Hedge Funds News, February 2025

The European Banking Authority (EBA) published its final Guidelines on the management of Environmental, Social and Governance (ESG) risks.

The Guidelines set out requirements for institutions for the identification, measurement, management and monitoring of ESG risks, including through plans aimed at ensuring their resilience in the short, medium and long term.

The Guidelines specify requirements regarding the internal processes and ESG risk management arrangements that institutions should have in place in accordance with the Capital Requirements Directive (CRD6). They will contribute to ensuring the safety and soundness of institutions as ESG risks intensify and the EU transitions towards a more sustainable economy.

The Guidelines specify the content of plans to be prepared by institutions with a view to monitoring and addressing the financial risks stemming from ESG factors, including those arising from the adjustment process towards the objective of achieving climate neutrality in the EU by 2050.

These plans will support the preparedness of institutions for the transition and should be consistent with transition plans prepared or disclosed by institutions under other pieces of EU legislation.

The Guidelines will apply from 11 January 2026 except for small and non-complex institutions for which the Guidelines will apply at the latest from 11 January 2027.

Executive Summary

The EBA is mandated in accordance with Article 87a(5) of Directive 2013/36/EU to issue guidelines on minimum standards and reference methodologies for the identification, measurement, management and monitoring of environmental, social and governance (ESG) risks by institutions.

ESG risks, in particular environmental risks through transition and physical risk drivers, pose challenges to the safety and soundness of institutions and may affect all traditional categories of financial risks to which they are exposed.

To ensure the resilience of the business model and risk profile of institutions in the short, medium and long term, the guidelines set requirements for the internal processes and ESG risk management arrangements that institutions should have in place.

Institutions, based on regular and comprehensive materiality assessments of ESG risks, should ensure that they are able to properly identify and measure ESG risks through sound data processes and a combination of methodologies, including exposure-, portfolio- and sector-based, portfolio alignment and scenario-based methodologies.

Institutions should integrate ESG risks into their regular risk management framework by considering their role as potential drivers of all traditional categories of financial risks, including credit, market, operational, reputational, liquidity, business model, and concentration risks.

Institutions should have a robust and sound approach to managing and mitigating ESG risks over the short, medium and long term, including a time horizon of at least 10 years, and should apply a range of risk management tools including engagement with counterparties.

Institutions should embed ESG risks in their regular processes including in the risk appetite, internal controls and ICAAP. Besides, institutions should monitor ESG risks through effective internal reporting frameworks and a range of backward- and forward-looking ESG risk metrics and indicators.

Institutions should develop specific plans to address the risks arising from the transition and process of adjustment of the economy towards the regulatory objectives related to ESG factors of the jurisdictions they operate in.

To this end, institutions should assess and embed forward-looking ESG risk considerations in their strategies, policies and risk management processes through transition planning considering short-, medium- and long-term time horizons.

CRD-based plans take a risk-based view and contribute to the overall resilience of institutions towards ESG risks and should be consistent with transition plans prepared or disclosed by institutions under other pieces of EU legislation.

Impact of ESG risks

1. Climate change, environmental degradation, biodiversity loss, social issues and other environmental, social and governance (ESG) factors pose considerable challenges for the economy.

The impact of acute and chronic physical risk events, the need to transition to a low-carbon, resource-efficient and sustainable economy, as well as other ESG challenges, are

causing and will continue to cause profound economic transformations that impact the financial sector.

EBA/GL/2025/01

08/01/2025

Final Report

Guidelines on the management of environmental, social and governance (ESG) risks

2. The Commission's Renewed Sustainable Finance Strategy and the banking package (Directive 2013/36/EU (Capital Requirements Directive, CRD) and Regulation (EU) No 575/2013 (Capital Requirements Regulation, CRR)) recognise that the financial sector has an important role to play both in terms of supporting the transition towards a climate-neutral and sustainable economy, as enshrined in the Paris Agreement, the United Nations 2030 Agenda for Sustainable Development and the European Green Deal, and for managing the financial risks that this transition may entail and/or those stemming from other ESG factors.

3. Environmental risks, including climate-related risks, are expected inter alia to become even more prominent going forward through different possible combinations of transition and physical risks. These may affect all traditional categories of financial risks to which institutions are exposed.

In addition, institutions' counterparties or invested assets may be subject to the negative impact of social factors, such as breaches of human rights, demographic change, digitalisation, health or working conditions, and governance factors, such as shortcomings in executive leadership or bribery and corruption, which may in turn lead to financial risks that institutions should assess and manage.

4. To maintain adequate resilience to the negative impacts of ESG factors, institutions established in the EU need to be able to systematically identify, measure and manage ESG risks. However, the specificities of ESG risks such as their forward-looking nature and distinct impacts over various time horizons, as well as the lack of relevant historical experience, means that understanding, measurement and management practices can differ significantly across institutions.

The EBA's observations stemming from the monitoring of supervisory colleges, as well as supervisory experience from competent authorities, also show that the management of ESG risks is still at an early stage and 'work in progress', with only nascent practices on ESG risks other than climate-related risks in most EU institutions.

Despite action taken in recent years, several shortcomings have been observed in the inclusion of ESG risks in business strategies and risk management frameworks that may pose challenges to the safety and soundness of institutions as the EU transitions towards a more sustainable economy and the materialisation of ESG risks intensifies.

To read more: https://www.eba.europa.eu/sites/default/files/2025-01/fb22982a-d69d-42cc-9d62-1023497ad58a/Final%20Guidelines%20on%20the%20management%20of%20ESG%20risks.pdf

Global Economy: Fragmentation, Decoupling or Slowbalisation?

Bank of Finland governor Olli Rehn delivered a keynote speech in a conference co-organised by the European Central Bank, Hong Kong Institute for Monetary and Financial Research and Bank of Finland Institute for Emerging economies.

SUOMEN PANKKI EUROJÄRJESTELMÄ FINLANDS BANK EUROSYSTEMET

Distinguished Guests, Ladies and Gentlemen, Dear Friends,

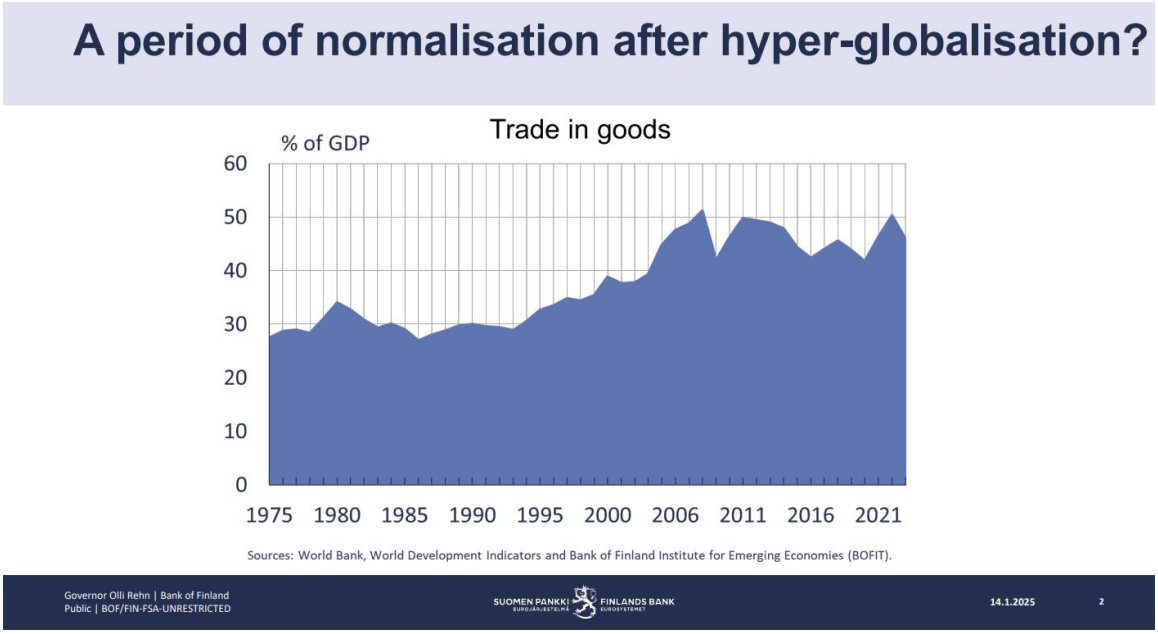
Let me start by thanking the Hong Kong Monetary Authority for hosting this topical and thought-provoking conference. Discussing the changing global economy in "Asia's World City" is, of course, very appropriate.

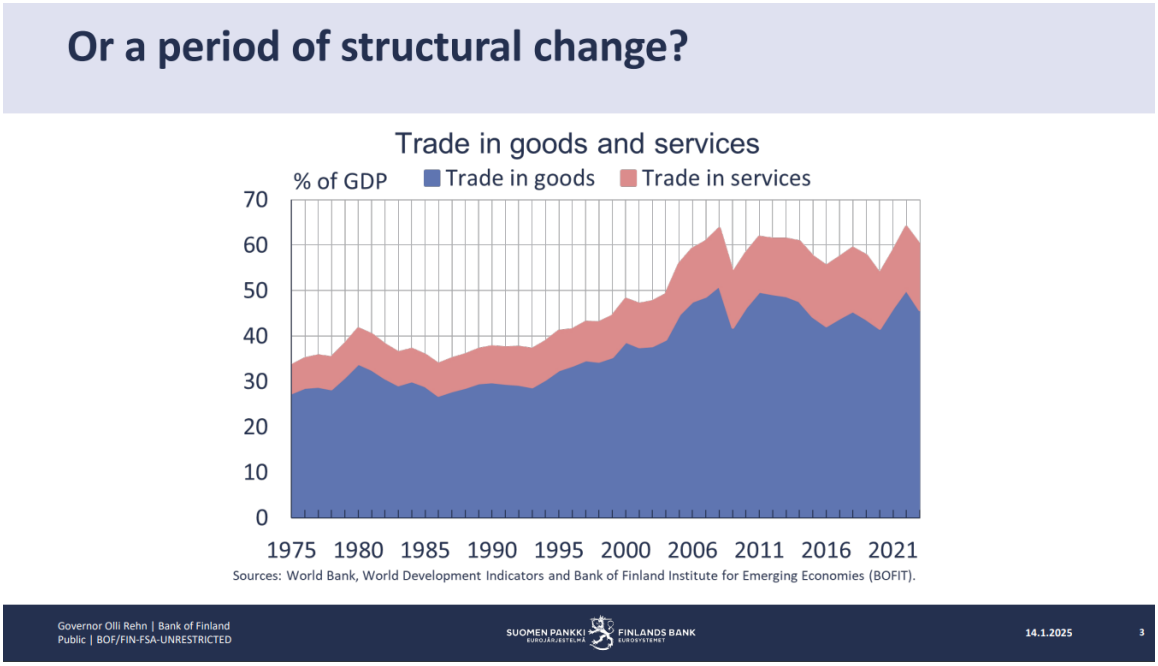
I would also like to thank the representatives of the European Central Bank for their involvement in putting together the programme for this excellent event. This conference is a good example of fruitful cooperation between central banking authorities from different parts of the world, and certainly a tradition worth preserving.

As the title of the conference implies, the global economy is undergoing a transformation. In my talk today I would like to address a key aspect of this transformation, namely decoupling and fragmentation in the global economy.

Is there evidence of geoeconomic fragmentation in the global trade and investment data? Or is global trade simply following the same trajectory as global economic output? There is, of course, an important difference between the paths of global trade and global output.

Slide 2. A period of normalisation after hyper-globalisation?





We can, in my view, reasonably start the analysis of any decoupling or fragmentation with a slide like this, which shows the value of the global goods trade in relation to the global gross domestic product (GDP).

We can observe how this percentage climbs in the late 1990s and 2000s, pushed by the integration of China and former socialist countries into the global economy and global value chains. In the early 1990s global trade was roughly 30% of the global GDP, and by 2008 this had increased to over 50%.

As the graph shows, the global financial crisis marked a clear turning point. Since then, the level of global trade in relation to global GDP has fluctuated between 45% and 50%. Should we call it ‘slowbalisation’?

There are of course many reasons for this relative stagnation, but here in Hong Kong we should note at least one factor. Whereas in the early 2000s many value chains in East Asia were international, by the 2010s a larger share of production had moved into one country: China.

If, for example, a component had previously crossed national borders, say, eight times, by the 2010s more of the value-added was accruing to Chinese companies, and the component would cross national borders only five times.

What is the main implication of this in terms of globalisation currently? So far, various trade restrictions and higher tariffs have not been enough to reverse the gains in globalisation.

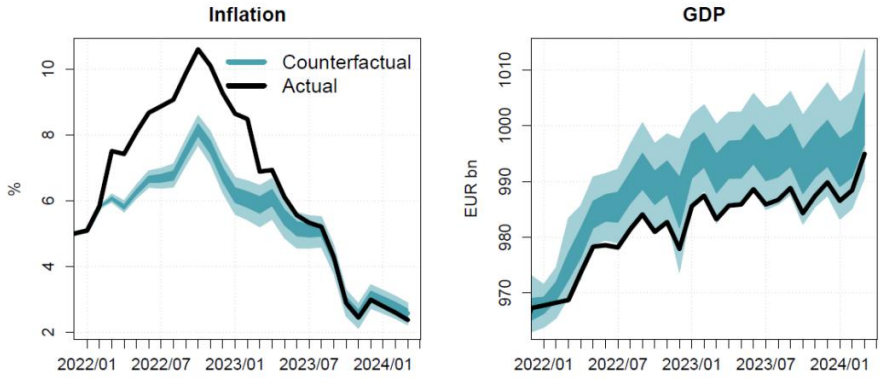
Slide 3. Or a period of structural change?

Another aspect of the transformation of world trade is sectoral. We typically look at the trade in goods, but the trade in services is often neglected in public debate. The share of services in total international trade is already about one quarter, and this has been increasing. I am confident that this trend will continue in the coming years.

In many OECD countries, including the United States and Finland, services already account for one third of their total external trade.

With telecommunications costs falling, many companies even in middle-income countries can participate effectively in the global trade in services. This is hopefully and perhaps also likely an area where trade barriers of various kinds will be more difficult to implement.

Geopolitical risks can materialise: Russia's invasion of Ukraine also harmed the euro area economy



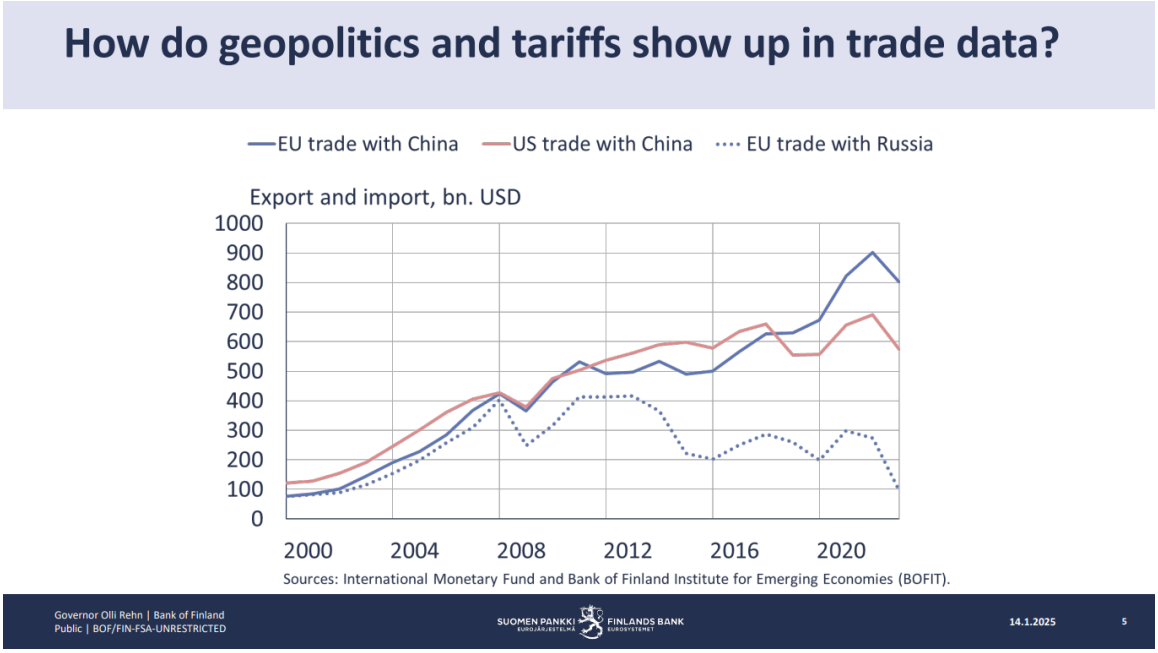
Source: Anttonen and Lehmus (2024).

Slide 4. Geopolitical risks can materialise: Russia's invasion of Ukraine also harmed the euro area economy

Trade restrictions and tariffs are not the only geopolitical factors that can affect trade and economic development. Clearly, major geopolitical events and shocks can have huge consequences.

Russia's illegal and brutal invasion of Ukraine has been devastating for Ukraine and the Ukrainian people. At the same time, it has also been a massive negative supply shock and an adverse geopolitical shock for the euro area. According to the Bank of Finland's analysis, this shock caused the inflation rate in the euro area to be 2 percentage points higher, and GDP to be correspondingly lower, than would otherwise have been the case.

It is also worth noting that the energy price shock following Russia's invasion was not limited to Europe. Global energy prices went up, and this had a negative effect in Asia too. What happens in Europe doesn't stay in Europe.



Slide 5. How do geopolitics and tariffs show up in trade data?

Furthermore, even if tariffs and protectionism have not yet led to a decline in total global trade, this may not be the case in the future.

We are already witnessing signs of trade fragmentation, primarily in two significant ways.

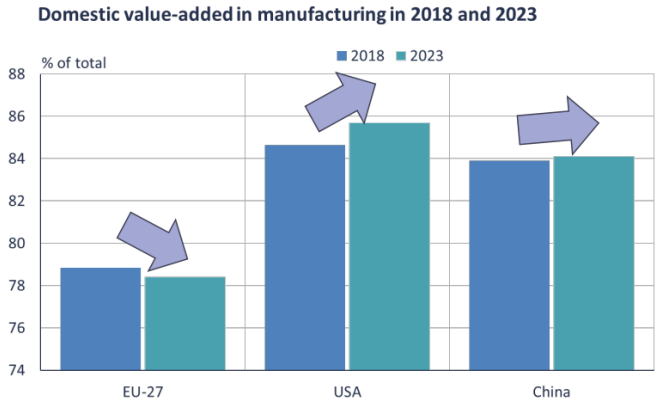
Firstly, bilateral trade between the US and China has stalled, and some supply chains have been relocated from China to Southeast Asia, Mexico and emerging economies in Europe. These shifts aim to mitigate supply chain disruption risks and avoid import tariffs or export restrictions.

Secondly, Russia's war in Ukraine has effectively isolated Russia from the European Union, the G7 countries and their allies. This has resulted in a dramatic reduction in trade between the EU and Russia since February 2022. The goal of the sanctions is clear: to cause damage to the Russian war machine and its imperialistic invasion.

Slide 6. Domestic value-added has decreased in the EU

In this complex environment, it is useful to examine whether production is being reshored – transferred back home – at significant levels. In other words, is globalisation truly reversing?

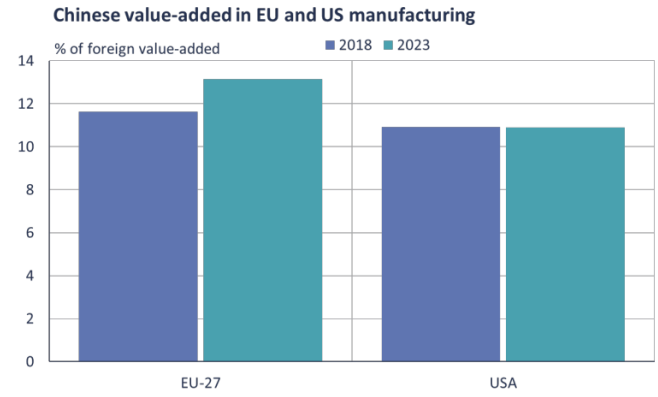
Domestic value-added has decreased in the EU



Sources: Bank of Finland Institute for Emerging Economies (BOFIT), based on Asian Development Bank (ADB) data.

Our staff analysis of the origins of value-added in manufacturing indicates that in the United States, the share of domestically produced value-added increased between 2018 and 2023. Conversely, in the EU, there was a small decrease in domestic value-added. This suggests some reshoring dynamics in the US and the opposite in Europe.

Chinese value-added has increased in the EU and remains unchanged in the US



Sources: Bank of Finland Institute for Emerging Economies (BOFIT), based on Asian Development Bank (ADB) data.

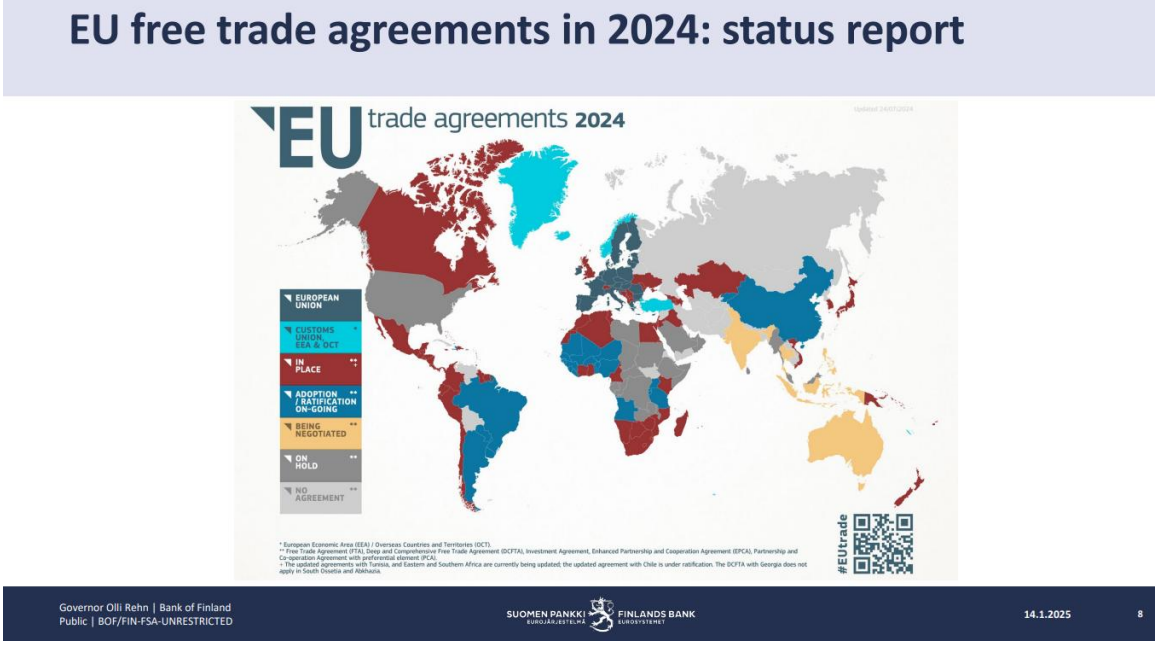
Slide 7. Chinese value-added has increased in the EU and remains unchanged in the US

Our findings also highlight the challenges of decoupling or de-risking from China, due to the deeply integrated nature of global production networks. Even though direct trade between China and the United States shows signs of a modest decline, the share of Chinese value-added in US manufacturing imports remained stable during the period

examined. It appears that value chains are simply being re-routed through connector countries like Mexico and Vietnam.

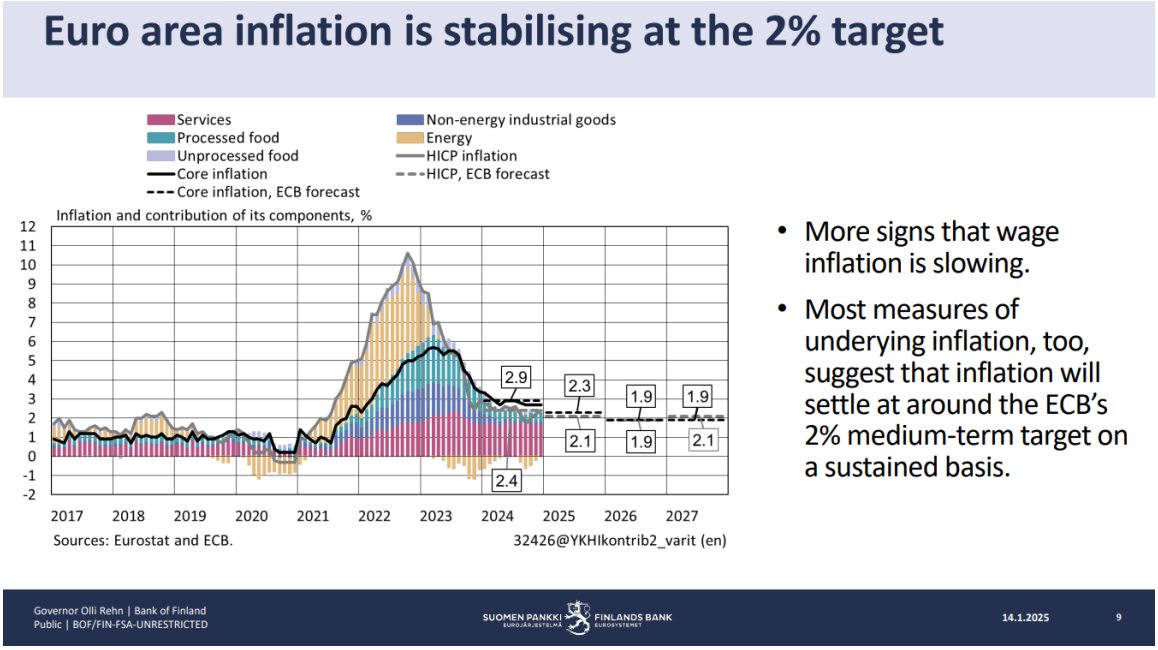
In the European Union, Chinese value-added in manufacturing has in fact increased since 2018. This illustrates the challenges related to even moderate decoupling, which in Europe is seen as necessary de-risking in today's geopolitical context.

In this challenging global context, the European Central Bank's monetary policy aims at ensuring price stability, which also supports the EU's general economic policies.



Slide 8. EU free trade agreements in 2024: status report

In this challenging global context, the European Central Bank's monetary policy aims at ensuring price stability, which also supports the EU's general economic policies.



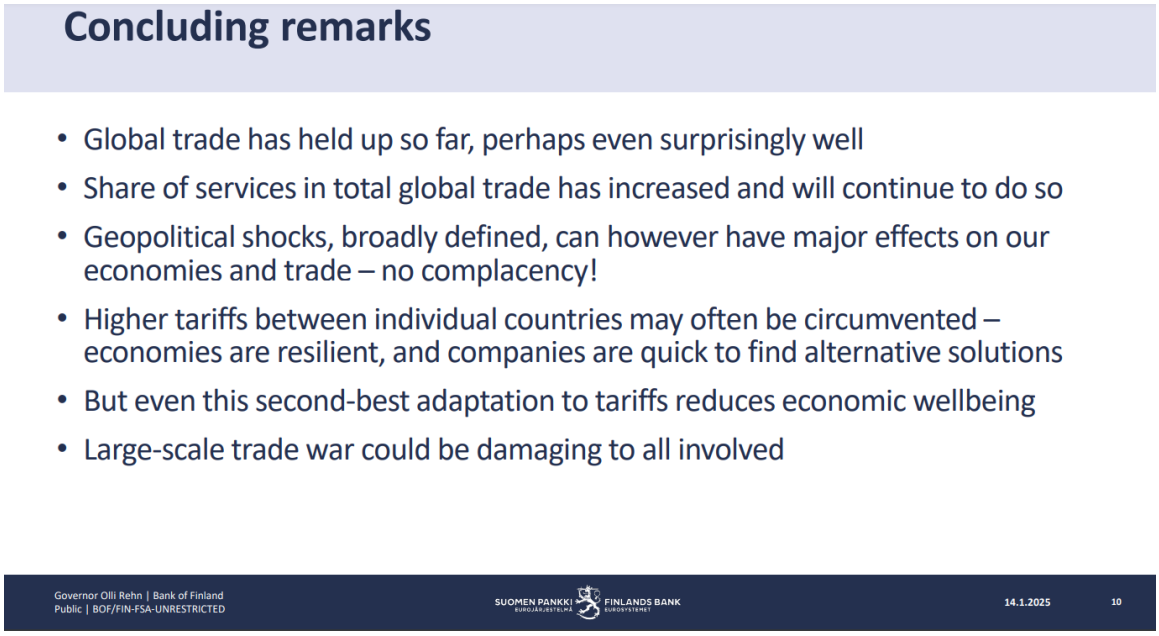
Slide 9. Euro area inflation is stabilising at the 2% target

In the euro area, disinflation is well on track. Wage pressures have also somewhat receded. Meanwhile the growth outlook has weakened. This has prompted us at the ECB's Governing Council to cut interest rates four times in the last six months.

Going forward, the direction of our monetary policy is clear. The scope and speed of rate cuts will depend on incoming data regarding three factors, in particular: the inflation outlook, the underlying inflation dynamics and monetary policy transmission.

The Governing Council will decide on interest rates in each of its monetary policy meetings, taking into account all the new information and analysis that has accrued since the previous meeting. In the forthcoming meetings we should also have more information on the policies of the incoming US administration and on the European response to those policies.

In light of the current economic outlook and our reaction functions, I would assume that our monetary policy will leave restrictive territory in the coming months, at the latest by midsummer.



Slide 10. Concluding remarks

So, is the glass of global trade half empty or half full?

Total trade has held up so far, perhaps surprisingly well. Services have become more and more important in global trade, and this trend will continue.

But we must not be complacent. Geopolitical shocks, like Russia's invasion of Ukraine or higher barriers to trade, can have negative effects on our economies.

Tariffs between any two countries, like the US and China, may often be circumvented one way or another. Companies are nimble in moving production to avoid tariffs. This kind of adaptation makes economies more resilient, but at the same time it does add to the costs of doing business. If considerably higher tariffs or other trade restrictions were

introduced, these costs of doing business would increase more significantly – for all of us.

Furthermore, such a trade war could have a negative impact in other areas as well. Fraying and frozen international relations would, in turn, make ending a trade war more difficult. There are no winners in a trade war.

This is the reason why we in Finland and Europe continue to defend the rules-based international order in security and trade and the legal rights of independent nations – in Europe, in the global South and across the world. In my view, this is crucial for global peace and development of the humankind.

Thank you for your attention!

To read more: https://www.suomenpankki.fi/en/news-and-topical/speeches-and-interviews2/2025/global-economy-fragmentation-decoupling-or-slowbalisation/

The presentation: https://www.suomenpankki.fi/globalassets/bof/fi/ajankohtaista/puheet/2025/2025-01-14-rehn_slides_hkma-ecb-bof_2.pdf

Reading between the lines

Sarah Breeden, Deputy Governor for Financial Stability of the Bank of England, at the University of Edinburgh Business School, Edingburgh, 9 January 2025.

It has been a little over a year since I joined the Monetary Policy Committee (MPC). Lots has happened over that period. I'm going to use this speech to review what we have learned and where that leaves my view of the outlook for the economy and for monetary policy. In doing that, I will aim to explain how important it is for us to keep asking ourselves which shocks could be hitting the economy and what implications those different shocks would have for medium-term inflation.

We are always reading between the lines. Before I get into the meat of the speech, I wanted to thank you for inviting me to come to speak to you today. I can think of few better places to come to talk about the economy than one of the homes of Adam Smith, the father of the discipline – I just can't promise to be as insightful and groundbreaking as he was in his day!

Why do shocks matter?

Inflation has fallen materially over the past year. That is welcome news, especially given the painful high inflation period we found ourselves in during the prior couple of years. But as monetary policymakers we must stay focused on where the economy might be heading, not where it has been.

That means taking a view on which shocks are hitting the economy and how they might play out over time. This is easier said than done. It is notoriously hard to know which shocks are hitting the economy in real time. Reasonable people could take different views on the shocks that explain the same set of data.

For example, is a reduction in economic activity a sign of lower domestic demand, lower demand from abroad or a reduction in the supply capacity of the economy? Is a fall in import price inflation a sign of past shocks easing off or a new shock hitting? Does it reflect a weaker global economy or more productive global suppliers? This isn't just an intellectual exercise.

Attributing data news to the 'wrong' shocks can have material implications for our understanding of the evolution of the economy in the future, and therefore what we should do with monetary policy. As policymakers we are constantly discussing and revising our views on which shocks best explain what we are seeing in the economy.

At the Bank we do this by drawing on a wide range of hard and soft data, reports from people closer to the ground – such as the intelligence gathered via our Agency network, including from here in Scotland – and a large set of modelling and analytical techniques.

Learning from recent experience

In the past few years the economy has been hit by a series of very large shocks. We had no examples of shocks of the same type and scale under our current monetary policy regime, and so little in the way of past experience to guide us on how the economy would react to them. Perhaps naturally then, our understanding of those shocks has evolved with the passing of time, as more data has come in and as we have conducted more analysis.

I am going to walk you through a few important and very practical examples where we have changed our view in a way that makes a difference for our understanding of inflationary dynamics, and therefore for monetary policy. And then I'll turn to some of the current puzzles we are facing.

Example 1: Demand environment

The first example relates to the demand environment – by which I mean the level of demand relative to supply, as captured in the output gap.

There was very material uncertainty – considerably more than usual – about the balance of demand and supply during the pandemic, as well as uncertainty about how that balance might respond to the shocks that hit the economy after the pandemic was over.

As I'll explain, uncertainty about this balance between demand and supply matters, given its key role in inflationary dynamics.

We reassess the balance of demand and supply, as reflected in the estimated level of the output gap, every quarter using a set of statistical models, which draw on a range of data including nominal and real indicators.

We use the steer from those models – along with a judgement overlay and evidence from other indicators of spare capacity, for example in the labour market and within businesses – to judge whether data news reflects demand or supply factors.

That process means we sometimes end up revising our view of the past as well as the current level of the output gap, given that the data and so the steer we take from it can change materially over time.

Chart 1: We have consistently revised up our view of the strength of demand

Range of output gap estimates in all MPR forecasts from Covid to November 2024(a)

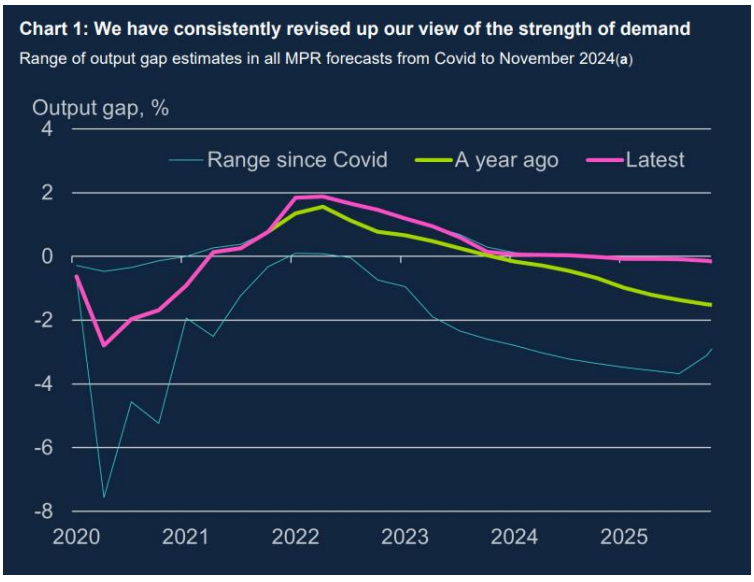


Chart 1 shows the range of our output gap estimates since the pandemic. During the pandemic itself in 2020 the MPC took the view that low inflation was explained by a very large output gap. But given the scale and nature of the changes in the structure of the economy at that time, they highlighted the material uncertainty around those estimates.

We have since concluded that the output gap was much less negative than we thought at that time. Our latest estimates – for the recent past and into the future – have been revised up materially and are right at the top of the range.

Many of the upwards revisions came in periods when GDP data was coming in stronger than we expected (I'll return to this in my second example).

Taking the changes together, we now judge the output gap to have been 2-3 percentage points stronger in 2022 and 2023 than we previously thought, which changes the picture from an economy that was broadly in balance to one with material excess demand.

That upwards revision is sizeable and persistent. The scale of these revisions in a relatively short space of time underlines quite how uncertain output gap estimation can be. One driver of stronger demand could be our evolving view on how monetary policy affects the economy.

Our latest assessment points to a faster and lower peak impact of Bank Rate on the output gap than we thought before this cycle. The reasons for faster transmission to a lower peak are complex relating both to the evolution of interest rates during the tightening cycle and to the conditions prevailing in the economy at the time.

Why might these changes in the output gap matter? The output gap is a key determinant of medium-term inflation, via the Philips curve.

A rough rule-of-thumb might map a 1 percentage point increase in the output gap into around a 0.3 to 0.4 percentage point increase in inflation a year or so later. There is of course huge uncertainty around that rough relationship and a large literature on the shape of the Phillips curve, which can change over time. But the main point is that the revisions I am pointing to here are not small. Taken at face value, on their own these revisions might imply higher inflation next year and into 2026 by up to 1 percentage point.

It is important to note that an increase in the output gap does not necessarily imply a positive demand shock. It could just as well be driven by a fall in supply with a less than one-for-one fall in demand, which would open up an output gap alongside weaker activity. Given the absolute weakness of economic activity in the UK data in recent years, it seems plausible that some of the strength in the output gap might have been driven by weaker supply rather than stronger demand.

To read more: https://www.bankofengland.co.uk/speech/2025/january/sarah-breeden-speech-at-the-university-of-edinburgh

The Relevance of Transition Plans for Financial Stability

FSB FINANCIAL STABILITY BOARD

Executive Summary

Climate transition planning and the resulting outputs – transition plans – have seen increased interest in recent years as a tool for firms (both non-financial companies and financial institutions) to articulate their strategies and management of climate-related risks.

Transition plans may be used for various purposes by shareholders, investors and regulators to be informed of a company's strategy and approaches to climate change and transition. Some governments may require, or otherwise use, the corporate transition planning process as a means to encourage corporate action in order to achieve national climate goals.

Multiple initiatives aim to standardise transition plans to support preparers and help meet the needs of users of the plans.

The FSB has examined the relevance of transition plans and planning for financial stability, and whether and how they may have uses for financial stability authorities.

A stocktake of member jurisdictions revealed differing views on the relevance of transition plans for financial stability monitoring.

Some authorities require firms to prepare and disclose transition plans, while some others do not require transition plans nor envision using transition plans for prudential purposes in the near future.

Even for authorities that have initiatives relating to transition plans and recognise the potential usefulness of this tool, their use for financial stability and macroprudential purposes remains in the early stages.

The specific mandates of authorities are also relevant to the potential use of transition plans for financial stability objectives. As such, this report does not provide recommendations but, rather, an early analysis of the role that transition plans and planning could play for financial stability purposes, drawing on a range of practices and perspectives.

Transition plans may potentially offer financial authorities a forward-looking perspective on transition pathways, enhancing the understanding of climate-related financial risks at both micro and macro-levels.

These plans could enable an assessment of how firms may adjust their activities in response to climate risks and include information that could support financial stability objectives, including through metrics for financial stability monitoring. Although subject to uncertainty about the future, the disclosure of forward-looking information in transition plans may also benefit financial stability through enhanced market transparency about envisaged strategies and identified risks and opportunities, and it may give firms an incentive to improve their own transition planning processes.

Transition plans can interact with climate-related financial risks through three main channels:

- Facilitating firms' strategy setting, which informs better climate-related risk management: A firm's transition planning process could assist in its strategy setting. Financial institutions' access to forward-looking information from their counterparties could support their own transition and risk management of climate-related risks. At scale and under relevant conditions, this could reduce the financial stability risks from the transition.

- Informing investment decisions: Greater consistency in forward-looking information in transition plans, and wider production and use of plans, could improve asset pricing and transition financing, by addressing information gaps and reducing market failures. This increases market efficiency and helps firms to better align their transition strategies, by reducing information asymmetries across firms in the financial and nonfinancial sector.

- Supporting financial authorities' macro-monitoring of transition and physical risks both in the financial system and the real economy: Transition plans could assist authorities in monitoring climate-related financial risks and facilitate the identification and assessment of systemic risks. Transition plans could inform scenario narratives and modelling, while scenario analysis could help firms assess the impact of climate risks on their strategies and business models.

However, there are important caveats to using transition plans for financial stability assessments effectively.

First, transition plans are not inherently designed for the purpose of financial stability assessments; their primary purpose is business strategy and linked to target setting.

Second, they are currently only developed by a limited population of firms, with wide differences in format, content and methodological assumptions.

Third, mechanisms to assure the reliability of information in transition plans are still emerging.

Lastly, analytical thinking on how they could be used specifically for financial stability analysis is still at an early stage.

Certain enabling conditions would need to be met to enable the use of transition plans for financial stability purposes, including greater standardisation to support credibility and reliability, comparability and broader adoption.

Limited data availability, and differences in scope, coverage and quality of key metrics in transition plans of both financial and non-financial corporates reduce the ability of financial authorities to draw comparisons or overarching conclusions across financial institutions and for the financial system as a whole.

For information in transition plans to be useful for financial stability monitoring, it would need to be credible, transparent, based on clearly stated assumptions and on sufficiently consistent methodologies and metrics. Enabling conditions for such use include sufficient coverage, transparency, credibility, comparability and broader availability of information.

Table of Contents

At the current stage, information about transition plans is neither fully standardised nor widely disclosed. That said, there are signs that these enabling conditions could be partially satisfied over time and that the usefulness of transition plans for macroprudential authorities could grow.

The implementation of the International Sustainability Standards Board (ISSB)'s inaugural sustainability disclosure standards, the IFRS Foundation's announcement on their plans to support work to streamline and consolidate frameworks and standards for disclosures about transition plans, and the development of a global assurance framework for sustainability-related reporting could improve disclosure comparability and reliability and thereby enhance the usefulness of transition plans for financial stability.

These developments may also enable financial institutions and non-financial firms to make more informed decisions and adjust their strategies in response to climate related risks, thereby also supporting financial stability.

It is early days for jurisdictions and financial sector authorities in making concrete use of transition plans from a policy standpoint, also in light of their different mandates and objectives.

Transition plans hold potential for enhancing financial stability by providing forward-looking information that can be useful to measure and monitor climate-related risks. However, certain challenges and the enabling conditions mentioned above would need to be addressed before transition plans can be used for financial stability purposes.

Transition plan practice will continue to develop over the coming years. In jurisdictions where authorities intend to use transition plans for financial stability assessment, this will provide a clearer picture of how transition plans could be used for climate vulnerability assessment and for macroprudential purposes. Ongoing and planned work by international organisations and standard setters contributes to these efforts.

Box 1. Market failures that could potentially be addressed by transition plans

Figure 1. Macroprudentially-relevant market failures that could potentially be addressed by transition plans

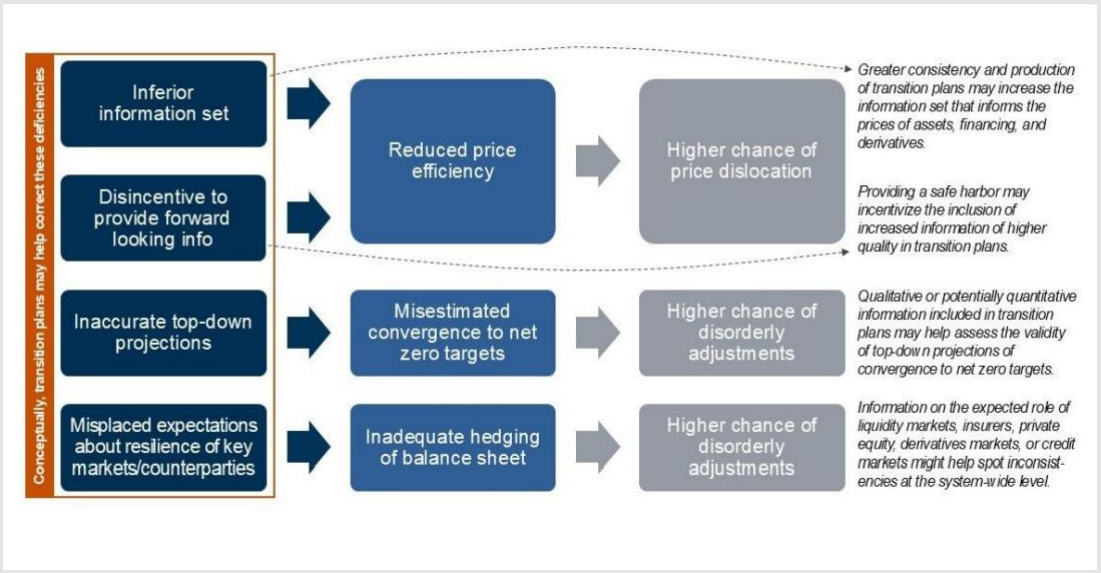
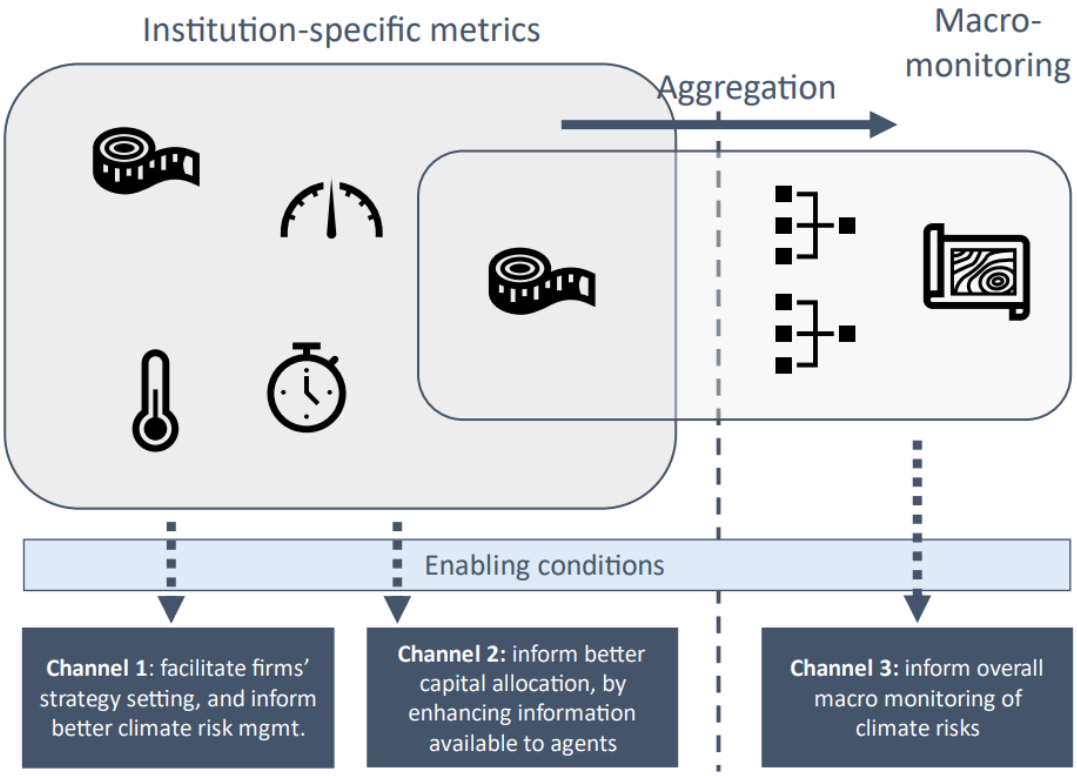


Figure 2. Interaction between transition plans and macro-monitoring



Note: The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

To read more: https://www.fsb.org/uploads/P140125.pdf

Wearable Technologies - Potential Opportunities and Deployment Challenges in Manufacturing and Warehousing

What GAO found

Certain wearable technologies (wearables) may provide some benefits to workers experiencing musculoskeletal pain or discomfort, such as back pain, but GAO found limited evidence to support wearables' ability to reduce injuries. GAO examined the effects on worker safety of two of the most commonly deployed wearable technologies in manufacturing and warehousing: exoskeletons and ergonomic sensors.

Exoskeletons are designed to reduce muscular fatigue and injuries by providing support to specific muscle groups. Laboratory studies generally show that exoskeletons can reduce muscle strain in a controlled environment. Deployments in the workplace, however, have produced limited public studies demonstrating a reduction in worker injuries, in part due to the short duration of many field studies.

Ergonomic sensors are designed to detect postures or motions that could cause injury. Ergonomic sensor manufacturers have self-reported case studies with improved safety outcomes. GAO, however, found limited evidence that current ergonomic sensors improve worker safety, in part because multiple factors contribute to musculoskeletal injuries and posture measurements alone may not accurately predict risk. Stakeholders have described several challenges from their past experiences deploying exoskeletons and ergonomic sensors.

For example:

• Workers expressed concerns about the practicality of wearables. Workers are more likely to use wearables that are comfortable and convenient for their jobs.

• Warehousing and manufacturing company representatives expressed that they may prefer to deploy other injury hazard controls—such as elimination or substitution—before considering wearables. For example, providing a lift table to eliminate a worker's need to lift objects may be more effective at preventing injuries than using a back-support exoskeleton.

• Many stakeholder groups voiced concerns about data that some wearables may collect, particularly regarding data ownership, privacy, and security.

The wearables market is evolving quickly. Stakeholders told GAO they need more time to assess how well ongoing efforts address these challenges. GAO identified a set of ongoing activities that stakeholder groups (such as wearables manufacturers and companies interested in deploying wearables) are undertaking.

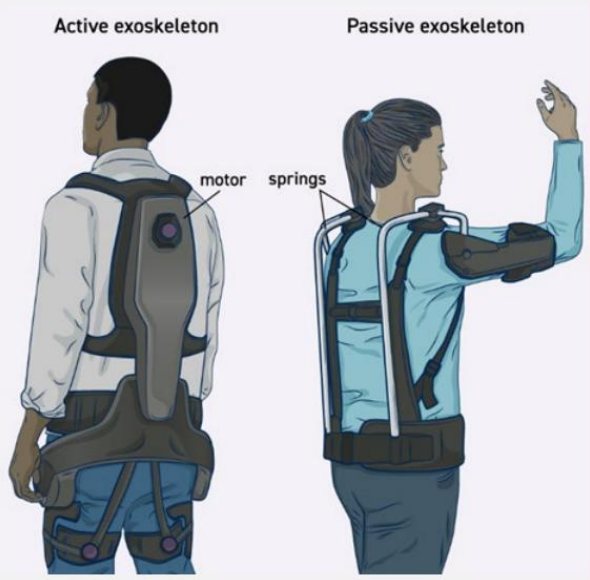
These activities include collecting additional data on accuracy and efficacy of wearables and gathering worker feedback as wearables are deployed. Additionally, national consensus committees are currently developing standards to address these challenges. Stakeholders told GAO that continuing these activities may address current challenges and did not favor other policy actions, such as additional standards and regulations.

Passive and active exoskeletons

Exoskeletons can be passive or active, depending on whether the system uses an onboard battery. Passive systems have springs and dampers that provide a counterforce to relieve the strain on targeted muscle groups, such as a worker's shoulders. Some models include an adjustment to change the tension and provide more or less support.

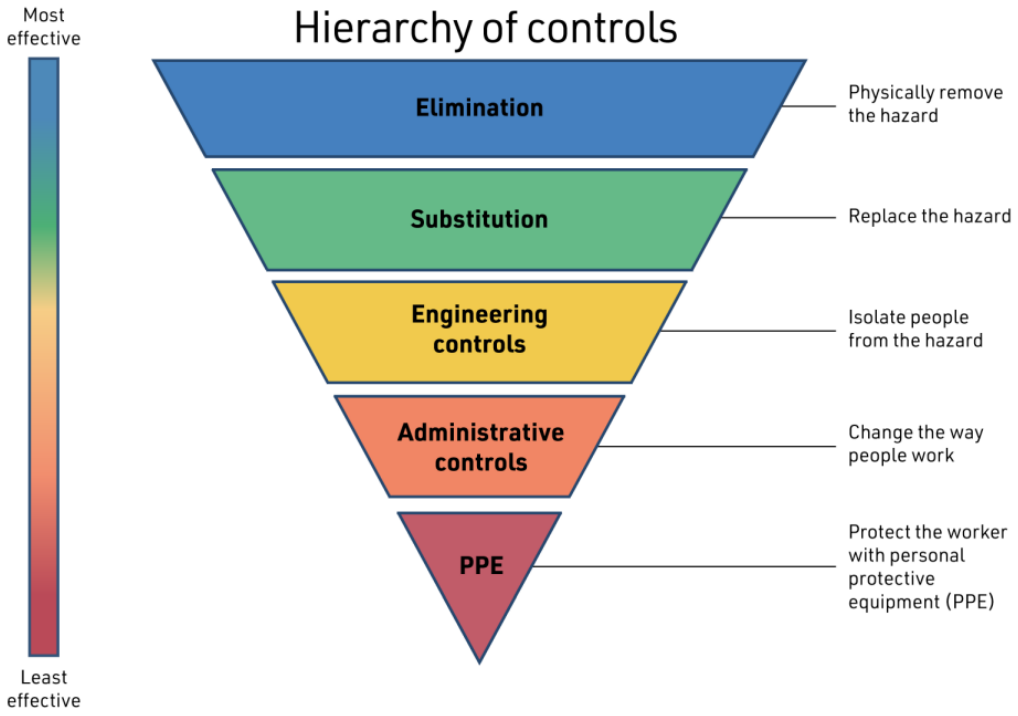
By contrast, active systems use battery-powered motors in the suit to adjust the level of support depending on the worker's movements. For example, an active suit can vary support depending on how fast the worker moves to make a lift or bend. In general, active exoskeletons are designed for heavier-than-normal lifts, but these devices also tend to weigh and cost more.

In our site visits and discussions with deploying companies, we found they predominantly used passive exoskeletons, but some stakeholders noted that active systems may be deployed more frequently outside the U.S. In particular, one manufacturer of active exoskeletons said they have deployed systems primarily in Europe and had only recently begun to expand to the U.S. market.



Source: GAO (analysis and illustration). | GAO-25-107213

Figure 2: The hierarchy of controls to reduce or remove workplace hazards



Source: GAO adaptation of National Institute for Occupational Safety and Health figure. | GAO-25-107213

United States Government Accountability Office

Report to the Ranking Member
Committee on Health, Education, Labor and Pensions
U.S. Senate

Table of Contents

To read more: https://www.gao.gov/assets/gao-25-107213.pdf

AI Cybersecurity Collaboration Playbook

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

The AI Cybersecurity Collaboration Playbook provides guidance to organizations across the AI community –including AI providers, developers, and adopters – for sharing AI-related cybersecurity information voluntarily with the Cybersecurity and Infrastructure Security Agency (CISA) and other partners through the Joint Cyber Defense Collaborative (JCDC).

While focused on strengthening collaboration within JCDC, the playbook also identifies actionable information sharing categories applicable to broader critical infrastructure stakeholders and other sharing mechanisms.

CISA encourages organizations to adopt the playbook's guidance to enhance their own information-sharing practices, contributing to a unified approach to AI-related cybersecurity threats across critical infrastructure.

This playbook aims to:

- Facilitate collaboration between federal agencies, private industry, international partners, and other stakeholders to raise awareness of AI cybersecurity risks and improve the resilience of AI systems.
- Guide JCDC partners on how to voluntarily share information related to cybersecurity incidents and vulnerabilities associated with AI systems.
- Delineate information sharing protections and mechanisms.
- Outline CISA's actions upon receiving shared information to strengthen collective defense.

AI safety topics, such as risks to human life, health, property, or the environment, are outside the intended scope of the JCDC AI Cybersecurity Collaboration Playbook. Stakeholders should address any risks or threats involving human life, health, property,

or the environment in a timely and appropriate manner, in accordance with their own applicable process or procedures for such events.

Similarly, issues related to AI fairness and ethics are also outside the scope of this playbook. This playbook does not create policies, impose requirements, mandate actions, or override existing legal or regulatory obligations.

All actions taken under this playbook are voluntary. This playbook will undergo periodic updates, evolving to address these challenges through active collaboration among government, industry, and international partners.

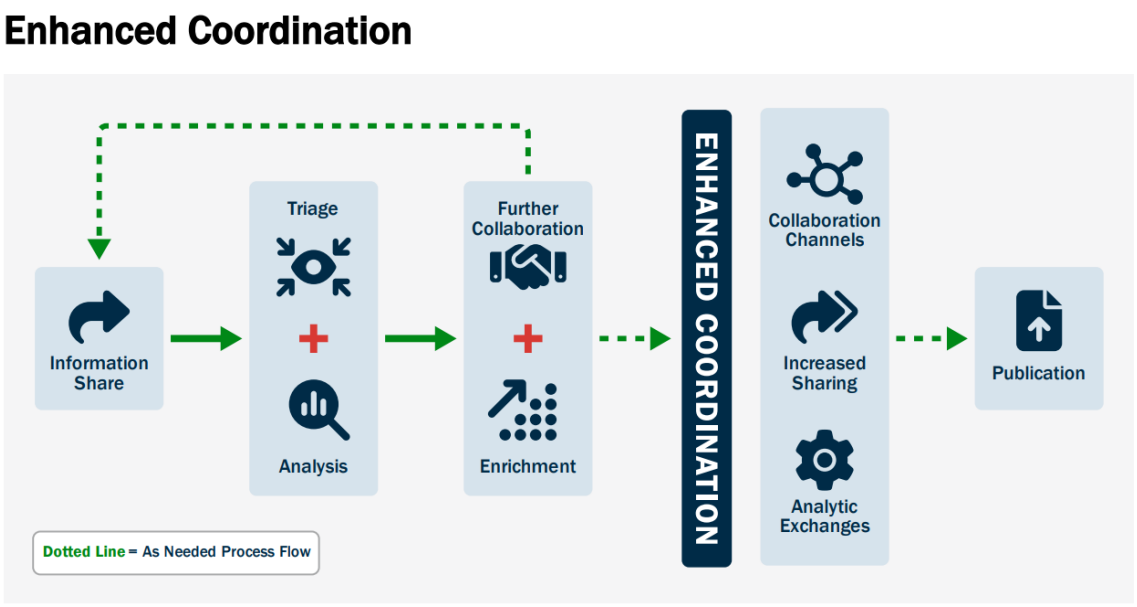


Figure 3: CISA Information Sharing and Collaboration Process

To read more: https://www.cisa.gov/news-events/news/cisa-jcdc-government-and-industry-partners-publish-ai-cybersecurity-collaboration-playbook

https://www.cisa.gov/sites/default/files/2025-01/JCDC%20AI%20Playbook.pdf

Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products

The Cybersecurity and Infrastructure Security Agency (CISA) and partners warn that cyber threat actors, when compromising operational technology (OT) components, target specific OT products rather than specific organizations.

Many OT products are not designed and developed with Secure by Design principles and commonly have weaknesses, such as weak authentication, known software vulnerabilities, limited logging, insecure default settings and passwords, and insecure legacy protocols.

You may visit: https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf

Cyber threat actors can easily exploit these weaknesses across multiple victims to gain access to control systems.

When security is not prioritized nor incorporated directly into OT products, it is difficult and costly for owners and operators2 to defend their OT assets against compromise.

This Secure by Demand guide, authored by CISA with contributions from the following partners, describes how OT owners and operators should integrate security into their procurement process when purchasing industrial automation and control systems as well as other OT products.

OVERVIEW: VULNERABLE BY DESIGN

Technology is integrated into nearly every facet of daily life, as internet facing systems increasingly connect us to critical systems that directly impact our economic prosperity, livelihoods, and even health, ranging from personal identity management to medical care. One example of the disadvantage of such conveniences are the global cyber breaches resulting in hospitals canceling surgeries and diverting patient care. Insecure technology and vulnerabilities in critical systems may invite malicious cyber intrusions, leading to potential safety[1] risks.

As a result, it is crucial for software manufacturers to make secure by design and secure by default the focal points of product design and development processes. Some vendors have made great strides driving the industry forward in software assurance, while others continue to lag behind. The authoring organizations strongly encourage every technology manufacturer to build their products based on reducing the burden of cybersecurity on customers, including preventing them from having to constantly perform monitoring, routine updates, and damage control on their systems to mitigate cyber intrusions. We also urge the software manufacturers to build their products in a way that facilitates automation of configuration, monitoring, and routine updates. Manufacturers are encouraged to take ownership of improving the security outcomes of their customers. Historically, software manufacturers have relied on fixing vulnerabilities found after the customers have deployed the products, requiring the customers to apply those patches at their own expense. Only by incorporating secure by design practices will we break the vicious cycle of constantly creating and applying fixes. **Note:** The term "secure by design" encompasses both secure by design and secure by default.

To accomplish this high standard of software security, the authoring organizations encourage manufacturers to prioritize the integration of product security as a critical prerequisite to features and speed to market. Over time, engineering teams will be able to establish a new steady-state rhythm where security is truly designed-in and takes less effort to maintain.

Reflecting this perspective, the European Union reinforces the importance of product security in the Cyber Resilience Act, emphasizing that manufacturers should implement security throughout a product's life-cycle in order to prevent manufacturers from introducing vulnerable products into the market.

When procuring products, OT owners and operators should select products from manufacturers who prioritize the following security elements:

1. Configuration Management: The product supports controlling and tracking modifications to configuration settings and engineering logic. Seek out manufacturers whose products backup and deploy system configurations in a secure and simple manner.

2. Logging in the Baseline Product: The product supports logging of all actions—including changes to configuration, security events, and safety events—in the baseline

versions using open standard logging formats. Seek out products that come with standardized access and change logs for building incident response capabilities.

3. Open Standards: The product uses open standards to support secure functions and services and for migrating configuration settings and engineering logic. Seek out products that support open, interoperable standards to facilitate replacing or adding products.

4. Ownership: The product gives owners and operators full autonomy over said product, including maintenance and changes. Seek out products that enable operator autonomy while minimizing dependency on the vendor.

5. Protection of Data: The product protects the integrity and confidentiality of data, services, and functions, including a product's configuration settings and engineering logic. Seek out products that treat operational data as valuable and protect it at rest and during transit to and from vendors and manufacturers.

6. Secure by Default: The product is delivered secure out of the box, reducing the attack surface and removing the burden on owners and operators. Seek out products that include all security features in all versions; eliminate default passwords; allow for appropriate length and complexity for passwords; use secure up-to-date versions of protocols with older insecure protocols (e.g., SNMPv1/2, Telnet, SSL, TLS 1.0/1.1) disabled by default; do not unnecessarily expose external interfaces; and provide authorized users the ability to reset product configuration to its original state.

7. Secure Communications: The product supports secure authenticated communication with digital certificates deployed that fail loudly (e.g., when a certificate expires) but allows critical processes to continue. Seek out products that simplify digital certificate deployment and renewal such that operators do not need to be cyber experts to achieve secure authenticated communications.

8. Secure Controls: The product is resilient to threat actors sending malicious emergency, safety, or diagnostic commands; protects the availability of essential functions; withstands active security scanning; and minimizes the impact of an incident on the overall system. Seek out manufacturers who can demonstrate trusted safety-critical controls and explain how operators can continuously verify and regain that trust.

9. Strong Authentication: The baseline version of the product, especially safety-critical equipment, protects against unauthorized access through appropriate control measures, including role-based access control and phishing-resistant multifactor authentication. Seek out manufacturers that have eliminated the use of shared role-based passwords in their products.

10. Threat Modeling: The product has a full and detailed threat model. Seek out products that have an up-to-date threat model that articulates the ways in which it might be compromised, along with security measures implemented to reduce these threat scenarios.

11. Vulnerability Management: The manufacturer has a comprehensive vulnerability management regime in which products are rigorously tested to help ensure they contain no known exploitable vulnerabilities. Each product has a clearly defined support period during which vulnerabilities are managed and patches are supplied free of charge. Seek out manufacturers who include hardware and software bill of materials with product delivery and who commit to timely remediation of vulnerabilities through a vulnerability disclosure program.

12. Upgrade and Patch Tooling: The product has a well-documented and easy to follow patch and upgrade process and supports moving to a supported operating system version at no extra cost if the original operation system is soon to be no longer supported. Seek out products that can be verified and that support owner-controlled patch management.

To read more: https://media.defense.gov/2025/Jan/13/2003626906/-1/-1/0/JOINT-GUIDE-SECURE-BY-DEMAND-PRIORITY-CONSIDERATIONS-OT-OWNERS-OPERATORS.PDF

Taking legal action to protect the public from abusive AI-generated content

Steven Masada, Assistant General Counsel, Microsoft's Digital Crimes Unit

Microsoft's Digital Crimes Unit (DCU) is taking legal action to ensure the safety and integrity of our AI services. In a complaint unsealed in the Eastern District of Virginia, we are pursuing an action to disrupt cybercriminals who intentionally develop tools specifically designed to bypass the safety guardrails of generative AI services, including Microsoft's, to create offensive and harmful content.

Microsoft continues to go to great lengths to enhance the resilience of our products and services against abuse; however, cybercriminals remain persistent and relentlessly innovate their tools and techniques to bypass even the most robust security measures. With this action, we are sending a clear message: the weaponization of our AI technology by online actors will not be tolerated.

Microsoft's AI services deploy strong safety measures, including built-in safety mitigations at the AI model, platform, and application levels. As alleged in our court filings unsealed today, Microsoft has observed a foreign-based threat–actor group develop sophisticated software that exploited exposed customer credentials scraped from public websites. In doing so, they sought to identify and unlawfully access accounts with certain generative AI services and purposely alter the capabilities of those services.

Cybercriminals then used these services and resold access to other malicious actors with detailed instructions on how to use these custom tools to generate harmful and illicit content. Upon discovery, Microsoft revoked cybercriminal access, put in place countermeasures, and enhanced its safeguards to further block such malicious activity in the future.

This activity directly violates U.S. law and the Acceptable Use Policy and Code of Conduct for our services. Today's unsealed court filings are part of an ongoing investigation into the creators of these illicit tools and services. Specifically, the court order has enabled us to seize a website instrumental to the criminal operation that will allow us to gather crucial evidence about the individuals behind these operations, to decipher how these services are monetized, and to disrupt additional technical infrastructure we find.

At the same time, we have added additional safety mitigations targeting the activity we have observed and will continue to strengthen our guardrails based on the findings of our investigation.

Every day, individuals leverage generative AI tools to enhance their creative expression and productivity. Unfortunately, and as we have seen with the emergence of other technologies, the benefits of these tools attract bad actors who seek to exploit and abuse technology and innovation for malicious purposes.

Microsoft recognizes the role we play in protecting against the abuse and misuse of our tools as we and others across the sector introduce new capabilities. Last year, we committed to continuing to innovate on new ways to keep users safe and outlined a comprehensive approach to combat abusive AI-generated content and protect people and communities. This most recent legal action builds on that promise.

Beyond legal actions and the perpetual strengthening of our safety guardrails, Microsoft continues to pursue additional proactive measures and partnerships with others to tackle online harms while advocating for new laws that provide government authorities with necessary tools to effectively combat the abuse of AI, particularly to harm others. Microsoft recently released an extensive report, "Protecting the Public from Abusive AI-Generated Content," which sets forth recommendations for industry and government to better protect the public, and specifically women and children, from actors with malign motives.

Note: You may visit: https://blogs.microsoft.com/on-the-issues/2024/07/30/protecting-the-public-from-abusive-ai-generated-content/

https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Protecting-Public-Abusive-AI-Generated-Content.pdf

Protecting the Public from Abusive AI-Generated Content

For nearly two decades, Microsoft's DCU has worked to disrupt and deter cybercriminals who seek to weaponize the everyday tools consumers and businesses have come to rely

on. Today, the DCU builds on this approach and is applying key learnings from past cybersecurity actions to prevent the abuse of generative AI.

Microsoft will continue to do its part by looking for creative ways to protect people online, transparently reporting on our findings, taking legal action against those who attempt to weaponize AI technology, and working with others across public and private sectors globally to help all AI platforms remain secure against harmful abuse.

To read more: https://blogs.microsoft.com/on-the-issues/2025/01/10/taking-legal-action-to-protect-the-public-from-abusive-ai-generated-content/

Report on the feasibility for further centralisation of reporting of major ICT-related incidents - Article 21 of DORA (REGULATION (EU) 2022/2554)

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Executive Summary

1. DORA under article 21 requires that European Supervisory Authorities (ESAs) prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for ICT-related incident reporting.

To this end, this report presents the results of the study performed to understand and assess the options of further centralisation of incident reporting under DORA. This study has also been carried out concurrently with the drafting of DORA technical standards on incident reporting.

2. Considering the DORA legal mandate for this work, the report serves as a guide for exploration and comprehension of further centralisation of incident reporting.

Accordingly, the report aims at informing any further discussions towards centralisation of incident reporting and thus any future decision to set up a further centralised solution would require further technical implementation studies and DORA amendments.

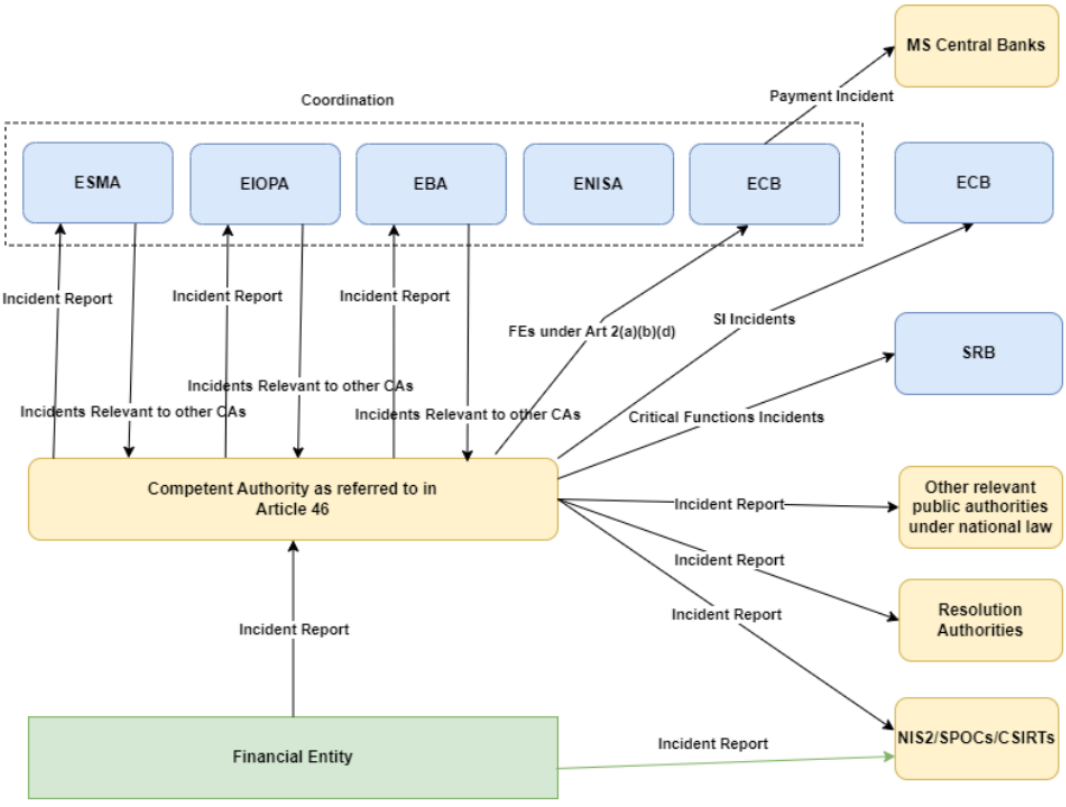


FIGURE 1 INCIDENTS DATA FLOW UNDER DORA

Contents

3. The report was prepared by the ESAs in collaboration with the Competent Authorities (CAs), who provided significant input in view of their existing experience and incident reporting solutions. The ESAs also collaborated closely with the European Central Bank (ECB) and Single Resolution Board (SRB), as per the DORA mandate, they are key stakeholders and receivers of incidents in the DORA reporting regime.

Further, the European Union Agency for Cybersecurity (ENISA) also participated due to its expertise in cybersecurity and its EU role particularly in incident reporting and management. This collaborative approach ensured a comprehensive perspective, drawing on the insights from both financial and cybersecurity viewpoints.

4. The structure of the report mirrors the methodology used to perform this feasibility study. It includes a thorough analysis of the DORA legal basis and the incident reporting flows and roles and responsibilities established therein, comprehensive stock-taking exercises both on existing incident reporting regimes in the financial sector at EU level, as well as different available solutions, the general minimum high level requirements of

an incident reporting system, the identification of the three scenarios to be assessed, the assessment based on the elements identified in Article 21(2) and the subsequent cost and benefit analysis, as well as the overall conclusion. The report thus presents comprehensive information on each of these elements, with additional supporting information and analyses in the technical annexes.

5. The identification of the different scenarios with increasing levels of centralisation, as well as the definition of the baseline scenario, are derived from DORA, particularly Recital 55 and Article 21:

a. the baseline,

b. the data sharing (baseline encompassing also other national authorities, such as the NIS authorities); and

c. the fully centralised model (single EU hub).

6. The baseline scenario is the model which implements the existing DORA incident reporting flows, as per Article 19, and which according to DORA should be operational from 17 January 2025.

This model remains largely decentralised, where financial entities report directly to the designated competent authorities in accordance with the reporting modalities and tools in place at national level. The competent authorities then transmit these reports onwards to other national and European authorities, with the ESAs then disseminating the incidents to relevant competent authorities.

7. The data sharing is a model based on the baseline solution, but where financial entities (FEs) would continue to report to the competent authority responsible for their supervision, in accordance with the reporting modalities and tools in place at national level.

The main difference, however, is that in this scenario, decentralised dissemination is no longer required. Once the report is submitted to the single solution available to competent authorities, it is automatically disseminated both nationally and at the European level to the relevant stakeholders, according to their respective responsibilities.

8. The fully centralised model envisages financial entities reporting directly to the EU hub, which is accessible to stakeholders based on their specific roles and responsibilities and from which they receive notifications. This model also allows for the development of enhanced analytical capabilities, eliminating the need to duplicate such capabilities at a decentralised level.

In this scenario, while the financial entities will report onto a centralised system, the competent authorities are still expected to be a first point of contact from the perspective of supervisory engagement, response, and follow-up. This solution would aim at facilitating the collection, dissemination and offering of advanced analytical capabilities of the incidents and at creating efficiencies at EU level.

9. The assessment across these three models was performed considering the elements identified in Article 21(2) on technical and legal prerequisites for the establishment of the EU hub, limitations and risks , especially related to the high concentration of sensitive information, capabilities to ensure interoperability with other reporting schemes, operational management, conditions of membership, technical arrangements

for access of financial entities and national competent authorities, and preliminary assessment of financial costs incurred.

10. The report also identified the key limitations of the analysis, in view of important known unknowns at the time that the assessment was performed. Specifically, those relate to unknown number of total major ICT-related incidents expected, unknown specific design and development needs, interoperability with NCAs IT systems used for supervisory response and follow-up, and unknown timelines for the decision to move to a fully centralised solution.

To read more: https://www.eba.europa.eu/sites/default/files/2025-01/7249d67f-250d-48ae-9cf5-4a2c1a10c7cf/JC%202024%20108_Report%20on%20the%20feasibility%20for%20further%20Centralisation%20of%20reporting%20of%20major%20ICT%20incidents_%20(002).pdf

Artificial Imagination

A Brookhaven Lab researcher has conceptualized an "exocortex," an extension of the human brain that will generate inspiration and imagination for scientific discovery
By Stephanie Kossman and Danielle Roedel

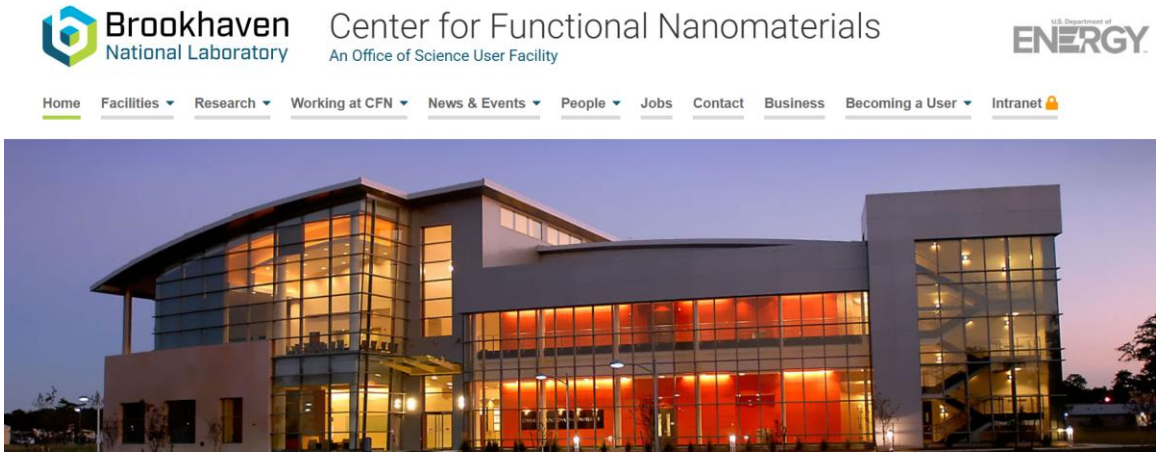
Brookhaven National Laboratory

Artificial intelligence (AI) once seemed like a fantastical construct of science fiction, enabling characters to deploy spacecrafts to neighboring galaxies with a casual command. Humanoid AIs even served as companions to otherwise lonely characters.

Now, in the very real 21st century, AI is becoming part of everyday life, with tools like chatbots available and useful for everyday tasks like answering questions, improving writing, and solving mathematical equations.

AI does, however, have the potential to revolutionize scientific research — in ways that can feel like science fiction but are within reach.

At the U.S. Department of Energy's (DOE) Brookhaven National Laboratory, scientists are already using AI to automate experiments and discover new materials. They're even designing an AI scientific companion that communicates in ordinary language and helps conduct experiments. And Kevin Yager, the Electronic Nanomaterials Group leader at the Center for Functional Nanomaterials (CFN), has articulated an overarching vision for the role of AI in scientific research.



It's called a science **exocortex** — "exo" meaning outside and "cortex" referencing the information processing layer of the human brain. Rather than simple chatbots and scientific assistants, the conceptualized exocortex will be an extension of a scientist's brain. Researchers will interact with it through conversation, without the need for any invasive brain-computer interfaces.

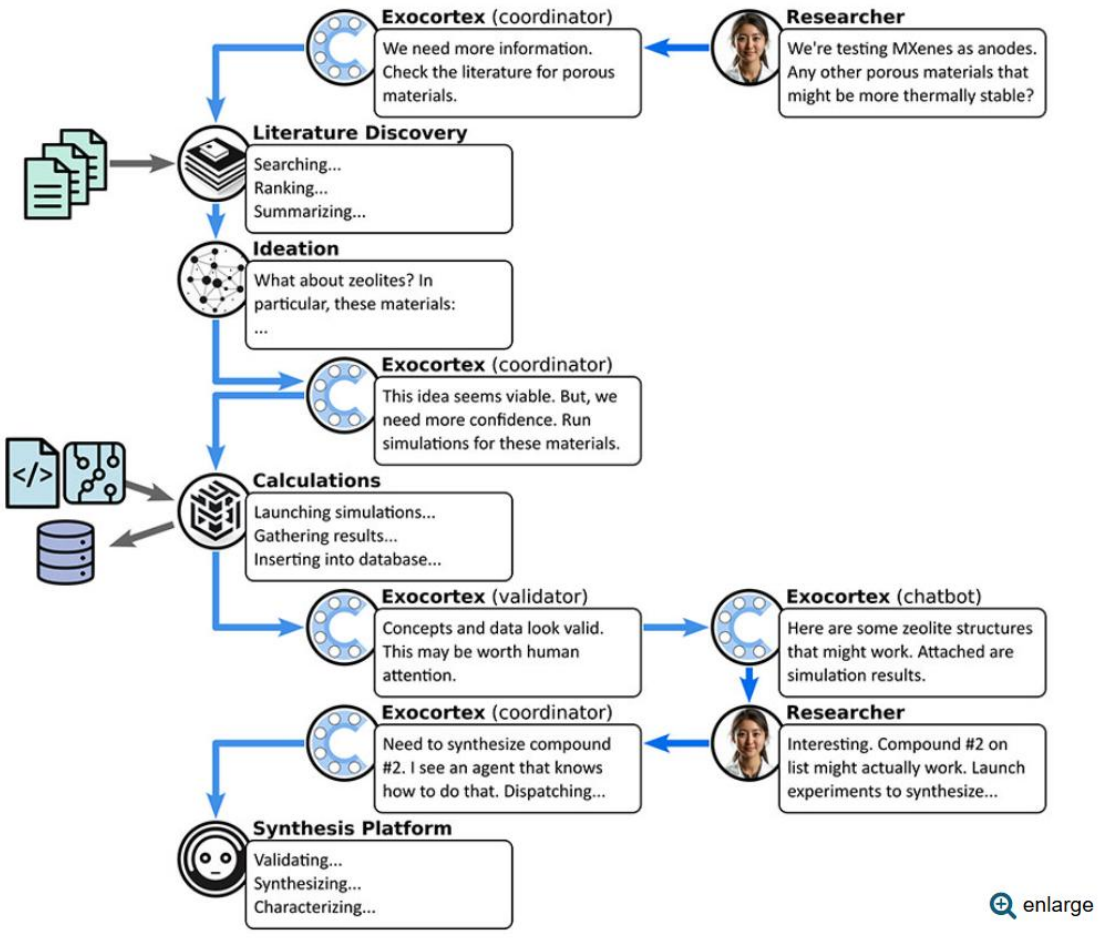
Extending the human brain

"An exocortex, realized through software, would serve as a new source of thinking, inspiration, and imagination," said Yager, whose vision was recently published in Digital Discovery. "If we design and build the exocortex correctly, our interactions with it will feel like those 'aha' moments we sometimes have upon waking from sleep or while

otherwise ruminating on a problem. You won't check in with an exocortex; you'll experience it."

Yager describes the exocortex as analogous to the layers of the human brain, which developed through the course of human evolution. Over millions of years, the human brain became the information processing masterpiece it is today by accumulating new layers, each one more sophisticated than the last. The bottom of the brain controls basic survival functions, like breathing. Other, more advanced layers tackle increasingly complicated functions, like emotional regulation and language processing. Most importantly, all facets of the brain work together in harmony to form "the human experience."

"Technologically, we have the potential now to add another, external layer to the brain — one that connects us to AI," Yager said. "And just like the specialized regions of the brain that coordinate with each other to give emergence to what we call intelligence, the exocortex will integrate individualized AI capabilities to solve a problem or generate creativity."



This diagram conveys how information may flow between a researcher and their exocortex — and between the individual AI agents that make up the exocortex. In this example, a materials scientist asks their exocortex a question about battery materials. Then, the exocortex prompts the constituent AIs to work on the problem, and each contributes their area of expertise. These example interactions are just a small sample, as real conversations would be long and complex. (Kevin Yager/Brookhaven National Laboratory).

Note: Brookhaven National Laboratory delivers discovery science and transformative technology. Primarily supported by the U.S. Department of Energy's (DOE) Office of Science, Brookhaven Lab is a multidisciplinary laboratory with seven Nobel Prize-winning discoveries, 37 R&D 100 Awards, and more than 70 years of pioneering research. The Laboratory's 2,500-plus staff members lead and support diverse research teams that address the DOE mission to ensure the nation's security and prosperity by addressing its energy, environmental, and nuclear challenges through transformative science and technology solutions. Among Brookhaven Lab's current initiatives are nuclear science, energy science, data science, particle physics, accelerator science and technology, quantitative plant science, and quantum information science.

An "app store" of AI agents

Compared to the average chatbot, which is a single AI system, the exocortex would be a collection of dozens of AI agents working together — customized to a researcher's individual needs.

Each agent would be trained to carry out specific science-related tasks. A scientific literature agent, for example, could sift through published papers to find an optimal protocol for an experiment, while another AI agent collects and analyzes data from a running experiment. Additional agents could launch experiments or simulations, compare findings to previous studies, or even propose ideas for subsequent experiments.

All of the agents' tasks will happen in concert, simultaneously, and without manual intervention, culminating in new insights delivered to the human researcher.

One design aspect of Yager's proposed exocortex is that the AI agents will communicate with one another in plain English language. This will enable human scientists to study and audit the chains of decisions that lead to a particular AI outcome, providing much-needed opportunities to assess accuracy and exert engineering control.

Yager says the task of building an exocortex is enormous, and the developmental effort should be shared among scientists worldwide, so individual research groups can leverage their own expertise to design new agents. Ideally, scientists will one day have "an app store" from which they can download AI agents that will enhance the abilities of their own exocortex, similar to how downloading new apps adds functionality to phones. Individual AI "apps" could also be efficiently updated and replaced.

"I expect to see a multiplicative effect," explained Yager. "As scientists simultaneously improve the individual AIs and the foundational exocortex technology, the capabilities of the exocortex will likely grow much faster than people expect."

Of course, making the exocortex a reality won't be easy. While scientists have designed a plethora of AIs that can interface with a user and complete specific tasks, building a network of AIs that can interact with each other is an entirely new challenge.

Yager expects each AI agent to require access to a "catalog" of the other agents and their specialized abilities, so they each can send messages describing the work they've done and explaining what they need from other AI agents.

"No one knows how to do this yet," Yager said. Among the challenges is determining the ideal organization of agents. "Should it be a hierarchy where there is a chief with leaders and employees, like how a company operates? Or should it be more fluid, so the AIs figure out the workflow themselves? There is no obvious answer, and this is an exciting research question about the exocortex design that we are investigating."

The final output of the exocortex will be a result of some sequence of decisions, planning, execution, verification, and summarization, rather than the simple text that a generative chatbot outputs. This extra iteration, promoted by the communication between AI agents and the exocortex structure, will ultimately improve the output and make the AI even more intelligent.

To read more:
https://www.bnl.gov/newsroom/news.php?a=122257

Joint Report - Recent developments in crypto-assets

Executive Summary

1. This report sets out the outcome of the analysis undertaken by the EBA and ESMA on specific elements covered by Article 142 of MiCAR and constitutes the EBA and ESMA's contribution to the production of the EC's report to the European Parliament and Council on recent developments in crypto assets. The analysis has been informed by extensive research on DeFi and crypto lending, borrowing and staking.

2. The report is of analytical nature and does not set out any specific policy recommendations or legislative proposals to the EC or co-legislators. In addition, it makes use of terms proposed by the industry, such as "centralised" and "DeFi protocols", which should not be interpreted as a view of the actual level of (de)centralisation for the purposes of recital 22 of MiCAR.

3. The first chapter of the report is focused on DeFi, including the engagement of EU consumers and businesses into DeFi. It finds that DeFi remains a niche phenomenon, with amounts locked in DeFi protocols representing 4% of all crypto-asset market value at the global level. It also finds that EU adoption of DeFi, while above global average, is behind other developed economies (e.g. the US, South Korea).

The report sets out the different types of businesses providing access to DeFi, namely DeFi application interfaces, self-custodial wallets, and centralised platforms, and finds that the preferred method of access to DeFi depends on the activity.

Lastly, the chapter delves into risks associated with DeFi (mainly ICT risks, as requested by the EC, and ML/TF risks, due to their relevance) and assesses the implications of maximal extractable value (MEV) on DeFi markets.

4. The report finds that the number of DeFi hacks and the value of stolen crypto assets has generally evolved in correlation with the DeFi market size.

While historically the majority of DeFi hacks have stemmed from on-chain vulnerabilities (mainly through the exploit of smart contract vulnerabilities), recent attacks on DeFi appear to be more successful when exploiting off-chain vulnerabilities (e.g. compromising users' private keys).

The report also finds that DeFi protocols present significant risks of ML/TF, with flows on decentralised exchanges representing 10% of spot crypto trading volumes globally. This is mainly due to the current absence of adequate AML/CFT controls, which means that users can transact in practice without being identified and verified.

The risk is increased due to the cross-border nature of transactions as the funds or crypto-assets from potentially illegitimate sources can be transferred via DeFi without any obligations on the protocols to perform AML/CFT checks on such funds or crypto-assets and report them to Financial Intelligence Units. The report identifies some initiatives to apply KYC in DeFi protocols.

In relation to MEV, the report concludes that these activities are widespread in DeFi because of the decentralised nature of the underlying blockchain. However, mitigating the negative externalities of MEV requires further consideration of technical solutions.

5. The second chapter sets out a description of the business models present in the market for the lending, borrowing and staking of crypto assets. For each of the three types of services, the report analyses the main types and most typical features of the business models observed in the market, regarding both centralised and decentralised forms.

The report finds that crypto lending, borrowing and staking services are offered by a number of CASPs in EU jurisdictions, which in some cases also offer regulated crypto-asset services.

In provision of services under assessment, the report finds that users may receive insufficient information on conditions in relevant areas such as fees, interest rates paid or yields, changes to collateral requirements, the actions the service provider may take with regard to any assets used as collateral or placed in a staking account, or rights and liabilities in case of dispute or insolvency.

The chapter then sets out the existing (limited) evidence of the engagement of EU consumers and financial institutions with those services and sets out the specific risks associated with each of them.

Finally, it assesses the risks associated with crypto lending, borrowing and staking, such as excessive leverage, information asymmetries, exposure to ML/TF risks, and systemic risks arising from re-hypothecation and collateral chains, procyclicality and interconnectedness.

Box 1. ICT risks associated with the use of DeFi protocols and DORA

To understand to which the extent requirements established under the Digital Operational Resilience Act (DORA)[56] sufficiently address the range of ICT risks associated with a potential use of DeFi by entities in scope of DORA, albeit considering that their engagement is so far minimal (see Section 2.1.3), the EBA and ESMA carried out a survey of NCAs in July 2024.

The majority of responses suggested that while DORA provides a solid framework to enhance the digital operational resilience of regulated financial entities, some risks associated with the engagement with DeFi protocols may require further attention due to the lack of 'entry points' in DeFi contexts. Specifically, DORA applies to regulated financial entities such as credit institutions, insurance companies, CASPs or issuers of ARTs. If these entities were to adopt or integrate DeFi activities (e.g. as briefly explained in Section 2.2, should CASPs facilitate their users' access to DeFi), they may need to ensure compliance with operational resilience and ICT risk management requirements under DORA. However, absent such engagement from regulated financial entities, there may not be relevant addressees for the purposes of DORA applicability where DeFi market participants operate in a fully decentralised manner.

To read more: https://www.eba.europa.eu/sites/default/files/2025-01/5fe168a2-e5a6-41a1-a1b4-87a35ecebb5c/Joint%20Report%20on%20recent%20developments%20in%20crypto-assets%20%28Art%20142%20MiCAR%29.pdf

NIST NCCoE Published Inital Public Draft NIST IR 8374 Revision 1, Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile

The NIST National Cybersecurity Center of Excellence (NCCoE) has published preliminary draft NIST Internal Report (NIST IR) 8374 Revision 1, Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile for public comment.

1 **NIST Internal Report**
2 **NIST IR 8374r1 ipd**

3 **Ransomware Risk Management:**
4 *A Cybersecurity Framework 2.0 Community Profile*

5 Initial Public Draft

6 Murugiah Souppaya
7 William C. Barker
8 William Fisher
9 Karen Scarfone
10

11 This publication is available free of charge from:
12 https://doi.org/10.6028/NIST.IR.8374r1.ipd

Organizations at home and abroad use NIST IR 8374 to guard against ransomware. We are seeking your feedback on the publication's contents and the future direction of NIST's ransomware guidance.

NIST IR 8374 Revision 1 incorporates content from Cybersecurity Framework (CSF) 2.0—the updated version of CSF 1.1. The Cybersecurity Framework 2.0 Community Profile identifies security objectives from NIST CSF 2.0 that support managing, detecting, responding to, and recovering from ransomware events.

You can also use this publication to gauge your organization's readiness to counter ransomware threats, mitigate potential consequences of a ransomware event, and develop a ransomware countermeasure playbook.

Share Your Feedback - The public comment period is open now until March 14, 2025. Please send your feedback about this publication and what content would be most valuable in future NIST ransomware guidance to ransomware@nist.gov.

BASIC RANSOMWARE TIPS

Even without undertaking all the measures described in this Ransomware Community Profile, there are some basic preventative steps that an organization can take now to protect against and recover from the ransomware threat. These include:

1. Educate employees on avoiding ransomware infections.

- **Don't open files or click on links from unknown sources** unless you first run an antivirus scan or look at links carefully.
- **Avoid using personal websites and personal apps** – like email, chat, and social media – from work computers.
- **Don't connect personally owned devices to work networks without prior authorization.**

2. Avoid having vulnerabilities in systems that ransomware could exploit.

- **Keep relevant systems fully patched.** Run scheduled checks to identify available patches and install these as soon as feasible.
- **Employ zero trust principles in all networked systems.** Manage access to all network functions, and segment internal networks where practical to prevent malware from proliferating among potential target systems.
- **Allow installation and execution of authorized apps only.** Configure operating systems and/or third-party software to run only authorized applications. This can also be supported by adopting a policy for reviewing, then adding or removing authorized applications on an allow list.
- **Inform your technology vendors of your expectations** (e.g., in contract language) that they will apply measures that discourage ransomware attacks.

3. Quickly detect and stop ransomware attacks and infections.

- **Use malware detection software, such as antivirus software at all times.** Set it to automatically scan emails and flash drives.
- **Continuously monitor** directory services (and other primary user stores) for indicators of compromise or active attack.
- **Block access to untrusted web resources.** Use products or services that block access to server names, IP addresses, or ports and protocols that are known to be malicious or suspected to be indicators of malicious system activity. This includes using products and services that provide integrity protection for the domain component of addresses (e.g., hacker@poser.com).

4. Make it harder for ransomware to spread.

- **Use standard user accounts** with multi-factor authentication versus accounts with administrative privileges whenever possible.
- **Introduce authentication delays or configure automatic account lockout** as a defense against automated attempts to guess passwords.
- **Assign and manage credential authorization** for all enterprise assets and software and periodically verify that each account has only the necessary access following the principle of least privilege.
- **Store data in an immutable format** (so that the database does not automatically overwrite older data when new data is made available).
- **Allow external access to internal network resources via secure virtual private network (VPN) connections only.**

5. Make it easier to recover stored information from a future ransomware event.

- **Make an incident recovery plan.** Develop, implement, and regularly exercise an incident recovery plan with defined roles and strategies for decision making. This can be part of a continuity of operations plan. The plan should identify mission-critical and other business-essential services to enable recovery prioritization, and business continuity plans for those critical services.
- **Back up data, secure backups, and test restoration.** Carefully plan, implement, and test a data backup and restoration strategy—and secure and isolate backups of important data.
- **Keep your contacts.** Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement, legal counsel, and incident response resources.

Abstract

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. Attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public.

This Cybersecurity Framework (CSF) 2.0 Community Profile identifies the security objectives from the NIST CSF 2.0 that support governing management of, identifying, protecting against, detecting, responding to, and recovering from ransomware events.

The Profile can be used as a guide to managing the risk of ransomware events. That includes helping to gauge an organization's level of readiness to counter ransomware threats and to deal with the potential consequences of events. This Profile can be leveraged in developing a ransomware countermeasure playbook.

View the publication here:
https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8374r1.ipd.pdf

To read more: https://www.nccoe.nist.gov/news-insights/nist-nccoe-published-inital-public-draft-nist-ir-8374-revision-1-ransomware-risk

Call for action
Urgent plan needed to transition to post-quantum cryptography together

On 7 February 2025, Europol hosted a Quantum Safe Financial Forum (QSFF) event, during which the QSFF has issued a call to action for financial institutions and policymakers, urging them to prioritise the transition to quantum-safe cryptography. With the rapid advancement of quantum computing, the financial sector faces an imminent threat to its cryptographic security.

This transition presents both a challenge and an opportunity to enhance cryptographic management practices across the industry. During the event, representatives from leading organisations discussed the need to urgently address the transition and the challenges industry peers, vendors, policymakers, and society are facing.

EXECUTIVE SUMMARY

Modern cryptography is fundamental to securing the financial ecosystem. The emergence of quantum computers capable of breaking current cryptographic methods presents a challenge to the entire financial ecosystem.

Addressing this challenge requires a transition to postquantum cryptography (PQC). This transition also presents an opportunity to enhance cryptography management practices. Achieving this complex goal requires immediate action and a coordinated effort involving industry peers, vendors, policymakers, and society.

The Quantum Safe Financial Forum (QSFF) is committed to supporting companies and policymakers in the transition to a quantum-safe financial sector. The Quantum Safe Financial Forum recognises the growing global awareness of the quantum threat. However, without a common approach, the financial industry could face increased complexity and costs.

QSFF recommendations:

1. Financial institutions and policymakers should prioritise the transition to quantumsafe cryptography and actively support its implementation.

2. Coordination among different stakeholders will be key; ensuring alignment on their planning, roadmaps and the concrete implementation of the transition to PQC, establishing common goals and a shared view of the requirements to achieve them.

3. There is no need for additional legislation to be made; a voluntary framework established between regulators and the private sector would be sufficient to set guidelines for quantum-safe cryptography and promoting standardisation across institutions.

4. This transition presents an opportunity to enhance cryptography management practices. A forward-looking framework to cryptography management is needed.

5. Promoting collaboration, knowledge sharing and fostering a cohesive approach across jurisdictions at global scale is key to a secure transition. This means encouraging the industry — including the private and public sector actors — to partner up in the context

of quantum-safe experiments, projects, Points of Contact (POCs) and any other relevant initiatives.

INTRODUCTION: THE THREAT QUANTUM COMPUTERS POSE TO CRYPTOGRAPHY

The development of the information society has been made possible due to the widespread use of cryptographic techniques, which ensure authentication, integrity, and confidentiality in digital communications and processes. The financial industry relies heavily on cryptography to provide secure services to customers and society.

Quantum computers, while offering exciting opportunities to solve complex problems, also pose significant challenges. A sufficiently advanced quantum computer could break current public key cryptographic algorithms, compromising the confidentiality of internet communications and the integrity of digital contracts.

These challenges have been identified by Europol and presented in the First Report on Encryption, published by the EU Innovation Hub, and The Second Quantum Revolution report, published by Europol's Innovation Lab. Even though these reports focus on the law enforcement perspective, there are synergies that can also be applied to the financial industry.

For the financial industry, the advent of quantum computers poses a risk to customer confidentiality and peer communications, authentication processes, and trust in digital signatures which enable dynamic legal agreements. Quantum computers capable of posing such threats are expected to be available within the next 10 to 15 years, though this timeline could accelerate due to intense interest from both the public and private sectors.

Public institutions have already started to address this transition

In Europe: The Digital Operational Resilience Act (DORA regulation) establishes requirements to improve cryptography management in the financial sector. It entered into force on 16 January 2023. The European Commission released a recommendation on a "Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography", which encourages EU member states to coordinate efforts among relevant stakeholders, public and private, including Europol. ◦

In the UK: The Financial Conduct Authority (FCA) in collaboration with the World Economic Forum (WEF) produced the report "Quantum Security for the Financial Sector: Informing Global Regulatory Approaches", building on views from regulators, central banks, industry players and academia. The report identifies four guiding principles along with a roadmap to serve as a blueprint to reduce complexity and align stakeholders' activities and calls for an open dialogue between regulatory authorities and industry.

In the USA: the White House has published the "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems".

In Singapore: The Monetary Authority of Singapore (MAS) has issued an advisory to financial institutions urging them to implement quantum security.

To read more:
https://www.europol.europa.eu/cms/sites/default/files/documents/Quantum-safe-financial-forum-2025.pdf

Revisiting COMMISSION RECOMMENDATION (EU) 2024/1101 of 11 April 2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Having regard to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (1) (NIS 2 Directive).

Whereas:

(1) Safeguarding data and securing sensitive communications are vital for Union's society, economy, security and prosperity. Cybersecurity is of strategic importance in building 'Europe Fit for the Digital Age', and a key objective of the Digital Decade policy programme.

(2) The EU Security Union Strategy and the EU Cybersecurity Strategy both highlight encryption as a key technology for achieving resilience, technological sovereignty and for building operational capacity to prevent cyberattacks. In fact, encryption is essential to the digital world for securing digital systems and transactions, for protecting a series of fundamental rights as well as for securing defence capabilities.

The race pursued by various countries and private entities for developing quantum computing capabilities, and unlocking new potentially rewarding opportunities, poses threats to current cryptographic standards. These standards play a pivotal role in ensuring data confidentiality, and integrity, the protection of sensitive communications, and supporting essential elements of network security.

(3) The future potential development of quantum computers capable of breaking today's encryption makes it necessary for Europe to look for stronger safeguards, ensuring the protection of sensitive communications and the long-term integrity of confidential information, i.e., by switching to Post-Quantum Cryptography as swiftly as possible.

This new type of cryptography will remove the known vulnerabilities of current asymmetric cryptography and enhance the robustness against the threats posed by the malicious use of quantum computers.

(4) The Commission has been funding research and development Post-Quantum Cryptography for over a decade, recognizing the potential threat quantum computing poses to present public key cryptography.

(5) Member States should consider migrating their current digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography as soon as possible, inducing a fundamental shift in cryptographic algorithms, protocols and systems. As highlighted in the Commission's recent White

Paper 'How to master Europe's digital infrastructure needs', this requires a coordinated effort involving government agencies, standardization bodies, industry stakeholders, researchers and cybersecurity professionals.

(6) This Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronized transition among the different Member States and their public sectors. The strategy should define clear goals, milestones, and timelines resulting in the definition of a joint Post-Quantum Cryptography Implementation Roadmap.

This should lead to the deployment across the Union of Post-Quantum Cryptography technologies into existing public administration systems and critical infrastructures via hybrid schemes that may combine Post-Quantum Cryptography with existing cryptographic approaches or with Quantum Key Distribution.

(7) For an effective transition to Post-Quantum Cryptography, the Post-Quantum Cryptography Coordinated Implementation Roadmap should provide the list of actions to be addressed by the Member States, including the consideration of Post-Quantum Cryptography algorithms, with a clear timeline for different phases and milestones to be reached, taking into account their interdependencies, as well as the stakeholders to be involved.

(8) For a harmonized implementation of Post-Quantum Cryptography across the Union it is essential to develop common European standards and develop a framework for identifying and selecting Post-Quantum Cryptography algorithms to be deployed in the digital networks and services across the Union.

Through the active participation of EU-funded researchers, the Union is already supporting the development and testing of Post-Quantum Cryptography algorithm candidates for standards in international Post-Quantum Cryptography selection processes.

This Commission Recommendation encourages Member States to work at EU-level closely with the Union's cybersecurity experts, with the NIS Cooperation Group and with the European Union Agency for Cybersecurity (ENISA), on the evaluation and selection of the appropriate Post-Quantum Cryptography algorithms and their adoption as EU standards for a harmonized implementation across the Union.

(9) Member States and the Union should continue to cooperate actively with their international strategic partners in the development of international standards in Post-Quantum Cryptography with a view to ensuring interoperability of communications going forward.

(10) Once agreed by the Member States, the Post-Quantum Cryptography Coordinated Implementation Roadmap should serve as blueprint for the definition of the national transition plans towards Post Quantum Cryptography, or, where national plans exist, their alignment with the common Post-Quantum Cryptography Coordinated Implementation Roadmap.

(11) To ensure progress is made against the objectives of this Recommendation, the Commission intends to monitor closely the actions taken in response to the Recommendation. Member States are therefore encouraged to submit to the Commission, upon its request, all relevant information, which they can reasonably be expected to provide, to ensure such monitoring. On the basis of the information thus obtained and all other available information, the Commission will assess the effects of

this Recommendation and determine whether additional steps, including proposing binding acts of Union law, are required.

(12) This Recommendation on Post-Quantum Cryptography builds on the policy objectives set out in the EU Cybersecurity Strategy for improving the end-to-end security and resilience of the Union's digital infrastructures and services for public administrations and other critical infrastructures; it serves the objectives of the Digital Single Market, and of the Joint Communication on European Economic Security Strategy 10919/23; and it considers the risks to the physical and cyber security of critical infrastructures, as well as those identified under the recently conducted risk assessment for quantum technologies.

It respects the fundamental rights and observes the principles recognized in particular by the EU Charter of Fundamental Rights (Articles 7, 8, and 11) and European Convention on Human Rights (Articles 8 and 10), which imply positive obligations on governments to minimize the risk of unlawful access and control of information, necessitating the safeguarding and promotion of cryptographic technologies.

HAS ADOPTED THIS RECOMMENDATION

1. SCOPE AND OBJECTIVES

The purpose of this Recommendation is to foster the transition to Post-Quantum Cryptography for the protection of digital infrastructures and services for public administrations and other critical infrastructures in the Union by enabling Member States to:

(1) define a 'Post-Quantum Cryptography Coordinated Implementation Roadmap' aimed at synchronising the efforts of Member States to design and implement national transition plans while ensuring cross-border interoperability;

(2) support the evaluation and selection of relevant Post-Quantum Cryptography EU algorithms with the help of cybersecurity experts, and further adoption of such algorithms as Union standards that should be implemented across the Union as part of the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(3) take appropriate and proportionate measures to prepare for this transition.

2. COORDINATED IMPLEMENTATION ROADMAP ADDRESSING THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY

(4) This Recommendation encourages Member States to coordinate their actions at Union level through a dedicated Member States forum. For this purpose, the Commission recommends that Member States take advantage of existing structures at Union level in the area of cybersecurity and establish a sub-group of the NIS Cooperation Group. Such sub-group could include representatives of national security agencies and cybersecurity experts, notably from national cybersecurity authorities and ENISA.

The sub-group may invite representatives of relevant stakeholders to participate in its work such as those of advisory bodies of public organisations, industry, service providers, and operators, with a view to gather input and exchange information on the transition of digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography in different sectors, coordinate their efforts at national level, and develop the Post-Quantum Cryptography Coordinated

Implementation Roadmap, in accordance with the Union competition rules and Union data protection law.

(5) This sub-group on Post-Quantum Cryptography should consider appropriate, effective and proportionate measures for defining and coordinating the development of the Post-Quantum Cryptography Coordinated Implementation Roadmap. The sub-group on Post-Quantum Cryptography is encouraged to engage in discussions with other relevant bodies, such as Europol, NATO, or others, to avoid duplication of efforts and ensure a cohesive approach to addressing emerging challenges.

(6) To this effect, soon after the publication of this Recommendation, Member States are invited to establish such a sub-group on Post-Quantum Cryptography pursuant to Commission Implementing Decision (EU) 2017/179 and to appoint expert representatives who should work in close cooperation with the Commission and who should be tasked to define and develop the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(7) The Post-Quantum Cryptography Coordinated Implementation Roadmap should be available after a period of two years following the publication of this Recommendation, which will be followed by the development and further adaptation of Post-Quantum Cryptography transition plans of individual Member States, in accordance with the principles set out in the Post-Quantum Cryptography Coordinated Implementation Roadmap.

3. ACTIONS AT UNION LEVEL

(8) The overall work will be monitored and assessed periodically by the Commission in cooperation with the expert representatives of the Member States.

(9) To this effect, the Commission may request Member States' representatives to submit all relevant information, which they can reasonably be expected to provide, to ensure the monitoring of the progress achieved in drafting such Post-Quantum Cryptography Coordinated Implementation Roadmap and the effectiveness of such measures.

(10) On the basis of those and all other available information the Commission will assess the designed measures and the operation of the network of Member States' representatives and determine whether additional actions, including proposing binding acts of Union law, are required.

4. REVIEW

(11) Member States should cooperate with the Commission to assess the effects of this Recommendation maximum three years after its publication, with a view to determine appropriate ways forward. This assessment should take into account the outcome of the work by the sub-group on Post-Quantum Cryptography of national experts.

To read more: https://eur-lex.europa.eu/eli/reco/2024/1101/oj/eng

Revisiting US National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

THE WHITE HOUSE

SUBJECT: Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

This memorandum outlines my Administration's policies and initiatives related to quantum computing. It identifies key steps needed to maintain the Nation's competitive advantage in quantum information science (QIS), while mitigating the risks of quantum computers to the Nation's cyber, economic, and national security.

It directs specific actions for agencies to take as the United States begins the multi-year process of migrating vulnerable computer systems to quantum-resistant cryptography. A classified annex to this memorandum addresses sensitive national security issues.

THE WHITE HOUSE

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

BRIEFING ROOM › STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

Section 1. Policy. (a) Quantum computers hold the potential to drive innovations across the American economy, from fields as diverse as materials science and pharmaceuticals to finance and energy.

While the full range of applications of quantum computers is still unknown, it is nevertheless clear that America's continued technological and scientific leadership will depend, at least in part, on the Nation's ability to maintain a competitive advantage in quantum computing and QIS.

(b) Yet alongside its potential benefits, quantum computing also poses significant risks to the economic and national security of the United States. Most notably, a quantum computer of sufficient size and sophistication — also known as a cryptanalytically relevant quantum computer (CRQC) — will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world.

When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions.

(c) In order to balance the competing opportunities and risks of quantum computers, it is the policy of my Administration:

(1) to maintain United States leadership in QIS, through continued investment, partnerships, and a balanced approach to technology promotion and protection; and

(2) to mitigate the threat of CRQCs through a timely and equitable transition of the Nation's cryptographic systems to interoperable quantum-resistant cryptography.

(d) Additional guidance and directives may be required in the future as quantum computing technologies and their associated risks mature.

Sec. 2. Promoting United States Leadership. (a) The United States must pursue a whole-of-government and whole-of-society strategy to harness the economic and scientific benefits of QIS, and the security enhancements provided by quantum-resistant cryptography. This strategy will require a coordinated, proactive approach to QIS research and development (R&D), an expansion of education and workforce programs, and a focus on developing and strengthening partnerships with industry, academic institutions, allies, and like-minded nations.

(b) The United States must seek to encourage transformative and fundamental scientific discoveries through investments in core QIS research programs. Investments should target the discovery of new quantum applications, new approaches to quantum-component manufacturing, and advances in quantum-enabling technologies, such as photonics, nanofabrication, and cryogenic and semiconductor systems.

(c) The United States must seek to foster the next generation of scientists and engineers with quantum-relevant skill sets, including those relevant to quantum-resistant cryptography. Education in QIS and related cybersecurity principles should be incorporated into academic curricula at all levels of schooling to support the growth of a diverse domestic workforce. Furthermore, it is vital that we attract and retain talent and encourage career opportunities that keep quantum experts employed domestically.

(d) To promote the development of quantum technology and the effective deployment of quantum-resistant cryptography, the United States must establish partnerships with industry; academia; and State, local, Tribal, and territorial (SLTT) governments. These partnerships should advance joint R&D initiatives and streamline mechanisms for technology transfer between industry and government.

(e) The United States must promote professional and academic collaborations with overseas allies and partners. This international engagement is essential for identifying and following global QIS trends and for harmonizing quantum security and protection programs.

(f) In support of these goals, within 90 days of the date of this memorandum, agencies that fund research in, develop, or acquire quantum computers shall coordinate with the Director of the Office of Science and Technology Policy to ensure a coherent national strategy for QIS promotion and technology protection, including for workforce issues.

To facilitate this coordination, all such agencies shall identify a liaison to the National Quantum Coordination Office to share information and best practices, consistent with section 102(b)(3) of the National Quantum Initiative Act (Public Law 115-368) and section 6606 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law

117-81). All coordination efforts shall be undertaken with appropriate protections for sensitive and classified information and intelligence sources and methods.

Sec. 3. Mitigating the Risks to Encryption. (a) Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a CRQC.

To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035.

Currently, the Director of the National Institute of Standards and Technology (NIST) and the Director of the National Security Agency (NSA), in their capacity as the National Manager for National Security Systems (National Manager), are each developing technical standards for quantum-resistant cryptography for their respective jurisdictions. The first sets of these standards are expected to be released publicly by 2024.

(b) Central to this migration effort will be an emphasis on cryptographic agility, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards. This effort is an imperative across all sectors of the United States economy, from government to critical infrastructure, commercial services to cloud providers, and everywhere else that vulnerable public-key cryptography is used.

(c) Consistent with these goals:

(i) Within 90 days of the date of this memorandum, the Secretary of Commerce, through the Director of NIST, shall initiate an open working group with industry, including critical infrastructure owners and operators, and other stakeholders, as determined by the Director of NIST, to further advance adoption of quantum-resistant cryptography.

This working group shall identify needed tools and data sets, and other considerations to inform the development by NIST of guidance and best practices to assist with quantum-resistant cryptography planning and prioritization. Findings of this working group shall be provided, on an ongoing basis, to the Director of the Office of Management and Budget (OMB), the Assistant to the President for National Security Affairs (APNSA), and the National Cyber Director to incorporate into planning efforts.

(ii) Within 90 days of the date of this memorandum, the Secretary of Commerce, through the Director of NIST, shall establish a "Migration to Post-Quantum Cryptography Project" at the National Cybersecurity Center of Excellence to work with the private sector to address cybersecurity challenges posed by the transition to quantum-resistant cryptography. This project shall develop programs for discovery and remediation of any system that does not use quantum-resistant cryptography or that remains dependent on vulnerable systems.

(iii) Within 180 days of the date of this memorandum, and annually thereafter, the Secretary of Homeland Security, through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), and in coordination with Sector Risk Management Agencies, shall engage with critical infrastructure and SLTT partners regarding the risks posed by quantum computers, and shall provide an annual report to the Director of OMB, the APNSA, and the National Cyber Director that includes

recommendations for accelerating those entities' migration to quantum-resistant cryptography.

(iv) Within 180 days of the date of this memorandum, and on an ongoing basis, the Director of OMB, in consultation with the Director of CISA, the Director of NIST, the National Cyber Director, and the Director of NSA, shall establish requirements for inventorying all currently deployed cryptographic systems, excluding National Security Systems (NSS).

These requirements shall include a list of key information technology (IT) assets to prioritize, interim benchmarks, and a common (and preferably automated) assessment process for evaluating progress on quantum-resistant cryptographic migration in IT systems.

(v) Within 1 year of the date of this memorandum, and on an annual basis thereafter, the heads of all Federal Civilian Executive Branch (FCEB) Agencies shall deliver to the Director of CISA and the National Cyber Director an inventory of their IT systems that remain vulnerable to CRQCs, with a particular focus on High Value Assets and High Impact Systems. Inventories should include current cryptographic methods used on IT systems, including system administrator protocols, non-security software and firmware that require upgraded digital signatures, and information on other key assets.

(vi) By October 18, 2023, and on an annual basis thereafter, the National Cyber Director shall, based on the inventories described in subsection 3(c)(v) of this memorandum and in coordination with the Director of CISA and the Director of NIST, deliver a status report to the APNSA and the Director of OMB on progress made by FCEB Agencies on their migration of non-NSS IT systems to quantum-resistant cryptography.

This status report shall include an assessment of the funding necessary to secure vulnerable IT systems from the threat posed by adversarial access to quantum computers, a description and analysis of ongoing coordination efforts, and a strategy and timeline for meeting proposed milestones.

(vii) Within 90 days of the release of the first set of NIST standards for quantum-resistant cryptography referenced in subsection 3(a) of this memorandum, and on an annual basis thereafter, as needed, the Secretary of Commerce, through the Director of NIST, shall release a proposed timeline for the deprecation of quantum-vulnerable cryptography in standards, with the goal of moving the maximum number of systems off quantum-vulnerable cryptography within a decade of the publication of the initial set of standards. The Director of NIST shall work with the appropriate technical standards bodies to encourage interoperability of commercial cryptographic approaches.

(viii) Within 1 year of the release of the first set of NIST standards for quantum-resistant cryptography referenced in subsection 3(a) of this memorandum, the Director of OMB, in coordination with the Director of CISA and the Director of NIST, shall issue a policy memorandum requiring FCEB Agencies to develop a plan to upgrade their non-NSS IT systems to quantum-resistant cryptography.

These plans shall be expeditiously developed and be designed to address the most significant risks first. The Director of OMB shall work with the head of each FCEB Agency to estimate the costs to upgrade vulnerable systems beyond already planned expenditures, ensure that each plan is coordinated and shared among relevant agencies to assess interoperability between solutions, and coordinate with the National Cyber Director to ensure plans are updated accordingly.

(ix) Until the release of the first set of NIST standards for quantum-resistant cryptography referenced in subsection 3(a) of this memorandum, the heads of FCEB Agencies shall not procure any commercial quantum-resistant cryptographic solutions for use in IT systems supporting enterprise and mission operations.

However, to assist with anticipating potential compatibility issues, the heads of such FCEB Agencies should conduct tests of commercial solutions that have implemented pre-standardized quantum-resistant cryptographic algorithms.

These tests will help identify interoperability or performance issues that may occur in Federal environments at an early stage and will contribute to the mitigation of those issues. The heads of such FCEB Agencies should continue to implement and, where needed, upgrade existing cryptographic implementations, but should transition to quantum-resistant cryptography only once the first set of NIST standards for quantum-resistant cryptography is complete and implemented in commercial products. Conformance with international standards should be encouraged, and may be required for interoperability.

(x) Within 1 year of the date of this memorandum, and annually thereafter, the Director of NSA, serving in its capacity as the National Manager, in consultation with the Secretary of Defense and the Director of National Intelligence, shall provide guidance on quantum-resistant cryptography migration, implementation, and oversight for NSS.

This guidance shall be consistent with National Security Memorandum/NSM-8 (Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems). The National Manager shall share best practices and lessons learned with the Director of OMB and the National Cyber Director, as appropriate.

(xi) Within 1 year of the date of this memorandum, and on an ongoing basis, and consistent with section 1 of NSM-8, the heads of agencies operating NSS shall identify and document all instances where quantum-vulnerable cryptography is used by NSS and shall provide this information to the National Manager.

(xii) Within 180 days of issuance by the National Manager of its standards on quantum-resistant cryptography referenced in section 3(a) of this memorandum, and annually thereafter, the National Manager shall release an official timeline for the deprecation of vulnerable cryptography in NSS, until the migration to quantum-resistant cryptography is completed.

(xiii) Within 1 year of issuance by the National Manager of its standards on quantum-resistant cryptography for referenced in subsection 3(a) of this memorandum, and annually thereafter, the heads of agencies operating or maintaining NSS shall submit to the National Manager, and, as appropriate, the Department of Defense Chief Information Officer or the Intelligence Community Chief Information Officer, depending on their respective jurisdictions, an initial plan to transition to quantum-resistant cryptography in all NSS.

These plans shall be updated annually and shall include relevant milestones, schedules, authorities, impediments, funding requirements, and exceptions authorized by the head of the agency in accordance with section 3 of NSM-8 and guidance from the National Manager.

(xiv) By December 31, 2023, agencies maintaining NSS shall implement symmetric-key protections (e.g., High Assurance Internet Protocol Encryptor (HAIPE) exclusion keys or

VPN symmetric key solutions) to provide additional protection for quantum-vulnerable key exchanges, where appropriate and in consultation with the National Manager. Implementation should seek to avoid interference with interoperability or other cryptographic modernization efforts.

(xv) By December 31, 2023, the Secretary of Defense shall deliver to the APNSA and the Director of OMB an assessment of the risks of quantum computing to the defense industrial base and to defense supply chains, along with a plan to engage with key commercial entities to upgrade their IT systems to achieve quantum resistance.

Sec. 4. Protecting United States Technology. (a) In addition to promoting quantum leadership and mitigating the risks of CRQCs, the United States Government must work to safeguard relevant quantum R&D and intellectual property (IP) and to protect relevant enabling technologies and materials. Protection mechanisms will vary, but may include counterintelligence measures, well-targeted export controls, and campaigns to educate industry and academia on the threat of cybercrime and IP theft.

(b) All agencies responsible for either promoting or protecting QIS and related technologies should understand the security implications of adversarial use and consider those security implications when implementing new policies, programs, and projects.

(c) The United States should ensure the protection of U.S.-developed quantum technologies from theft by our adversaries. This will require campaigns to educate industry, academia, and SLTT partners on the threat of IP theft and on the importance of strong compliance, insider threat detection, and cybersecurity programs for quantum technologies.

As appropriate, Federal law enforcement agencies and other relevant agencies should investigate and prosecute actors who engage in the theft of quantum trade secrets or who violate United States export control laws. To support efforts to safeguard sensitive information, Federal law enforcement agencies should exchange relevant threat information with agencies responsible for developing and promoting quantum technologies.

(d) Consistent with these goals, by December 31, 2022, the heads of agencies that fund research in, develop, or acquire quantum computers or related QIS technologies shall develop comprehensive technology protection plans to safeguard QIS R&D, acquisition, and user access.

Plans shall be coordinated across agencies, including with Federal law enforcement, to safeguard quantum computing R&D and IP, acquisition, and user access. These plans shall be updated annually and provided to the APNSA, the Director of OMB, and the Co-Chairs of the National Science and Technology Council Subcommittee on Economic and Security Implications of Quantum Science.

Sec. 5. Definitions. For purposes of this memorandum:

(a) the term “agency” has the meaning ascribed to it under 44 U.S.C. 3502;

(b) the term “critical infrastructure” means systems and assets, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on the Nation’s security, economy, public health and safety, or any combination thereof;

(c) the term "cryptographic agility" means a design feature that enables future updates to cryptographic algorithms and standards without the need to modify or replace the surrounding infrastructure;

(d) the term "cryptanalytically relevant quantum computer" or "CRQC" means a quantum computer capable of undermining current public-key cryptographic algorithms;

(e) the term "Federal Civilian Executive Branch Agency" or "FCEB Agency" means any agency except the Department of Defense or agencies in the Intelligence Community;

(f) the term "high value asset" means information or an information system that is so critical to an organization that the loss or corruption of this information, or loss of access to the system, would have serious impacts on the organization's ability to perform its mission or conduct business;

(g) the term "high impact system" means an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a Federal Information Processing Standards (FIPS) 199 potential impact value of "high";

(h) the term "information technology" or "IT" has the meaning ascribed to it under 44 U.S.C. 3502;

(i) the term "National Security Systems" or "NSS" has the meaning ascribed to it in 44 U.S.C 3552(b)(6) and shall also include other Department of Defense and Intelligence Community systems, as described in 44 U.S.C. 3553(e)(2) and 44 U.S.C. 3553(e)(3);

(j) the term "quantum computer" means a computer utilizing the collective properties of quantum states, such as superposition, interference and entanglement, to perform calculations. The foundations in quantum physics give a quantum computer the ability to solve a subset of hard mathematical problems at a much faster rate than a classical (i.e., non-quantum) computer;

(k) the term "quantum information sciences" or "QIS" has the meaning ascribed to it under 15 U.S.C. 8801(6) and means the study and application of the laws of quantum physics for the storage, transmission, manipulation, computing, or measurement of information; and

(l) the term "quantum-resistant cryptography" means those cryptographic algorithms or methods that are assessed not to be specifically vulnerable to attack by either a CRQC or classical computer. This is also referred to as post-quantum cryptography.

Sec. 6. General Provisions. (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof, to include the protection of intelligence sources and methods; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This memorandum shall also be implemented without impeding the conduct or support of intelligence activities, and all implementation measures shall be designed to be consistent with appropriate protections for sensitive information and intelligence sources and methods.

(d) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

To read more: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

Disclaimer

The International Association of Hedge Funds Professionals (IAHFP)(hereinafter "Association") enhances public access to information. Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

The Association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The Association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided, as these are general information, not specific guidance for an organization or a firm in a specific country.

This information:

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

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

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

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

- is not professional or legal advice;

- is in no way constitutive of interpretative;

- 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.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. The Association does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

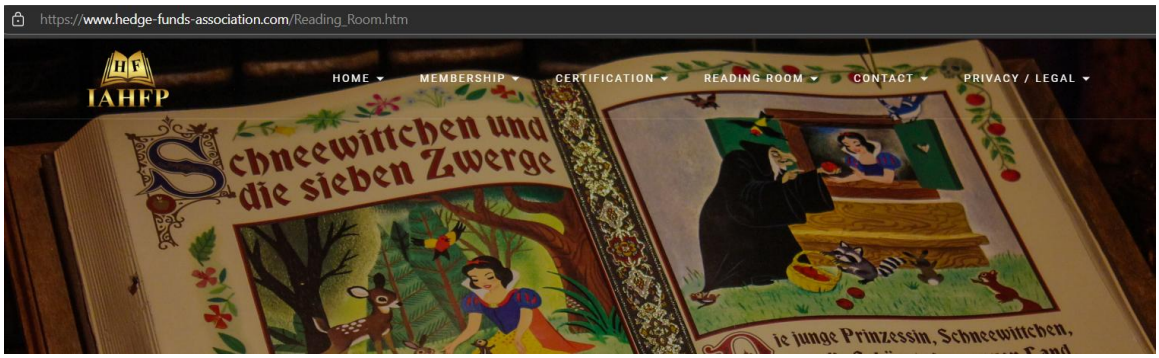
Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems. The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.

International Association of Hedge Funds Professionals (IAHFP)

The Association is a business unit of Compliance LLC, incorporated in Wilmington, NC, and offices in Washington, DC, a provider of risk and compliance training in 57 countries.

Our reading room:
https://www.hedge-funds-association.com/Reading_Room.htm



"Mirror, mirror on the wall, who in this land is fairest of all?"

Children's fiction can open up new perspectives for adults. Black swan events, exercising (or failing to exercise) the zero trust principle, risks and opportunities are all there.

Investigating the facts is the next pleasure. In 1994, Eckhard Sander claimed that the character of Snow White was based on the life of Margaretha von Waldeck, a German countess born in 1533. At the age of 16, Margaretha was forced by her stepmother, Katharina of Hatzfeld, to move away to Brussels. There, Margaretha fell in love with a prince who would later become Philip II of Spain.

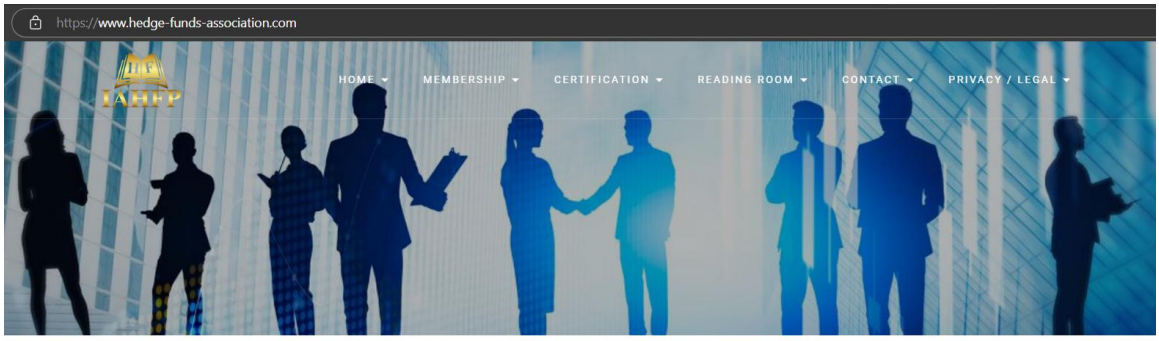
Graham Anderson compares the story of Snow White to the Roman legend of Chione, recorded in Ovid's Metamorphoses. The name Chione means "snow" in Greek and, in the story, she is described as the most beautiful woman in the land, so beautiful that the gods Apollo and Hermes both fell in love with her.

For Snow White, the death of her real mother and the arrival of a stepmother is a disaster. Snow White is forced to leave home, but she discovers who she is, and moves along the path to self-discovery and resilience. This is a story about development set in motion by the arrival of evil. Does it look familiar?

Contact Us

Lyn Spooner
Email: lyn@hedge-funds-association.com

George Lekatis
President of the IAHFP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Email: lekatis@hedge-funds-association.com
Web: www.hedge-funds-association.com



WELCOME

You are a risk and compliance officer working for hedge funds, or perhaps a consultant or analyst. You are part of a team that offers investors a unique range of strategies tailored to meet their specific investment objectives.

Your fund has the ability to generate positive returns in both rising and falling markets, and gives investors opportunities for absolute returns, skill-based strategies and diversification.