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

Monday, December 5, 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,

Cicero believed that glory follows virtue as if it were its *shadow*.

At the 2018 Plenary Meeting in Ottawa, the Financial Stability Board (FSB) decided to *replace* the term *"shadow banking"* with the term "Non-Bank Financial Intermediation (NBFI)".

Previously, the FSB defined shadow banking as "credit intermediation involving entities and activities (fully or partly) outside the regular banking system".

Banks and their affiliated broker-dealers are always a vital component of the financial system, but they are now part of a larger *mosaic of institutions* that route the flow of funds and facilitate trading. Especially important, from a financial stability perspective, has been the greater involvement of non-bank financial intermediaries.

The NBFI landscape is vast and varied, covering a diverse set of players with a number of business models and subject to different regulatory regimes.

Today we can read the latest newsletter from the BIS "on bank exposures to non-bank financial intermediaries". According to the newsletter, the collapse of Archegos Capital Management highlighted deficiencies in some *banks' risk management* practices.

Those deficiencies include:

- insufficient governance and risk management frameworks, including risk monitoring and stress testing in relation to the business strategy;

- inadequate collection of information on clients' positions and exposures as part of due diligence, and limited efforts to understand and assess clients' investing strategies;

- the absence of comprehensive limit frameworks;

- weak margining practices, including the use of "static" margining and inadequately calibrated margining by some banks; and

- possible regulatory arbitrage behaviour regarding the leverage ratio requirement.

Read more at number 4 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 6 (Page 27)

EIOPA consults on cyber component in its insurance stress testing framework

Number 7 (Page 30)

Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests

Number 8 (Page 33)

Securing tomorrow today: Why Google now protects its internal communications from quantum threats

Number 9 (Page 35)

Court Authorizes the Seizure of Domains Used in Furtherance of a Cryptocurrency "Pig Butchering" Scheme

Number 10 (Page 37)

Cranking the Power on Radar Capabilities

DARPA looks to build on previous success in radio frequency power output with new transistor-focused THREADS program

Number 1

That was the year that was

Sir David Ramsden, Deputy Governor for Markets, Banking and Resolution of the Bank of England, at the Bank of England Watchers' Conference, organised by the Money Macro Finance Society and King's Business School at King's College, London.

Thank you for the invitation to speak today. I am particularly pleased that I have close links with the two institutions, the Money Macro and Finance Society and Kings College London, who have organised this first Bank-watchers' conference.

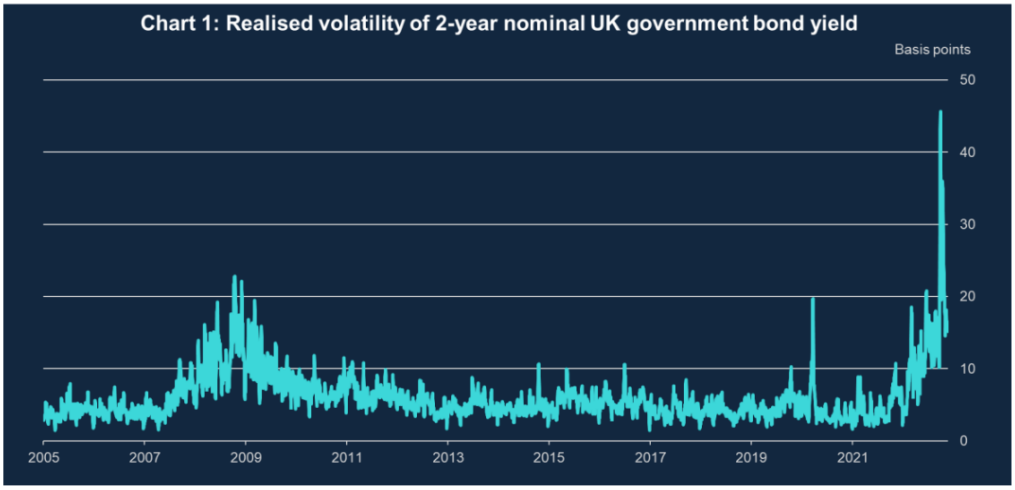
In the spirit of the sixty year old TV programme that inspired my title I want to give my personal review of why the economy, and in particular inflation, turned out to be very different over the past year, and suggest some potential consequences for the MPC's approach to forecasting the economy and setting policy to hit the 2% inflation target.

As a member of the MPC I hope to be able to do justice to how our thinking has evolved but I should stress at the outset that these are personal observations, which will nevertheless hopefully help set the scene for discussions at this conference.

In my other monetary policy speeches this year I've focused on the impact of shocks. Today I'm going to look more through the lens of the uncertainty generated by those shocks, which has made the course of the economy in general and inflation in particular increasingly hard to predict *.

Uncertainty has come not just from new shocks hitting the economy, most notably huge increases in energy prices, but also from unexpected developments, particularly in the labour market, as well as from other sources, like the on-going impact of Brexit and the pandemic. Economic uncertainty can be illustrated in various ways.

Chart 1 shows a market-based measure of volatility two years ahead, the horizon for monetary policy, which has been on a sustained and steeply rising trend over the last year, and spiked very recently at a much higher level even than during the global financial crisis.



Source: Bloomberg L.P., Tradeweb and Bank calculations

Notes: Realised volatility is a 5-day moving average of the difference between the highest and lowest 2-year nominal UK government bond yield within a day.

Without wishing to downplay the audience today, the Bank-watchers who matter most for whether the MPC meets its target of getting inflation back to 2% are households and businesses.

Uncertainty is impacting directly on them, undermining their confidence to make decisions and plan ahead, adding to what is already a very challenging economic situation in the face of the cost of living crisis and tightening financial conditions.

I want to frame my observations by going back twelve months. At that point the economy was recovering from the worst of the Covid pandemic and CPI inflation had started to rise.

Market expectations showed a 50:50 chance that Bank rate would be increased from 0.1% to 0.25% at the upcoming December 2021 MPC meeting.

* (In economics, the concepts of 'risk' and 'uncertainty' are usually distinguished using the terminology of Frank Knight (1921).

Risk refers to cases where we know the potential outcomes and the probability of them happening.

Uncertainty refers to cases where we don't know the possible outcomes (or their probabilities) in advance.

Another broad approach has been suggested by Kay and King (2020) in their book on 'radical uncertainty'.

They argue that successful decision-making under such uncertainty relies on collaborative processes, judgement, close attention to reliable data, and the use of narrative, rather than an overreliance on economic models).

To read more:
https://www.bankofengland.co.uk/speech/2022/november/dave-ramsden-keynote-speech-at-boe-watchers-conference

Number 2

The Deutsche Bundesbank publishes its 2022 Financial Stability Review

The macro-financial environment has deteriorated substantially over the course of 2022. It has been shaped by subdued growth prospects, high inflation as well as rising interest rates and risk premia.

Banks, insurers and investment funds have already recorded losses as a result of market corrections.

The sharply higher and extremely volatile stock market prices for energy products have sharply increased the collateral requirements of central counterparties in derivatives trading.

That said, government measures have been able to cushion liquidity shortages at enterprises in the energy sector. Overall, however, the supply of credit to the economy has worked well to date.

Major downside risks remain which require sufficient resilience. A worsening energy crisis, a sharp economic slump and abruptly rising market interest rates could put the German financial system under considerable pressure.

Rising costs are limiting the financial leeway of households and enterprises. Future credit risks are increasing as a result.

“To ensure that potential stress is not amplified via the financial system, financial institutions must be sufficiently resilient on their own,” said Claudia Buch, Vice-President of the Deutsche Bundesbank, at the presentation of the 2022 Financial Stability Review.

German financial system vulnerable to adverse developments

Vulnerabilities in the stock of loans have built up in the German financial system over a period of several years. Low interest rates as well as strong growth in loans and asset prices have contributed to this.

Insolvencies in the corporate sector and thus credit risk have declined in recent years. Banks still consider their credit risk to be fairly low. However, many of the assumptions made in the past when granting loans are likely to prove to be overly optimistic.

Macroeconomic risks require sufficient resilience of the financial system

The report highlights the need for sufficient resilience in the financial system in view of the existing macrofinancial risks. Not only supervisors but also financial market actors have a part to play.

“Financial institutions should assess the impact of adverse scenarios. Given the high uncertainty, they should engage in prudent risk provisioning and exercise caution when distributing profits,” emphasised Joachim Wuermeling, the Bundesbank Executive Board member responsible for banking supervision.

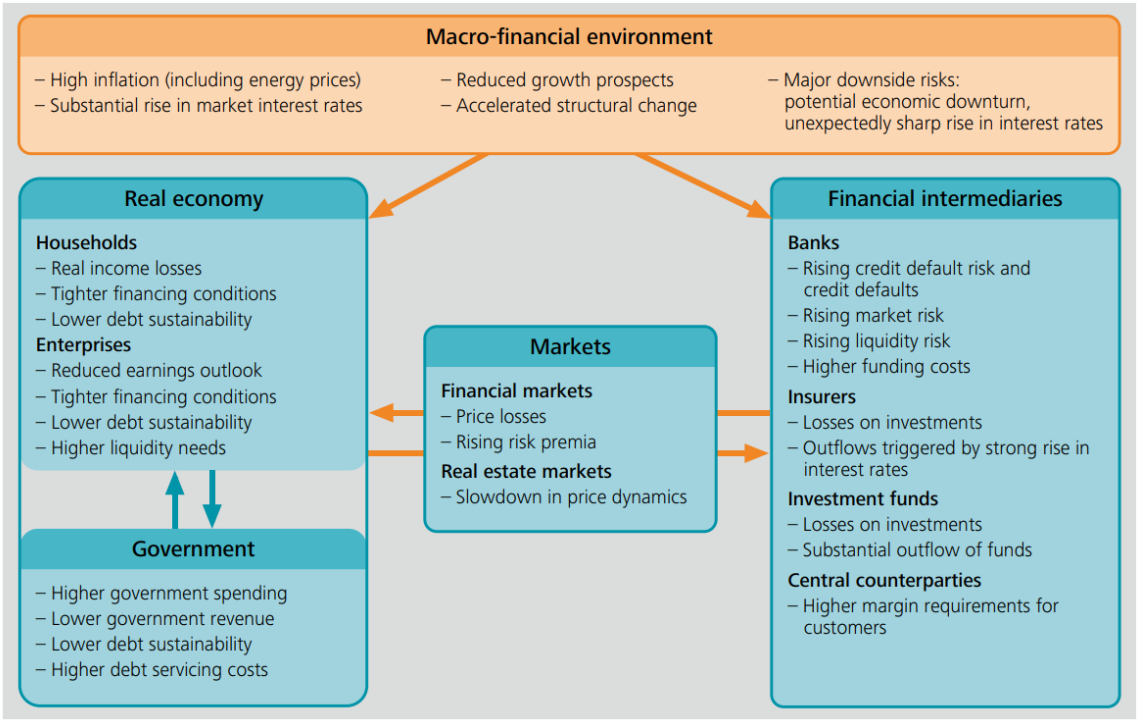
The Federal Financial Supervisory Authority (BaFin) announced a package of macroprudential measures aimed at strengthening the resilience of the financial system at the beginning of 2022.

The countercyclical capital buffer was raised and a sectoral systemic risk buffer was introduced. If necessary, BaFin can release the macroprudential buffers, but at the current juncture there is no need to do so.

“Macroprudential policy is not economic policy,” noted Vice-President Buch. A release would be appropriate, in particular, if substantial losses occur in the financial system or if they are clearly indicated and there is therefore a risk that the banking system will excessively restrict lending. Sufficient resilience is also important given the pressure for structural change in the German economy, which has intensified as a result of geopolitical factors and the climate crisis.

The Review includes two special chapters. One chapter describes the stabilising role of central clearing in derivatives trading. The second examines the relevance of commercial real estate to the financial system, also in light of commercial real estate’s global interconnectedness.

To read more:
https://www.bundesbank.de/en/press/press-releases/the-deutsche-bundesbank-publishes-its-2022-financial-stability-review-900616



Deutsche Bundesbank

Number 3

Breaking new ground - regulating for emerging risks

Derville Rowland, Deputy Governor of the Central Bank of Ireland, at the Annual Irish Funds UK Symposium, London

Good morning everyone. It is a pleasure to be with you in person at the ninth annual Irish Funds' UK symposium.

I want to begin by acknowledging Irish Funds' logistical feat in rescheduling the conference at short notice for the benefit of attendees – which cannot have been easy.

But I'm glad to say the timing is fortuitous – for it enables me to give an important update on the Central Bank of Ireland's macroprudential policy for the non-bank sector, which we are announcing this morning.

I'll begin, however, by saying a little about the Central Bank's strategy and regulatory philosophy, and our views on the concept of open strategic autonomy.

I'll also cover a number of other specific areas of interest, including sustainable finance, delegation and digital assets.

The common thread between all these topics is the breaking of complex new ground – for regulators and industry alike.

So I will talk to some of the challenges I see ahead and how the Central Bank of Ireland, together with our counterparts at European and international level, as well as industry, need to work together to tackle them.

Introduction

In his latest work, the scientist and academic Vaclav Smil asks why most people in modern societies have, in his words, "such a superficial knowledge" about how the world really works.

He suggests the complexities of the modern world are an obvious explanation: “People are constantly interacting with black boxes, whose relatively simple outputs require little or no comprehension of what is taking place inside the box.”

This, he says, is as true of physical items such as mobile phones and laptops to mass-scale procedures such as vaccination.

As Smil points out, general terms such as “physics” and “biology” are less meaningful in a world of increasingly specialised subject-matter expertise – what he calls the “atomisation of knowledge”.

I see significant parallels with the global financial sector. No longer can one person truly be an expert in its complexities. And such complexities, and the interdependencies they create, pose a real challenge – both in terms of managing and regulating risk.

As 2008 showed all too painfully, this is a critical challenge for regulators – not just to identify the black boxes in the first place but to look into and understand them. In the non-bank sector particularly, where work continues on issues such as channels of propagation and contagion for example, this is very much work in progress.

At the same time, regulation’s purpose is to safeguard stability and protect consumers and investors. It is not to stifle innovation or eliminate the right of an informed individual or firm to take a certain amount of risk.

In the Central Bank, therefore, we are focused on creating the regulatory context in which the potential benefits of innovation for consumers, investors, businesses and society can be realised, while the risks are effectively managed.

As our Governor recently noted, we believe regulation must be forward-looking, connected, proportionate, predictable, transparent and agile. And we work at home and abroad on that basis.

Open Strategic Autonomy

In that context, for the Central Bank and indeed, Ireland as a whole, the UK remains an important partner and interlocutor.

We have a long established and historic relationship with significant interlinkages and dependencies between our economies and financial sectors.

The recent turmoil in the UK pension sector, and the impact on GBP liability-driven investment (LDI) funds, was a clear example of these complex interlinkages.

Investment funds authorised by the Central Bank of Ireland have aggregate holdings in UK gilts of approximately stg£267bn, representing approximately 6% of total assets under management.

Of that stg£267bn, LDI funds represent the largest sub-component of UK gilt holdings by Irish domiciled funds.

Throughout this period, and in conjunction with other relevant NCAs, we engaged proactively with the managers of LDI funds to ensure they took the appropriate actions to strengthen their ability to absorb shocks.

The resilience of GBP LDI funds across Europe has subsequently improved.

But given the current market outlook, we do expect that levels of resilience and the reduced risk profile of GBP LDI funds should now be maintained, and do not consider any reduction in the resilience at individual sub-fund level to be warranted at this point.

This episode, and the effective interaction across the various NCAs, has emphasised again the importance of continuing to ensure a coordinated and effective response to market developments - particularly those with a cross-border dimension.

In the EU, attention is focused on the concept of “Open Strategic Autonomy” - to strengthen the EU’s resilience, while seeking to ensure it remains open to the world.

Here in the UK, the focus has turned to the development of domestic regulations, and with that comes the potential of moving away from established and agreed EU frameworks.

This dynamic brings new challenges, particularly that of divergence, where a lack of consistency in approaches risks undermining the collective effectiveness of regulatory frameworks, especially in the context of capital markets, given their global nature.

From a regulatory perspective, I believe it is important for the EU and UK to continue working closely together to ensure – to the maximum extent possible - the consistent and stable application of our frameworks.

As the challenges of the last few years have shown, strengthening our alliances with like-minded partners is more important than ever and makes the work of bodies such as the Financial Stability Board and IOSCO vital to support that cooperation and to build common approaches to collective challenges.

Macroprudential policy – an overview:

Which brings me to macroprudential policy. The events of 2008 led to a significant overhaul of financial regulation, especially for banking and certain markets activities to improve resilience and reduce systemic risk in a way that benefitted investor protection.

Since that time, as banks retreated from certain areas of activity, the non-bank sector has moved in to fill the gaps. We can see examples of this in practice - whether in business lending through loan-originating funds or the significant growth in money market funds as cash management vehicles.

The non-bank sector brings many benefits. It diversifies the channels of finance available to the real economy and it allows for a broader diversification of borrower risk that has benefits for financial stability.

As the sector continues to grow, so too does its systemic importance. In the context of investment funds specifically, systemic risks arise from the interplay between vulnerabilities (for example, liquidity mismatch and the use of leverage) and interconnectedness across the sector.

Changing dynamics in the supply and demand of market liquidity, combined with the use of leverage and the larger size of the sector, mean that market shocks can be amplified and transmitted to a greater and more rapid extent than previously has been the case.

The financial system in Ireland is heavily weighted towards the non-bank sector, including investment and money market funds. We have the third largest funds sector in the world.

As many in this room will know, by the end of 2021, there were nearly 10,000 such entities, up from about 6,000 in 2016. In the same period, asset values of these entities increased from approximately €3 trillion to €5.6 trillion.

Given the size of the non-bank sector in Ireland and the particular linkages of certain sub-sectors with the domestic economy, macroprudential policy for non-banks is a priority for the Central Bank. For open ended funds, the

Financial Stability Board recently published proposals to revise some of its 2017 recommendations on potential structural vulnerabilities in the asset management sector as they relate to liquidity management tools.

The Central Bank of Ireland co-chaired the group that produced those proposals and we look forward to continuing to engage with our international counterparts to implement them.

As the financial system and our economies adjust to higher interest rates and the end of a prolonged period of quantitative easing, it is imperative that we re-double our efforts globally to develop and operationalise the macroprudential framework for non-banks, especially investment funds.

Property fund measures:

The necessity to take action applies domestically, as well as internationally.

Today, the Central Bank of Ireland is announcing its first macroprudential policy measures for non-banks - targeting Irish property funds.

We are activating a macroprudential leverage limit and introducing Guidance for enhanced liquidity management at Irish-domiciled funds investing in Irish property. We are using European regulations for the leverage limit and we are the first national competent authority to take this approach for macroprudential purposes.

The commercial real estate (CRE) sector is systemically important for Ireland. Irish authorised funds investing in Irish property have become a key participant in that market, holding approximately 35% of investable CRE. This growing form of financial intermediation entails benefits for Irish macroeconomic and financial stability.

Often established and funded by overseas investors, property funds provide an alternative channel of financing for investment in the CRE market, reducing reliance on domestic sources of capital.

However, the changing nature of financial intermediation also raises the potential that new vulnerabilities could emerge, so it is important that we adapt the macroprudential framework accordingly – and in line our aforementioned regulatory principles of being forward-looking, connected, proportionate, predictable, transparent and agile.

These measure we are announcing today are designed to build the resilience of this growing form of financing to shocks.

Central Bank analysis has identified excessive leverage and liquidity mismatch as potential sources of vulnerability in Irish property funds. Following extensive engagement, consultation and analysis, we are now introducing measures to address these vulnerabilities.

For the leverage limit, we are introducing a sixty per cent limit on the ratio of property funds' total debt to total assets. We recognise that existing property funds will need time to adjust. As such, a five-year implementation period is being provided to allow for the gradual and orderly adjustment of leverage for this cohort.

The duration of the implementation period is also reflective of the current macro-economic environment of rising interest rates and a slowdown in global and Irish economic growth. For new funds, from today onwards, we will only authorise new Irish property funds which meet the sixty per cent leverage limit.

As I said, the leverage limit is implemented using European regulations. As part of our decision-making process, we notified the European Securities and Markets Authority (ESMA) of our intention to introduce the measures. ESMA's formal advice to the Central Bank is that the leverage limit is appropriate to address the concerns relating to the stability and integrity of the financial system.

We are issuing Guidance on the minimum liquidity timeframes expected for property funds. We expect that property funds should generally provide for a minimum liquidity timeframe of at least 12 months taking into account the nature of the assets held.

We are providing an 18-month implementation period for existing funds to take appropriate actions in response to the Guidance, and we expect that property funds newly authorised from today onwards will adhere to the Guidance from inception.

Due to their reduced systemic risk, funds primarily investing in social housing will not be covered by the leverage limit, subject to certain criteria. And we will allow a methodological adjustment for development assets to avoid an excessively tight application of the leverage limit for such activities.

These measures aim to guard against the potential risk that financial vulnerabilities in the property fund sector lead to forced selling behaviour in times of stress. They aim to build the resilience of this growing form of financial intermediation, so that property funds are better able to absorb – rather than amplify – future adverse shocks.

In turn, this will better equip the sector to continue to serve as a sustainable source of financial intermediation.

These are our first macroprudential policy tools for nonbanks. As I mentioned, the Central Bank of Ireland sees this as a priority area, and we are working with international counterparts to develop and implement a macroprudential policy framework for the sector more broadly.

Delegation

Delegation is another area of particular focus – for us and in Europe. Whilst the proposals are still to be finalised, the AIFMD review is likely to bring targeted changes to the current regime to enhance the reporting of delegation activity, particularly to third countries, and ESMA is positioned to conduct an in-depth review of delegation in the funds sector.

Ireland has robust requirements in place to protect against letterbox entities and to ensure effective oversight of delegates by fund management companies. We continue to develop and refine our domestic rules to ensure they reflect not only EU level requirements, but that firms also meet our expectations in terms of their substantive structures, activities and risk profile in Ireland.

The proposals contained in the AIFMD Review mark the start of a longer-term process that will take a deeper and more comprehensive look into delegation in Europe. It can be expected that, after a period of evaluation and reflection, further work in this area may be proposed.

I know industry will be actively engaged at both national and European level on this issue.

Your views will be vital to forming a balanced and objective approach to delegation in the future.

ESG

Turning to Environmental, Social and Governance (ESG) investment, the Central Bank is committed to supporting the growth of this segment in Ireland and enabling the significant investment in sustainable projects needed to support the transition to carbon neutrality.

We have been actively engaging with industry in order to give as much clarity around our expectations as possible.

Along with our fellow regulators, we have a number of priorities in this regard.

Firstly, we are concerned about the risks to regulated firms' sound functioning, and more broadly to financial stability, arising from increasingly frequent climate events or from the potential impact on investments as a result of the broader transition to a more sustainable economy that may have significant implications for firms.

Secondly, we want to ensure that investors are fully informed and not misled. Where investments or financial products are described as green or sustainable, this must be meaningful and accurate and based on reliable parameters that are consistently applied across Europe.

Investors have high expectations for the funds sector with regard to sustainable finance. It is critical that the sector is positioned to support a timely and effective transition to a more sustainable economy. Standards must be high.

From 1 January 2023, additional requirements under the EU SFDR Level 2 disclosure obligations will apply. The Central Bank considers these new obligations to be instrumental in terms of the level of information available to investors about the products in which they invest.

The new requirements will mean that Irish investment funds must make extensive updates to their fund documentation and provide more in-depth sustainability disclosure amendments to their pre-contractual documents.

The tolerance for any disclosures that do not meet the requirements will be low considering the length of time industry has now had to comply with these key regulatory changes.

In order assist industry, the Central Bank has recently published an information note in this area.

The note is designed to inform and assist industry in ensuring that investors and the market can have a high degree of trust and confidence in green and sustainable products produced and sold from the jurisdiction.

Digital Assets

The final topic I which to touch on is digital assets where, as events of the last year have shown, there are many black boxes and clearly not all of them are fully understood.

The collapse of FTX, following as it did the collapse of other crypto entities and the general turmoil we have seen across the sector this year, has reignited questions as to whether this is a sector that should – or should not – be regulated.

We have a rapidly growing sector that is increasingly intertwined with the "traditional" or mainstream financial sector; that is highly volatile and susceptible to fraud; and that has relatively high failure rates.

This asset class has done real harm to retail investors in the last year. The digital assets ecosystem is not a suitable or safe space for retail investors – something about which the Central Bank has been warning for some time.

Against that, there is still substantial demand for digital assets – which go wider than "crypto" alone – and in particular from professional investors. But the digital assets sector lacks the rules and protections that have benefited the development of the mainstream financial sector.

While European frameworks – namely MiCA and DORA - will bring important improvements, they do not present a complete set of answers to the many difficult issues within this space.

The FSB and IOSCO have set out the view that firms presenting the same or similar risks should be subject to similar regulation, a cornerstone of their efforts to develop international regulatory frameworks in digital assets and decentralised finance.

We need to start speaking the same language and building a similar view of issues whether it is around financial resilience, better management of conflicts of interest, or greater transparency and security for customers.

Conclusion

To finish where I started, Smil posits that a realistic grasp of our past, present and uncertain future is the "best foundation" for approaching the unknowable expanse of time ahead of us. We cannot be specific but know it will include both progress and setbacks.

"The future, as ever, is not predetermined," he writes. "Its outcome depends on our actions."

As a regulator, when thinking about the complexity of new terrain and its many challenges, that call to action chimes greatly with me.

In concluding, let me emphasise that, in the Central Bank of Ireland, as we cover new ground, we do not move in isolation or with our peer regulators only.

We are an open and engaged regulator, knowing the importance of listening to our stakeholders, building dialogue and being open to feedback.

We don't just welcome your continued engagement – we see it as essential to our mission of serving the public interest by maintaining monetary and financial stability while ensuring that the financial system operates in the best interests of consumers, investors and the wider economy.

Thank you for your attention and I wish you an enjoyable and productive conference.

To read more:
https://www.centralbank.ie/news/article/breaking-new-ground-regulating-for-emerging-risks-speech-by-derville-rowland-deputy-governor-consumer-and-investor-protection-at-the-annual-irish-funds-uk-symposium

Number 4

Bank exposures to non-bank financial intermediaries

BIS

1. The non-bank financial intermediary (NBFI) sector continues to grow and has the potential to cause financial stability concerns, though its size and the associated risks vary amongst member jurisdictions.

2. Recent episodes of distress highlighted vulnerabilities and deficiencies in some banks' risk management practices related to NBFIs. Supervisors consider exposures to highly leveraged counterparties via derivatives and securities financing to be the riskiest. Supervisors are observing similar deficiencies in some banks' management of commodity-related counterparties.

3. Supervisors will continue to monitor exposures, focus on the proper application of existing standards and guidance, and assess the level of observable data to improve the visibility of interconnections between banks and NBFIs.

The NBFI sector continues to gain relevance and increasingly provides credit intermediation and funding services to the real economy. This results in both direct and indirect interconnections between banks and NBFIs through multiple channels.

The Committee is concerned about the growth of these exposures, given the often opaque and quickly evolving nature of the attendant risks. Recent episodes of NBFI distress, including the collapse of Archegos Capital Management and events leading to stresses in government bond markets (eg liability-driven investment strategies), have highlighted vulnerabilities and deficiencies in banks' risk management practices.

The Committee recently conducted a risk horizon scanning exercise related to banks' NBFI activities and discussed supervisory and policy implications resulting from the recent distress of specific NBFIs. These discussions highlighted the following:

1. While the types of NBFIs and the size of banks' exposures to NBFIs vary across jurisdictions, these exposures are growing in size and have the potential to cause further financial stability concerns.

2. Banks engage with NBFIs across a wide range of transactions. Common NBFI counterparties for banks are investment and pension funds as well as insurance companies and broker-dealers. Banks' exposures to NBFIs

include traditional credit facilities such as credit lines and fully collateralised short-term wholesale loans. Banks are also exposed to NBFI counterparties through more complex instruments in the areas of derivatives and securities financing, leveraged lending and prime brokerage, which may give rise to counterparty credit and liquidity risks with concentration, illiquidity and leverage as key considerations.

3. Supervisors consider bank exposures to highly leveraged counterparties involving derivatives and securities financing transactions to be the riskiest. These types of exposures raise concerns about opaque concentration risks and potential sudden market stress, stemming from margin calls and fire sales of assets. In some instances, supervisors also note an increasing risk with regards to cryptoasset-related services provided by NBFIs.

4. The collapse of Archegos Capital Management highlighted deficiencies in some banks' risk management practices. Those deficiencies include:

- insufficient governance and risk management frameworks, including risk monitoring and stress testing in relation to the business strategy;

- inadequate collection of information on clients' positions and exposures as part of due diligence, and limited efforts to understand and assess clients' investing strategies;

- the absence of comprehensive limit frameworks;

- weak margining practices, including the use of "static" margining and inadequately calibrated margining by some banks; and

- possible regulatory arbitrage behaviour regarding the leverage ratio requirement.

5. Supervisors have encouraged banks to improve their practices by reviewing and enforcing existing guidelines and standards. Supervisors have put an increased focus on banks' risk management practices, emphasising rigorous onboarding due diligence and ongoing monitoring, risk-sensitive margining and the importance of robust information disclosures from investment fund counterparties.

6. Recent supervisory work revealed weaknesses in some banks' risk management practices related to commodities trading and highlighted broader counterparty credit risk measurement and management challenges. These weaknesses are often similar to those highlighted in the collapse of Archegos Capital Management, including the aggregation of counterparty risk exposure to effectively assess the concentration and

illiquidity of risk positions, with additional weaknesses unique to commodities in governance, onboarding, risk monitoring and margining.

7. Existing supervisory infrastructure regarding NBFI-related risk is generally sufficient. The Committee is discussing, including through other international forums, how to close data gaps and improve the visibility of interconnections between banks and NBFIs.

The Committee strongly encourages the proper application of existing standards and guidelines, as well as the full and timely implementation of the Basel III standards. It is committed to continuing to exchange supervisory views on banks' exposures to NBFIs including on recent episodes highlighting leverage, concentration and liquidity concerns in the non-bank sector and related supervisory practices. In addition, the Committee continues to contribute to the Financial Stability Board's work on assessing and addressing the risk from NBFIs.

To read more: https://www.bis.org/publ/bcbs_nl31.htm

Number 5

Token tactics: How to prevent, detect, and respond to cloud token theft - Microsoft Security Experts, Microsoft Detection and Response Team (DART)

As organizations increase their coverage of multifactor authentication (MFA), threat actors have begun to move to more sophisticated techniques to allow them to compromise corporate resources without needing to satisfy MFA. Recently, the Microsoft Detection and Response Team (DART) has seen an increase in attackers utilizing token theft for this purpose.

By compromising and replaying a token issued to an identity that has already completed multifactor authentication, the threat actor satisfies the validation of MFA and access is granted to organizational resources accordingly.

This poses to be a concerning tactic for defenders because the expertise needed to compromise a token is very low, is hard to detect, and few organizations have token theft mitigations in their incident response plan.

Why it matters

In the new world of hybrid work, users may be accessing corporate resources from personally owned or unmanaged devices which increases the risk of token theft occurring.

These unmanaged devices likely have weaker security controls than those that are managed by organizations, and most importantly, are not visible to corporate IT.

Users on these devices may be signed into both personal websites and corporate applications at the same time, allowing attackers to compromise tokens belonging to both.

As far as mitigations go, publicly available open-source tools for exploiting token theft already exist, and commodity credential theft malware has already been adapted to include this technique in their arsenal.

Detecting token theft can be difficult without the proper safeguards and visibility into authentication endpoints. Microsoft DART aims to provide defenders with the knowledge and strategies necessary to mitigate this tactic until permanent solutions become available.

Tokens are at the center of OAuth 2.0 identity platforms, such as Azure Active Directory (Azure AD).

To access a resource (for example, a web application protected by Azure AD), a user must present a valid token.

To obtain that token, the user must sign into Azure AD using their credentials.

At that point, depending on policy, they may be required to complete MFA. The user then presents that token to the web application, which validates the token and allows the user access.

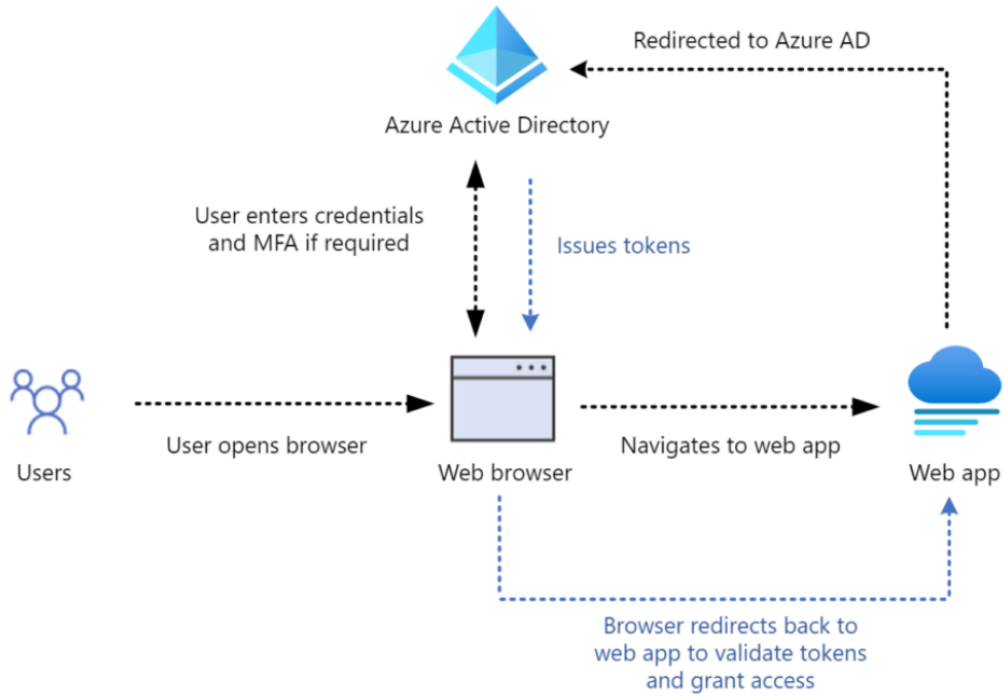


Figure 1. OAuth Token flow chart

When Azure AD issues a token, it contains information (claims) such as the username, source IP address, MFA, and more. It also includes any privilege a user has in Azure AD. If you sign in as a Global Administrator to your Azure AD tenant, then the token will reflect that.

Two of the most common token theft techniques DART has observed have been through adversary-in-the-middle (AitM) frameworks or the utilization of commodity malware (which enables a 'pass-the-cookie' scenario).

With traditional credential phishing, the attacker may use the credentials they have compromised to try and sign in to Azure AD. If the security policy requires MFA, the attacker is halted from being able to successfully sign in.

Though the users' credentials were compromised in this attack, the threat actor is prevented from accessing organizational resources.

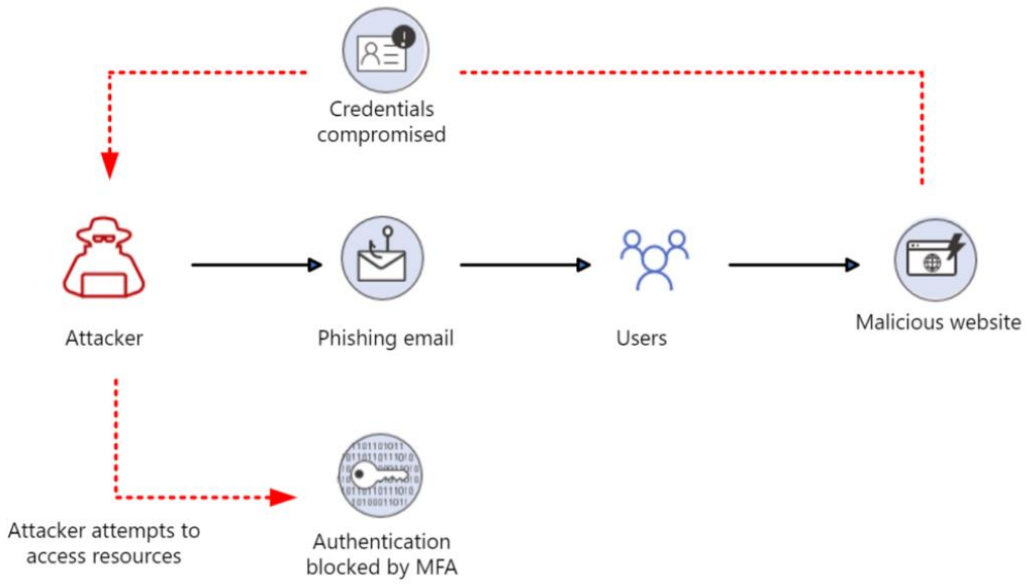


Figure 2. Common credential phishing attack mitigated by MFA

To read more:
https://www.microsoft.com/en-us/security/blog/2022/11/16/token-tactics-how-to-prevent-detect-and-respond-to-cloud-token-theft/

Number 6

EIOPA consults on cyber component in its insurance stress testing framework

The European Insurance and Occupational Pensions Authority (EIOPA) published a Discussion Paper on Methodological Principles of Insurance Stress Testing with focus on Cyber Risk.

This discussion paper contains a set of theoretical and practical approaches to support the design phase of potential future insurance stress tests with a focus on cyber risk. This should further enrich the bottom-up stress test toolbox with additional elements to be potentially applied in future exercises.

EIOPA aims at laying the groundwork for an assessment of insurers' financial resilience under severe but plausible cyber incident scenarios.

The paper elaborates on two main aspects:

1. Cyber resilience, understood as the capability of an insurance undertaking to sustain the financial impact of an adverse cyber event;

2. Cyber underwriting risk, understood as the capability of an insurance undertaking to sustain – from a capital and solvency perspective – the financial impact of an extreme but plausible adverse cyber scenario affecting underwritten business.

EIOPA invites stakeholders to share their feedback using the provided template no later than 28 February 2023. Contributions should be sent to the following email address: eiopa.stress.test@eiopa.europa.eu.

The feedback received will be considered in the preparation of a final methodological paper to be published on EIOPA's website.

Introduction

1. Stress testing, in its bottom-up form, almost since the establishment of EIOPA, became a key tool for the assessment of the vulnerability of the European insurance sector. In the fulfilment of its mandate, EIOPA regularly runs and evolves its bottom up stress test framework building on

the experience gained from past exercises, the contribution of its stakeholders and the analysis of the best practices implemented by other supervisors, financial institutions and standard setting bodies.

2. In its strive for continuous improvement, EIOPA published in the last three years two discussion papers whose content benefitted from the contribution of the insurance industry, actuarial associations and insurance associations, and generated three methodological papers that were used to design and operationalize the regular EU wide stress test exercises.

3. These papers aim at enhancing and strengthening by a technical and procedural perspective the EIOPA approach to bottom-up stress testing. As such, the information therein should not be considered as fully-fledged technical specifications for a stress test exercise, but rather as a reference to guide the design of future stress tests. Scenarios, shocks and their applications, data collected, will be inspired, but not limited, by the methodological papers according to the objective(s) and scope of each specific exercise.

4. This paper is the third discussion paper of the series and contains the set of theoretical and practical rules, guidelines and approaches to support the design phase of potential future insurance stress tests with a focus on cyber risk.

5. As shown in the EIOPA July 2022 Risk Dashboard, digitalisation and cyber risks have become one of the most important risks for the European insurance sector, with increasing momentum. These risks have been at high level since January 2022 and this risk level equates only to macro and market risks.

6. Furthermore, as outlined in the EIOPA June 2022 Financial Stability Report, the results of the EIOPA Spring 2022 insurance bottom-up survey (BUS) among supervisors show digitalisation and cyber risks ranking in the third place in terms of materiality, after market and macro risks, but above e.g. credit and profitability and solvency risks.

This represents an increase in materiality when compared to the EIOPA Autumn 2021 BUS, which ranked digitalisation and cyber risks in the fifth place. When considering the expected developments in terms of risk materiality over the next year, digitalisation and cyber risks are ranked second, behind macro risks.

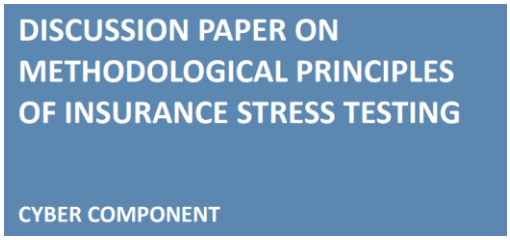
7. Cyber security risks are seen as the main driver of the developments in digitalisation and cyber risks (92% of supervisors), followed by cyber underwriting risks (4%).

Several supervisors associate the current war between Russia and Ukraine and resulting uncertainty to a potential increase in cyber risks. This adds to an already higher vulnerability of the sector during the Covid-19 pandemic due to an increased reliance on remote work and on digital solutions and infrastructure.

8. Cyber risk is receiving increasing attention by European and global regulators and standard setting bodies over the last two years. The IMF has identified cyber risk as a key threat to financial stability.

9 It estimates that the number of cyberattacks has tripled over the last decade, with financial services being the most affected industry due to the increased digitalisation of its business models. The Covid-19 crisis has accentuated the importance of cyber risk to financial institutions due to the increasing reliance on digital infrastructures and teleworking.

To read more:
https://www.eiopa.europa.eu/document-library/consultation/discussion-paper-methodologies-of-insurance-stress-testing-cyber_en



Number 7

Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests

Judicial and law enforcement authorities in Europe, Australia, the United States, Ukraine, and Canada have taken down a website that allowed fraudsters to impersonate trusted corporations or contacts to access sensitive information from victims, a type of cybercrime known as 'spoofing'.

The website is believed to have caused an estimated worldwide loss in excess of GBP 100 million (EUR 115 million).

In a coordinated action led by the United Kingdom and supported by Europol and Eurojust, 142 suspects have been arrested, including the main administrator of the website.

London's Metropolitan Police Commissioner Sir Mark Rowley stated: "The exploitation of technology by organised criminals is one of the greatest challenges for law enforcement in the 21st century. Together with the support of partners across UK policing and internationally, we are reinventing the way fraud is investigated. The Met is targeting the criminals at the centre of these illicit webs that cause misery to thousands. By taking

away the tools and systems that have enabled fraudsters to cheat innocent people at scale, this operation shows how we are determined to target corrupt individuals intent on exploiting often vulnerable people."

Eurojust President Mr Ladislav Hamran said: "As cybercrime knows no borders, effective judicial cooperation across jurisdictions is key in bringing its perpetrators to court. Eurojust supports national authorities in their efforts to protect citizens against online and offline threats, and to help see that justice gets done."

Europol's Executive Director Ms Catherine De Bolle said: "The arrests today send a message to cybercriminals that they can no longer hide behind perceived international anonymity. Europol coordinated the law enforcement community, enriched the information picture and brought criminal intelligence into ongoing operations to target the criminals wherever they are located. Together with our international partners, we will continue to relentlessly push the envelope to bring criminals to justice."

The services of the website allowed those who sign up and pay for the service to anonymously make spoofed calls, send recorded messages, and intercept one-time passwords.

The users were able to impersonate an infinite number of entities (such as banks, retail companies and government institutions) for financial gain and substantial losses to victims.

The investigations showed that the website has earned over EUR 3.7 million in 16 months. According to UK authorities, losses to victims at present are GBP 43 million (EUR 49 million), with estimated worldwide losses in excess of GBP 100 million (EUR 115 million).

In an international coordinated action carried out in November 2022, 142 users and administrators of the website were arrested across the world. The main administrator of the website was arrested in the UK on 6 November. On 8 November 2022, the website and server was seized and taken offline by US and Ukrainian authorities.

The case was opened at Eurojust in October 2021 at the request of the UK authorities. National authorities from ten countries, including European Union Member States and third countries, supported the investigation.

The Agency played a key role in facilitating the judicial cross-border cooperation among all parties involved. Two coordination meetings were hosted by Eurojust to coordinate the national investigations and to prepare for the action.

On a request of the United Kingdom, Europol started supporting the case earlier that same summer (August 2021). Since then, Europol's European Cybercrime Centre (EC3) has been providing continuous intelligence development to the national investigators through the Joint Cybercrime Action Taskforce (J-CAT).

In addition, EC3 provided a secure platform for law enforcement to exchange large packages of evidence. In the framework of its analytical work, Europol was able to identify additional users of the iSpoof service, a number of which were already known for their involvement in other high-profile cybercrime investigations at the European level.

To read more:
https://www.europol.europa.eu/media-press/newsroom/news/action-against-criminal-website-offered-%E2%80%98spoofing%E2%80%99-services-to-fraudsters-142-arrests

Number 8

Securing tomorrow today: Why Google now protects its internal communications from quantum threats

Google Cloud

When you visit a website and the URL starts with HTTPS, you're relying on a secure public key cryptographic protocol to shield the information you share with the site from casual eavesdroppers.

Public key cryptography underpins most secure communication protocols, including those we use internally at Google as part of our mission to protect our assets and our users' data against threats.

Our own internal encryption-in-transit protocol, Application Layer Transport Security (ALTS), uses public key cryptography algorithms to ensure that Google's internal infrastructure components talk to each other with the assurance that the communication is authenticated and encrypted.

Widely-deployed and vetted public key cryptography algorithms (such as RSA and Elliptic Curve Cryptography) are efficient and secure against today's adversaries.

However, as Google Cloud CISO Phil Venables wrote in July, we expect large-scale quantum computers to completely break these algorithms in the future.

The cryptographic community already has developed several alternatives to these algorithms, commonly referred to as post-quantum cryptography (PQC), that we expect will be able to resist quantum computer-driven attacks.

We're excited to announce that Google Cloud has already enabled one of the algorithms on our internal ALTS protocol today.

While current quantum computers do not have the capability to break widely-used cryptography schemes like RSA in practice, we still need to start planning our defense for two reasons:

1. An attacker might store encrypted data today, and decrypt it when they gain access to a quantum computer (also known as the store-now-decrypt-later attack).

2. Product lifetime might overlap with the arrival of quantum computers, and it will be difficult to update systems.

The first threat applies to encryption in transit, which uses quantum vulnerable asymmetric key agreements.

The second threat applies to hardware devices with a long lifespan — for example, certain secure boot applications which rely on digital signatures.

We focus on encryption in transit in this blog post, as ALTS traffic is often exposed to the public internet, and will discuss the implications for secure boot in our next blog post.

To read more:
https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms

Number 9

Court Authorizes the Seizure of Domains Used in Furtherance of a Cryptocurrency "Pig Butchering" Scheme

The U.S. Attorney's Office for the Eastern District of Virginia announced the seizure of seven domain names used in a recent cryptocurrency confidence crime, known as "pig butchering."

In pig butchering schemes, scammers encounter victims on dating apps, social media websites, or even random texts masquerading as a wrong number.

Scammers initiate relationships with victims and slowly gain their trust, eventually introducing the idea of making a business investment using cryptocurrency.

Victims are then directed to other members of the scam syndicate running fraudulent cryptocurrency investment platforms, where victims are persuaded to invest money.

Once the money is sent to the fake investment app, the scammer vanishes, taking all the money with them, often resulting in significant losses for the victim. And that is exactly what happened in this instance.

According to court records, from at least May through August 2022, scammers induced five victims in the United States by using the seven seized domains, which were all spoofed domains of the Singapore International Monetary Exchange.

The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters or hackers seek to persuade individuals that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal.

The scammers — using the confidence-building techniques described above — convinced the victims that they were investing in a legitimate cryptocurrency opportunity.

After the victims transferred investments into the deposit addresses that the scammers provided through the seven seized domain names, the victims' funds were immediately transferred through numerous private wallets and swapping services in an effort to conceal the source of the funds. In total, the victims lost over $10 million.

If you believe you are a victim, please contact IC3.gov to file a report.

Please provide detailed information in your report, including any purported investment websites visited, telephone numbers, email accounts, and social media profiles used by scammers, and any cryptocurrency addresses, transaction hashes, and dates of transactions.

Your responses are voluntary. Based on the information provided, you may be contacted by the United States Secret Service or other law enforcement entity and asked to provide additional information.

This office cannot act as your attorney or provide you with legal advice. However, you may seek the advice of an attorney with respect to this or other related legal matters.

To read more:
https://www.justice.gov/usao-edva/pr/court-authorizes-seizure-domains-used-furtherance-cryptocurrency-pig-butchering-scheme

Number 10

Cranking the Power on Radar Capabilities

DARPA looks to build on previous success in radio frequency power output with new transistor-focused THREADS program

Military and civilian uses for radar range broadly, and the possibilities for radar applications expand almost every day.

Whether they are being used to navigate, control air traffic, track weather patterns, carry out search-and-rescue missions, map terrain, or countless other functions, radar technologies are constantly advancing.

As radio-frequency (RF) systems, radar capabilities hinge on the ability to sense and communicate across long distances while maintaining signal strength.

Powerful RF signal capabilities extend mission-critical communications and situational awareness, but the microelectronic technologies that strengthen RF output – specifically, high power density transistors – must overcome thermal limitations to operate reliably and at significantly higher capacity.

Technologies for Heat Removal in Electronics at the Device Scale (THREADS) aims to overcome the thermal limits inherent to internal circuitry operations in general, and to critical power-amplifying functions specifically.

Today, RF systems operate well below the limits of electronic capacity simply because the transistors, the basic building blocks of RF amplifiers, get too hot. With new materials and approaches to diffusing the heat that degrades performance and mission life, THREADS targets thermal management challenges at the transistor level.

Central to this effort will be reducing the thermal resistance involved in dissipating internal heat without degrading performance or increasing the footprint of the transistors key to advancing radar capabilities.

To that end, the work under THREADS in overcoming thermal limits can help realize robust, high power density transistors that operate near their fundamental electronic limit – achieving new levels in amplifying RF output power.

"Wide bandgap transistors, such as gallium nitride (GaN), were developed specifically to improve output density in power amplifiers – and GaN does provide a greater than 5x improvement compared to previous-generation transistor technology. We also know that a further order-of-magnitude increase in power output is possible in GaN, but it can't be realized in sustained operation today due to excessive waste heat," said Thomas Kazior, the DARPA program manager for THREADS.

"If we can relax the heat problem, we can crank up the amplifier and increase the range of radar. If the program is successful, we're looking at increasing the range of radar by a factor of 2x to 3x."

A Proposers Day for THREADS is scheduled for Nov. 30, 2022, with abstracts due by Dec. 22, 2022. More information on the Proposers Day can be found on sam.gov, and further program details are available in the broad agency announcement at:
https://sam.gov/opp/4f04a2bcda114333a426c4d57ffa4081/view

To read more: https://www.darpa.mil/news-events/2022-11-23

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,

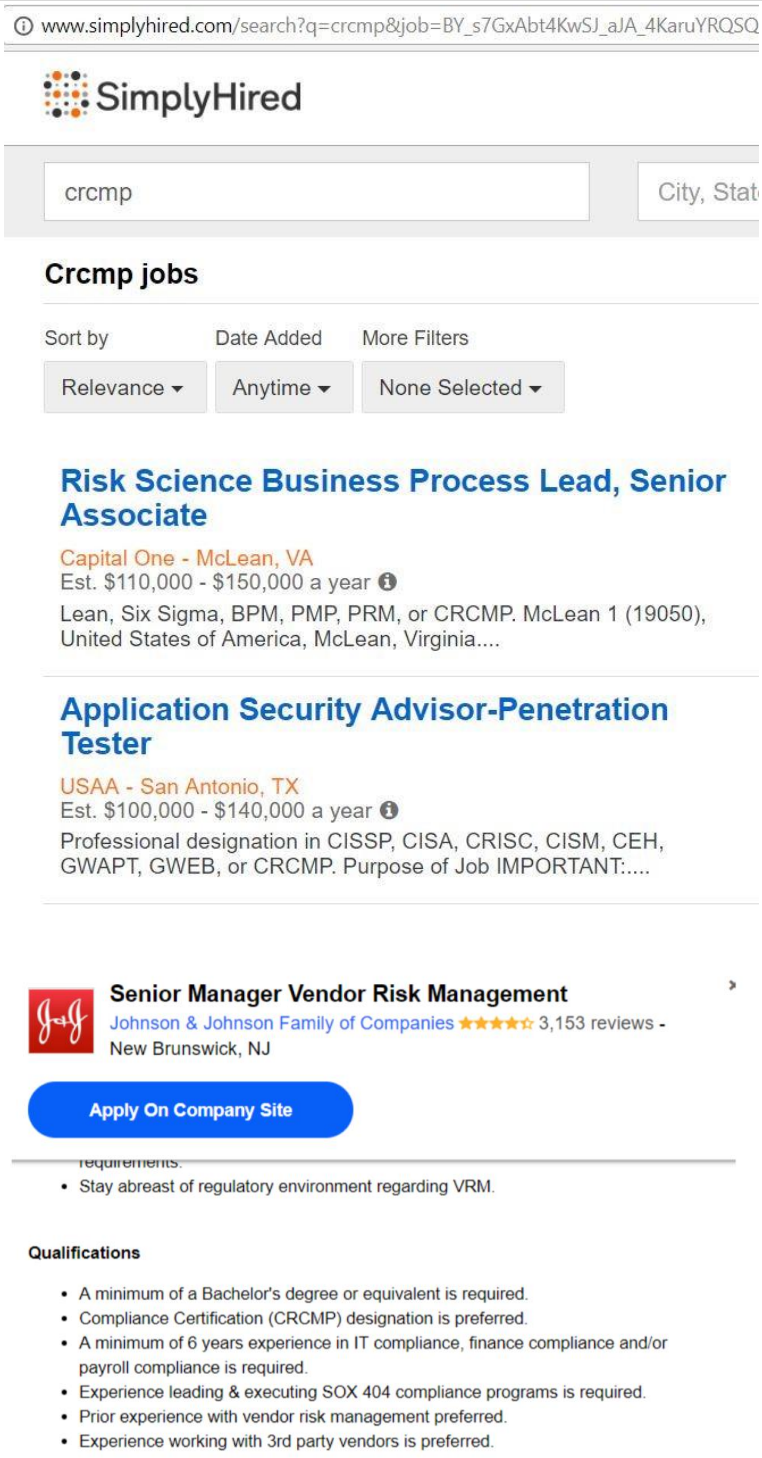
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.