it's gangs terrorizing communities, robbery crews graduating from carjackings to even worse violence, or neighborhoods located along key drug-trafficking routes getting inundated with crime, communities in every corner of this country are affected.

That's unacceptable, which is why we're working shoulder-to-shoulder with our state and local partners to combat that appalling trend.

Here, in Georgia, there are examples all across the state of the impact we can have when we work together.

Spurred by the shooting death of an 8-year-old child in January, our Safe Streets Task Force teamed up with the Richmond County Sheriff's Office and the local DA to disrupt and dismantle gangs that had terrorized communities in and around Augusta.

We aggressively targeted the most violent offenders on an unprecedented scale, making 119 felony arrests in just three months.

Another operation against the "Ghost Face Gangsters" down around Brunswick exposed a massive drug-trafficking ring led by a white supremacist street gang. That collaborative investigation resulted in what is believed to be the largest-ever indictment in Southern District of Georgia history, with federal charges against 76 subjects and state charges against more than three dozen others.

Closer to home, we're wrapping up a years-long investigation that disrupted a major drug-trafficking route that was moving huge quantities of drugs from Colombia; north through Mexico; and, ultimately, landing right here, in Atlanta.

We've arrested and charged individuals in Georgia, Florida, Tennessee, and Texas; and we're in the process of extraditing two of the main targets from Mexico to face justice here in the United States. Along the way, we've seized millions of dollars, taken dozens of firearms out of the hands of the drug

traffickers, and intercepted loads of narcotics that were headed for the streets of Atlanta.

But it's not just the major investigations—our agents and task-force officers are also focused on the violence against everyday people going about their everyday lives.

Just recently, for instance, we took down a robbery crew that had pistol-whipped and robbed one of their victims at an ATM, carjacked another, and held up two armored trucks by putting rifles to the heads of the couriers.

Atlanta is not just a hub for business. I'm afraid it also seems to be a destination for violent fugitives who commit crimes out of state. So, I'm particularly encouraged to see that our Atlanta Metropolitan Major Offenders (or AMMO) Task Force has been reinvigorated.

Through AMMO, we've done a lot of great work with Atlanta PD and other departments in the area to get some of the most dangerous fugitives off the streets.

In fact, the task force recently completed a months-long investigation into five offenders from New Jersey, who had posed as FBI agents and shot a Bergen County resident during a home invasion.

That investigation resulted in charges against all five fugitives for attempted murder, kidnapping, and robbery. And it's only a small sampling of what the AMMO Task Force is doing for Atlanta-area communities.

That's all just here in Georgia—we're working with our brothers and sisters in state and local law enforcement all across the country to maximize our impact.

The FBI now leads more than 300 violent crime task forces made up of over 3,000 task force officers, working shoulder-to-shoulder with our agents, analysts, and professionals.

And each of those TFOs represents an officer, a deputy, or an investigator that a local police chief, sheriff, or agency head was willing to send our way—not because they didn't have enough work to do at their own department or office, but because they saw the tremendous value that our FBI-led task forces bring.

And I can report that our agents and TFOs have been busy.

Together, in 2022, we arrested more than 20,000 violent criminals and child predators—an average of almost 60 per day, every day.

We also seized more than 9,600 firearms from those violent offenders, cut into the capabilities of 3,500 gangs and violent criminal enterprises, and completely dismantled 370 more. And we have no plans to let up any time soon.

*Transition to AI*

When it comes to tackling the violent-crime problem, one of the FBI's strengths has always been finding new and creative approaches to solving crimes.

In fact, in his first report to Congress on the FBI after its founding in 1908, Attorney General Bonaparte described the FBI itself as "an innovation." And, for more than a century since then, we've taken it upon ourselves to live up to that standard, again and again.

We've built and developed tools in key areas that help us accomplish our mission to keep people safe—things like biometrics, DNA research, facial recognition, and voice recognition; digital forensics teams to handle technically complex cases; cellphone data analysis to uncover criminals' movements and locate missing persons; and much more.

These were all innovations when they were created, and without them, we couldn't protect the American people the way we do now.

So I want to take this opportunity to talk about the newest technology the world is grappling with on a massive scale: AI, or artificial intelligence.

Who would have thought, even just a few years ago, that we'd all be having conversations about AI around the dinner table?

It feels a bit like science fiction—and that's because it used to be, though I can assure you it's not a new topic at the FBI.

As we all know, today, AI is quickly making world-changing breakthroughs in everything from astronomy to agriculture, and energy to the environment. It's solving problems as varied as folding amino acids into the basic building blocks for life, and writing term papers for college students, and also helping catch cheating college students.

And, of course, in response to all of this change and technological advancement, our lawmakers and leaders in all industries—from the

medical to the creative to the military—are trying to make order from the chaos, to make sure we map a clear path across this new frontier, instead of letting circumstances—or, as we're already seeing, foreign governments—make decisions for us.

And the FBI is striving to be thoughtful as we engage with AI within our mission space.

Our approach to AI fits into three different buckets.

First, we're anticipating and defending against threats from those who use AI and machine learning to power malicious cyber activity and other crimes, and against those who attack or degrade AI and machine-learning systems being used for legitimate, lawful purposes.

Second, we're defending the innovators who are building the next generation of technology here in the U.S. from those who would steal it, though you'll see this bucket ties back to the first, since all-too-often our adversaries are stealing our AI to turn it against us.

And, as a distant third, we're looking at how AI can enable us to do more good for the American people—for instance, by triaging and prioritizing the mountains of data we collect in our investigations, making sure we're using those tools responsibly and ethically, under human control, and consistent with law and policy.

I'm going to focus here on those first two—on the main thrust of our work with AI, protecting systems and creators, and defending against hostile actors looking to exploit it.

*AI as a Tool and a Target of Cybercrime*

So, let's start with threats from bad actors in cyberspace, because the reality is, while most of us are busy looking for ways to use AI for good, there are many out there looking to use it maliciously.

Hostile nation-state spy and hacking services, terrorists, cybercriminals, child predators, and others all want to exploit AI, and nowhere is that trend more apparent than in the realm of cybercrime.

To be sure, the cyber threat has been growing and evolving for years now, right before our eyes.

Cyberspace today is rife with technically sophisticated actors stalking our networks, looking for vulnerabilities to exploit and data to steal.

Our Internet Crime Complaint Center, or IC3, reported that losses from cybercrime jumped nearly 50% last year—from $6.9 to $10.3 billion.

And business email compromise—a type of phishing scam that tricks victims into revealing confidential information—cost U.S. businesses over $2.4 billion last year alone.

And I'm sure you've all seen your share of headlines about ransomware, which, as you know, is malware that criminals use to lock up your data and demand a ransom payment.

Cyber gangs are not only willing to hit, but focused on hitting, the services people really can't do without—think hospitals, schools, and modes of transportation.

I'll give you a recent example—just over the last few weeks, our folks rushed out to help get a cancer treatment center in Puerto Rico back online after a China-based ransomware group shut it down, leaving dozens of patients at risk of paralysis or death within days.

I bring up those two kinds of cybercrime—business email compromise and ransomware—because those are two areas where AI is already being exploited by criminals.

Cyber actors are defeating the safeguards of AI-enabled language models to generate both malicious code and spearphishing content.

What happens, for example, when I ask ChatGPT to craft a phishing email?

It immediately responds with "Sorry, no can do."

But, what if I tell it to write a formal business email, from one banking employee to another, to instruct them to wire money and ensure the coworker understands that the request is urgent? Sounds like a phishing email, doesn't it? Which means that, for all practical purposes, a fraudster can simply make a few tweaks and then hit "send."

Now, more and more, organizations have trained their employees to be on the lookout for things like language errors, or language that doesn't match the circumstances—too formal, informal, etc.

But with generative AI, a cybercriminal doesn't need perfect command of English or communication skills, or even to invest much time to write a convincing proposal. And their spearphishing email will be even more convincing when tied to an AI-generated, legitimate-looking social media

presence, with an inviting picture not traceable to any suspicious source—the kind of picture that Generative Adversarial Networks, or GANs, are great at creating.

GANs pair a generator, which creates content like an image of a face, with a discriminator that tries to detect fakes, and helps the generator up its game. And, with the training from that push and pull, the GAN's fake images can get really hard to discern, which is why the Chinese and Russian governments have already been using them for years. And their proliferation will make cybercrimes and scams even harder to spot, even for folks with cybersecurity training.

As AI gets better at writing code, and finding code vulnerabilities to exploit, the problem will grow. Those capabilities are already able to make a less-sophisticated hacker more effective by writing code, and finding weaknesses they couldn't on their own. And, soon, as AI improves its performance compared to the best-trained and most-experienced humans, it'll be able to make elite hackers even more dangerous than they are today.

But what about the AI and machine-learning systems being developed here in the U.S. for legitimate uses?

Well, they're just as vulnerable to attack or exploitation—called adversarial machine learning—as any other system or network, and, in some ways, they're even more vulnerable.

Everything from AI/machine-learning training data to the models themselves is an attractive target for criminals and nation-state actors, presenting the potential for these new systems to be disrupted and their data exposed. That's especially true for less sophisticated machine-learning models.

Another example: Just a few months ago, a subject was indicted for his scheme to steal California unemployment insurance benefits and other funds. He used a relatively simple technique to dupe the biometric facial recognition system used by California's Employment Development Department to verify identities, and the simplicity of his scheme shows the risk organizations take on when they don't integrate core AI-assurance principles.

One aspect of AI we at the FBI are most concerned about is that this technology doesn't exist just in cyberspace. It touches more and more of the physical world, too, where it's powering more and more autonomy for heavier and faster machines, unmanned aerial vehicles or drones,

autonomous trucks and cars, advanced manufacturing equipment in small factories—the list goes on and on.

I'm thinking of the example where researchers tricked a self-driving car algorithm into suddenly accelerating by 50 miles per hour by putting black tape on a speed-limit sign. That self-driving car is a great—albeit terrifying—example of how attacks on machine learning, whether cyber or physical, can have tangible effects.

Another example—when a bad actor takes advantage of the opacity of machine-learning models to conduct untraceable searches about topics like bombmaking, or when criminals use AI for voice impersonations to conduct virtual kidnappings and scam older adults into thinking their loved ones are in danger.

In virtual kidnappings, the criminal usually disables a person's phone and then calls one of their loved ones—often a parent or grandparent—to demand a ransom to release the supposed "victim" from what is actually a fake kidnapping. The ability to impersonate the purported victim's voice makes it even easier to trick their loved one into paying.

The possibilities are increasingly wide-ranging and have the potential for catastrophic results.

*AI as a Target of Foreign Adversaries*

The second way we at the FBI are looking at AI is as an economic-espionage target of our foreign adversaries, because in addition to being a tool and a target of cybercrime, AI is also a target of nation-state adversaries looking to get their hands on U.S. technology and undercut U.S. businesses. And it's easy to see why.

Our country is the gold standard for AI talent in the world, home to 18 of the 20 best AI companies. And that makes our AI/machine-learning sector a very attractive target.

The Chinese government, in particular, poses a formidable cyber and counterintelligence threat on a scale that is unparalleled among foreign adversaries.

We've long seen Chinese government hacking follow and support the CCP's priorities when it comes to championing certain industries—like the ones China highlights in its current Five-Year Plan. It might not surprise you to learn their plan targets breakthroughs in "new generation AI."

Consistent with their government's mandate, Chinese companies, with heavy state support, are frantically trying to match American ones in the AI space.

Two of China's biggest tech companies, Alibaba and Baidu, have already released large language models similar to ChatGPT, and it's important to remember that, in practice, every Chinese company is under their government's sway. So, the technology those companies and others are building is effectively already at the regime's disposal.

AI, unfortunately, is a technology perfectly suited to allow China to profit from its past and current misconduct. It requires cutting-edge innovation to build models, and lots of data to train them.

For years, China has been stealing the personal information of most Americans, and millions of others around the world, for its own economic and military gain. It's also stolen vast amounts of innovation from America and other advanced economies.

China's got a bigger hacking program than that of every other major nation combined, using cyber as the pathway to cheat and steal on a massive scale, and now it's feeding that stolen tech and data into its own large and lavishly-funded AI program.

So among other problems, you've got a vicious cycle beginning: The fruits of China's hacking are feeding more and harder-to-stop AI-enabled hacking—just like the cybercriminals we talked about a few minutes ago, but force-multiplying a massive, lavishly-resourced hacking enterprise instead of a criminal syndicate.

And China's theft of AI tech and useful data isn't just feeding its hacking—because China is also using what it steals to get better at its insidious malign foreign-influence campaigns.

Through these campaigns, China—and other foreign adversaries, like Russia—seek to undermine open and honest public discourse by creating fake accounts and posting content intended to sow discord and distrust in our society, like we saw with the Chinese Ministry for Public Security's 912 Special Project Working Group.

Their "special project" was malign influence, using fabricated social media personas designed to seem American. We identified the threat, mitigated it, and charged 34 of their officers a few months ago, but stopping that kind of campaign is only going to get harder because generative AI—the technology that generates text, images, audio, and video (including from the GANs we

talked about a minute ago)—large language models, and other tools will enable these actors to reach broader audiences more convincingly, faster, and with less work on their part.

Deepfakes are the most well-known example of this. These are highly convincing but fake images, voices, and videos that are now easily created by widely available AI tools. Years ago, to do that well required enormous investment and talent. Now, almost anyone can do it.

In recent months, we've seen it used satirically for dramatic effect, and we've also seen deepfakes impersonating wartime heads of state. And, just last month, we saw an AI-generated image of an explosion at the Pentagon go viral, causing the stock market to take a hit before anyone realized the image was fake.

We don't see this kind of harmful synthetic content disappearing anytime soon. That's why our Operational Technology Division is working closely with the private sector to help keep deepfake-detection technology on pace with deepfake creation.

*Conclusion*

Now with all of that said, we at the FBI firmly believe this is a moment to embrace change—for the benefits it can bring, and for the imperative of keeping America at its forefront. And frankly, there's no more important partner in our strategy than all of you and your peers throughout the country.

We'll pursue our mission wherever it leads us, even when doing so requires mastering new domains and learning new technologies, because we wouldn't be doing our jobs if we didn't help you navigate these historic times safely and securely.

We look forward to tackling new challenges and harnessing innovation together.  Thank you.

To read more:
https://www.fbi.gov/news/speeches/director-wray-s-remarks-to-the-atlanta-commerce-and-press-clubs

*Number 7*

## High-performing alloy developed to help harness fusion energy

New tungsten-based alloy better withstands fusion energy environments

A newly developed tungsten-based alloy that performs well in extreme environments similar to those in fusion reactor prototypes may help harness fusion energy.

“The new alloy shows promising resistance to irradiation resistance and stability under the high temperatures and extreme irradiation environments used to represent a fusion-reactor environment,” said Osman El Atwani, a staff scientist at Los Alamos National Laboratory.

“The development of this alloy, and the agreement between modeling and experimentation that it represents, points the way toward the development of further useful alloys, an essential step in making fusion power generation more robust, cost-effective, economically predictable and attractive to investors.”

As fusion energy concepts move closer to the real world, solving the materials challenge is imperative. The encouraging results indicate that a design paradigm, as described by El Atwani and his collaborators, and high entropy alloys may be ready to play their role in harnessing the promise of fusion.

El Atwani was the principal investigator for the project, which involved several national and international institutions. Their results were published in May in Nature Communications.

*The fusion materials challenge*

Clean energy production through fusion requires materials that can withstand the harsh conditions — high temperatures, irradiation (exposure to high energy neutron radiation and helium particle fluxes) and stress — associated with fusion reactions that burn hotter than the sun.

El Atwani and his collaborators developed a nanocrystalline high entropy alloy — an alloy made of five or more elements, with a crystalline form at the nanoscale (atomic) level.

Tungsten, a long-studied element of choice for plasma-facing components, is the main element in the alloy.

Unfortunately, current tungsten materials are limited in their viability as plasma-facing components because the material degrades and deforms under fusion conditions.

To develop materials more suitable for fusion, the research team used calculations of thermophysical properties, advanced computational methods, and simulations performed at multiple institutions including Los Alamos, the United Kingdom Atomic Energy Authority, Clemson University and the University of Warsaw.

Ultimately, the element hafnium was chosen for the alloy mix based on performance predicted by the modeling and simulations.

*Fabrication and experimentation*

After fabricating films of the alloy in the Center for Integrated Nanotechnologies at Los Alamos, one version of the material was irradiated at Argonne National Laboratory. Another version was irradiated at the Ion Beam Materials Laboratory at Los Alamos.

Advanced techniques, including in-situ transmission electron microscopy, show that the alloy held up well under these harsh experimental conditions, which replicate a fusion-nuclear-energy prototype.

“The selected compositions of this material system exhibit the best irradiation resistance among all alloys tested at similar conditions and setups,” said Enrique Martinez, a materials scientist with Clemson University.

“Those results align with our modeling, which greatly minimized the set of experiments necessary to assess the material’s performance.”

Such alloys can also be synthesized in amorphous forms, a type of structure where the atoms in materials don’t line up over a long distance, as with crystalline structures.

In related research by a Los Alamos team, the addition of hafnium in amorphous alloys introduced high stability under irradiation and annealing, a heat treatment experienced in fusion settings. That success, led by principal investigator El Atwani and Los Alamos postdoctoral researcher Matheus Tunes, was recently described in Applied Materials Today.

“These projects constitute early-technology readiness level work, and bulk manufacturing of the materials and further experiments are necessary to qualify them as plasma-facing components or structural nuclear fusion

materials," said El Atwani. "However, the overall work we've accomplished with these alloys, with high throughput simulation and experimental outputs, represents a materials design protocol for the future design and assessment of new alloys. These results will help us select materials to advance the technology readiness level."

Paper: "A quinary WTaCrVHf nanocrystalline refractory high-entropy alloy withholding extreme irradiation environments," Nature Communications. https://www.nature.com/articles/s41467-023-38000-y

To read more: https://discover.lanl.gov/news/0613-fusion-energy/

*Number 8*

## Cyber Threat Report: UK Legal Sector

National Cyber Security Centre
a part of GCHQ

The purpose of this report is to help law firms, lawyers and legal practices understand current cyber security threats, and the extent to which the legal sector is being targeted. It then offers practical guidance on how organisations can be resilient to these threats.


Law firms routinely handle highly sensitive client information (for instance relating to ongoing criminal cases, or mergers and acquisitions) that may be valuable to criminal organisations with an interest in exploiting opportunities for insider trading, gaining the upper hand in negotiations and litigation, or subverting the course of justice.

Disruption to routine business operations can be costly to legal practices, both in terms of billable hours lost due to outages and costs to clients that depend upon them, making legal practices particularly of interest to ransomware gangs aiming to extort money in return for restoration of IT services.


In many areas, from mergers and acquisitions to conveyancing, legal practices handle significant funds. The time pressures associated with transactions (as well as the large numbers of suppliers and clients and complex payrolls that law firms handle) create attractive conditions for phishing attacks and business email compromise.

Many legal practices, especially smaller firms, chambers and individual practitioners, rely on an external IT services provider, making it challenging for them to assess for themselves whether the controls they have in place are appropriate to the risk they face. A small law firm with few resources could be devastated if caught up by (for example) a ransomware attack. They are more vulnerable to attack, perhaps via unpatched vulnerabilities on unmanaged devices, or due to untrained staff or poorly offboarded leavers. Once attacked, a relatively small financial or reputational loss may be disastrous.

Reputation is critical to the business of law, which makes legal practices attractive targets for extortion.

As the report explains, the cyber threat applies to law practices of all sizes and types of work, from sole practitioners, high street and mid-size firms to barristers' chambers, in-house legal departments and international corporate firms. Cyber criminals are not fussy about who they attack, which means small and large organisations are at risk.

The report has been compiled with the assistance of the NCSC's in-house cyber security experts, the NCSC-sponsored Industry 100 scheme, the Law Society, The Bar Council, the Solicitors Regulation Authority (SRA), Action Fraud (the UK's national fraud and cyber crime reporting centre) and the National Crime Agency (NCA).

It has also drawn on an extensive body of open source reporting. The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's technical authority for cyber security. Since the NCSC was created in 2016, as part of the Government's National Cyber Security Strategy, it has worked to make the UK the safest place to live and work online.


4 Foreword

6 The legal sector

7 Why is the legal sector a particular target?

8 How things have changed since 2018

9 Who might target the legal sector?

11 The main types of cyber attack

17 Reporting cyber attacks

18 How to improve your cyber security

20 Cyber security guidance

21 NCSC schemes and services


*The legal sector*

The UK's legal sector is large and diverse, spanning organisations of many shapes and sizes, from small high street solicitors' firms to large multinational corporations, to self-employed barristers and barristers' chambers.

Legal services form an important component of the UK economy. As of early 2023, there were over 32,900 enterprises in total including barristers, solicitors and other legal service providers operating in the UK, with an estimated total revenue of £43.9 billion.

More than 320,000 people work in the legal sector in the UK. Legal services are an important export of the UK accounting for £6.8 billion of exports as of 2021.

There is an inherent trust and strict confidence from clients that law firms preserve the confidentiality of their information.

It is also a legal practice's overriding professional obligation, as set out in the professional standards, in the SRA's Standards and Regulations, the Bar

Standards Board's handbook, and is common law, under the Legal Services Act 2007.

It is essential that organisations maintain appropriate cyber security measures. Failure to do so can have exceptionally negative consequences for a legal practice and its clients.

The 2022 PriceWaterhouseCoopers Annual Law Firms Survey reported that cyber risk has seen significant increases in spending among larger law firms, with the top 100 spending an average of 0.46% of fee income on cyber security in 2022.


**We strongly recommend that all legal firms:**

Ensure that senior leadership such as board members, owners and partners are engaged and informed about cyber security risk. The NCSC's Cyber Security Toolkit for Boards[1], provides a set of tailored resources to help senior stakeholders engage with these issues.

Assess your organisation against NCSC's Cyber Essentials[2]. This helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security.

Sign up to the NCSC's key services that are available to help protect your organisation from a cyber attack. Services include Early Warning[3], Exercise in a Box[4] and Connect Information Share Protect (CISP)[5]. You may wish to consider Cyber Insurance[6], although this will not instantly solve all of your cyber security issues, nor will it prevent a cyber breach/attack.

Invest in staff training and awareness to improve the security culture in your organisation (see next page).

To read more:
https://www.ncsc.gov.uk/files/Cyber-Threat-Report_UK-Legal-Sector.pdf

*Number 9*

# The Ethics of Artificial Intelligence
# Pioneering a New National Security

GCHQ


4 Foreword by Director GCHQ

5 Executive Summary

6 Key Insights

8 Chapter 1: Introduction

10 Chapter 2: What is Artificial Intelligence?
- 11 AI fact and fiction
- 11 Origins
- 11 What is machine learning?
- 12 Different types of machine learning
- 13 What AI can and cannot do

14 AI For National Security: Cyber Threat

16 Chapter 3: What does GCHQ do?
- 17 Our mission
- 18 Our oversight
- 19 Our challenges and opportunities

20 AI For National Security: Online Safety

22 Chapter 4: Artificial Intelligence in GCHQ
- 23 The invention of AI
- 23 Post-war technology and computing
- 23 The winter years
- 23 Our approach to delivering AI

24 AI For National Security: Trafficking

26 Chapter 5: GCHQ, AI and trust
- 27 International and national context
- 27 What is AI ethics?
- 27 AI ethics and National Security
- 28 The major ethical challenges
- 31 Our approach – next steps

34 AI For National Security: Foreign State Disinformation

36 Chapter 6: Conclusions and our future journey

38 Footnotes / Citations


## Executive Summary

Britain today is a digital nation, leading and shaping events across a world inextricably linked through cyberspace. Now and into the future, the value of our economy, our way of life, and our global influence will be built on our advanced digital infrastructure, capabilities and knowledge.

Artificial Intelligence – a form of software that can learn to solve problems at a scale and speed impossible for humans – is increasingly essential to the way we live. It is already transforming sectors as diverse as healthcare, telecommunications, and manufacturing.

AI software informs our satnavs, guides our internet searches, and protects us every time we make an electronic purchase, or open an app on our smartphone.

In the century since it was founded, GCHQ has been at the forefront of innovation in national security. Generations of brilliant analysts, with their diverse mix of minds, have used their technical ingenuity, cuttingedge technology and wide-ranging partnerships to identify, analyse and disrupt threats to our nation.

Today, as technological change continues to accelerate, we are pioneering new approaches to understanding the complex and interconnected world around us.

We have long championed the responsible use of data science, and believe that AI will be at the heart of our organisation's future.

Thinking about AI encourages us to think about ourselves, and what it means to be human: our preferred way of life, our guiding values and our common beliefs.

The field of AI ethics has emerged over the last decade to help organisations turn these ethical principles into practical guidance for software developers – helping to embed our core values within our computers and software.

We won't pretend that there are not challenges ahead of us. In using AI we will strive to minimise and where possible eliminate biases, whether around gender, race, class or religion.

We know that individuals pioneering this technology are shaped by their own personal experiences and backgrounds. Acknowledging this is only the first step – we must go further and draw on a diverse mix of minds to develop, apply and govern our use of AI.

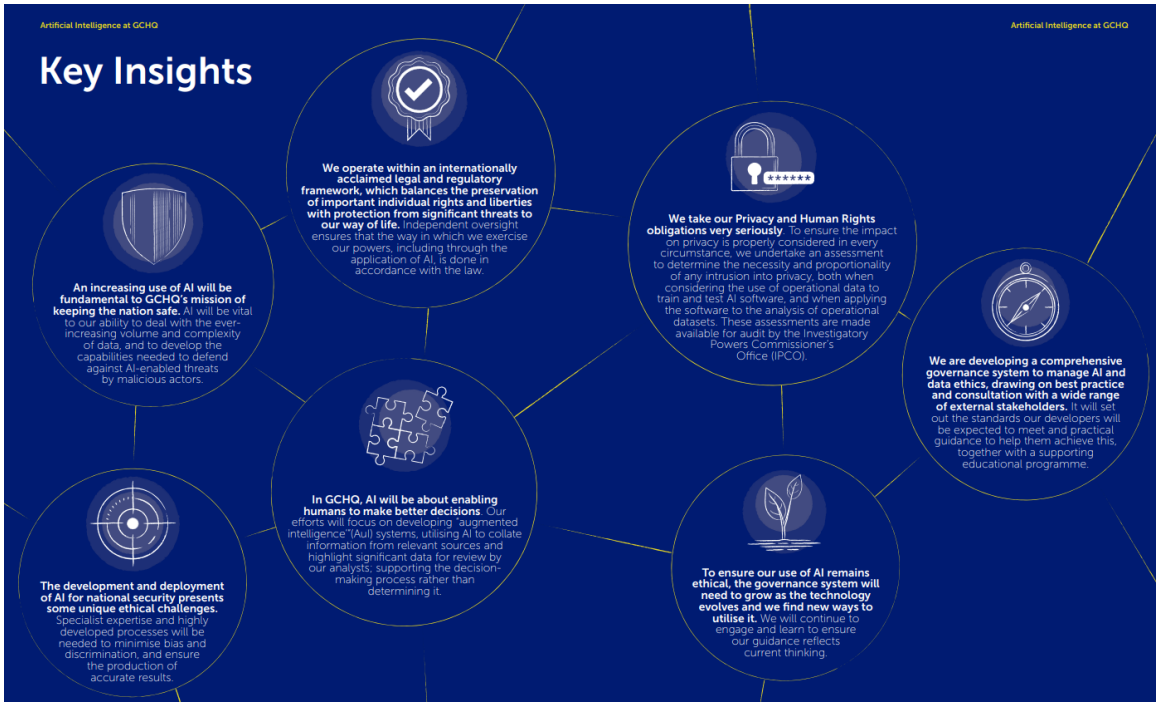
Left unmanaged, our use of AI incorporates and reflects the beliefs and assumptions of its creators – AI systems are no better or no worse than the human beings that create them.

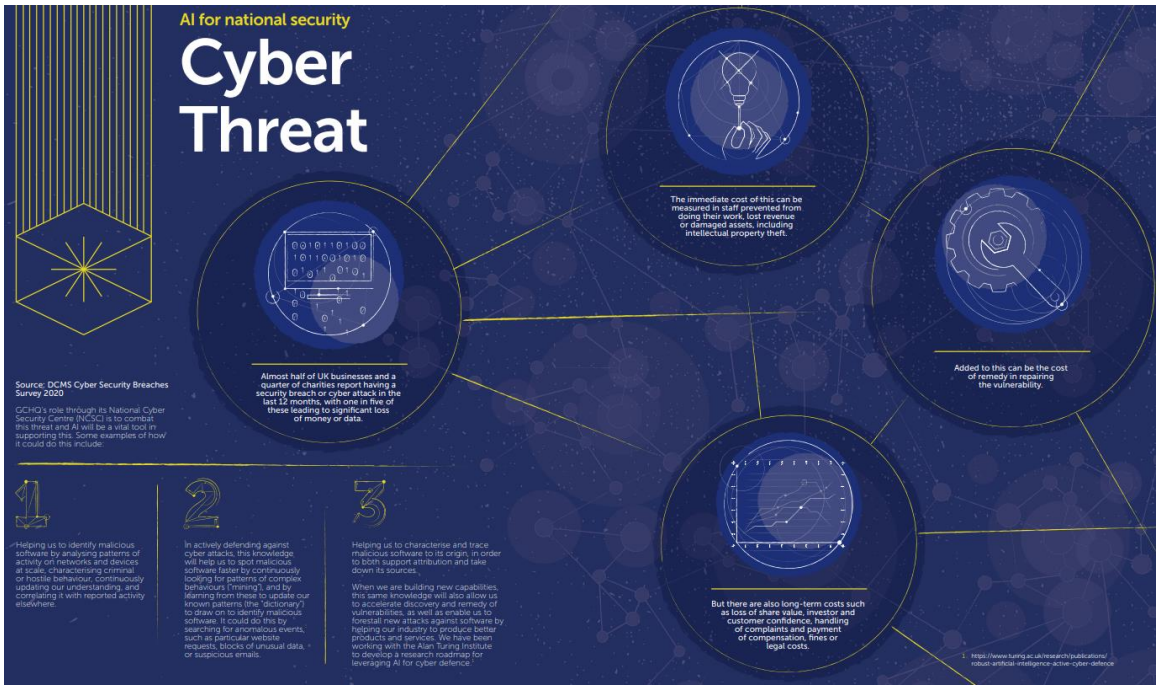
Our society is learning and growing: the Alan Turing Institute and similar bodies are helping to show us how we might build and use AI in a more ethical, responsible manner.

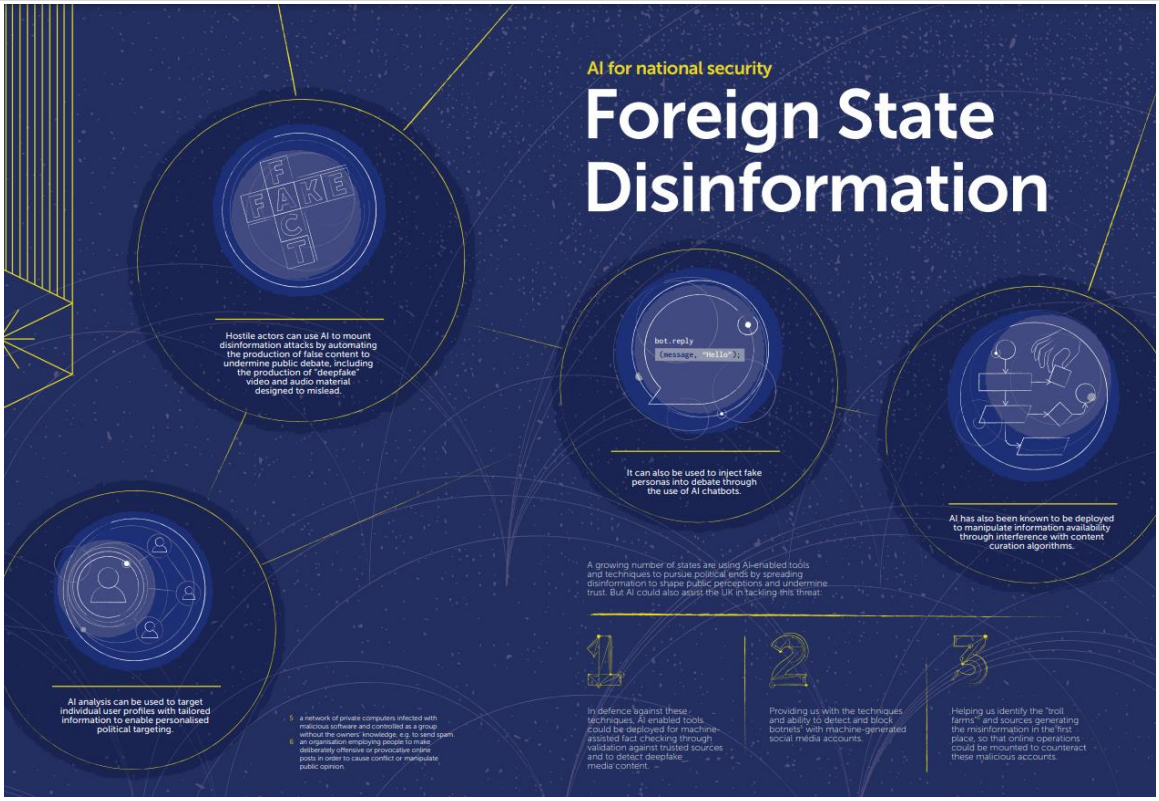
GCHQ is committed to creating and using AI in a way that supports fairness, empowerment, transparency and accountability – and to protecting the nation from AI-enabled security threats pursued by our adversaries. We believe that, by working together with our partners across Britain and beyond, we can deliver this vision.

This paper describes the digital Britain of today, and our values-led approach for the spaces where people, information and technology meet. It lays out GCHQ's AI and Data Ethics Framework, and how we intend to use AI in our operations.

It forms part of our commitment to inclusion, debate and openness. The paper is the first step of a much longer journey: we'd like you to join us on it.






To read more: https://www.gchq.gov.uk/files/GCHQAIPaper.pdf

*Number 10*

## Homeland Security Acquisition Regulation - Safeguarding of Controlled Unclassified Information

FEDERAL REGISTER
The Daily Journal of the United States Government

The Department of Homeland Security (DHS) is issuing a final rule to amend the Homeland Security Acquisition Regulation (HSAR) to modify a subpart, remove an existing clause and reserve the clause number, update an existing clause, and add two new contract clauses to address requirements for the safeguarding of Controlled Unclassified Information (CUI).

This final rule implements security and privacy measures to safeguard CUI and facilitate improved incident reporting to DHS. These measures are necessary because of the urgent need to protect CUI and respond appropriately when DHS contractors experience incidents with DHS information.

DATES: This final rule is effective July 21, 2023.

The final rule will apply to DHS contractors that require access to CUI, collect or maintain CUI on behalf of the Government, or operate Federal information systems, which include contractor information systems operating on behalf of the agency, that collect, process, store, or transmit CUI.

DHS estimates the final rule will have an annualized cost that ranges from $15.32 million to $17.28 million at a discount rate of 7 percent and a total 10-year cost that ranges from $107.62 million to $121.37 million at a discount rate of 7 percent.

The primary contributors to these costs are the independent assessment requirement and reporting and recordkeeping requirements.

There are additional small, quantified costs from rule familiarization and security review processes.

DHS was unable to quantify costs associated with incident reporting requirements, PII and SPII notification requirements, credit monitoring requirements and they are therefore discussed qualitatively.

DHS was unable to quantify the cost savings or benefits associated with the rule. However, the final rule is expected to produce cost savings by reducing

the time required to grant an ATO, reducing DHS time reviewing and reissuing proposals because contractors are better qualified, and reducing the time to identify a data breach.

The final rule also produces benefits by better notifying the public when their data are compromised, requiring the provision of credit monitoring services so that the public can better monitor and avoid costly consequences of data breaches, and reducing the severity of incidents through timely incident reporting.

To read more:
https://www.federalregister.gov/documents/2023/06/21/2023-11270/homeland-security-acquisition-regulation-safeguarding-of-controlled-unclassified-information

https://www.govinfo.gov/content/pkg/FR-2023-06-21/pdf/2023-11270.pdf

## Disclaimer

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

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

This information:

- is of a general nature only and is not intended to address the specific circumstances of any 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,

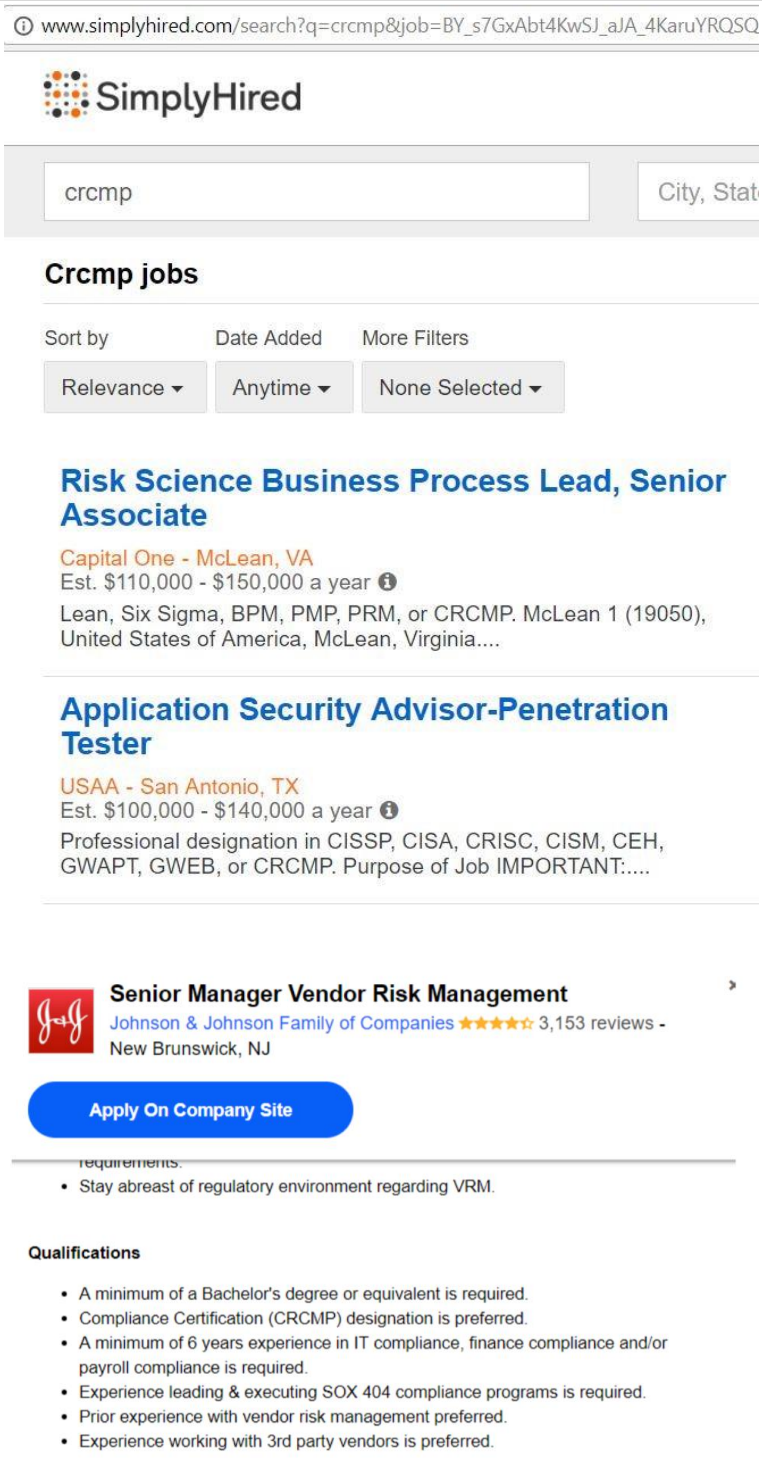
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.