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

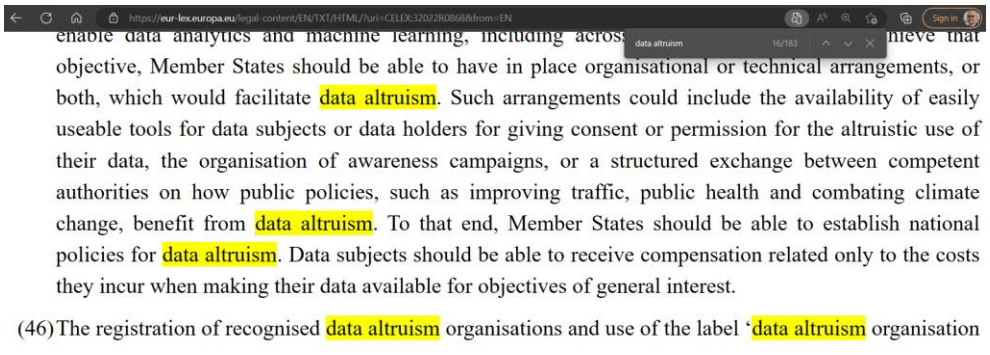
Monday, April 10, 2023

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

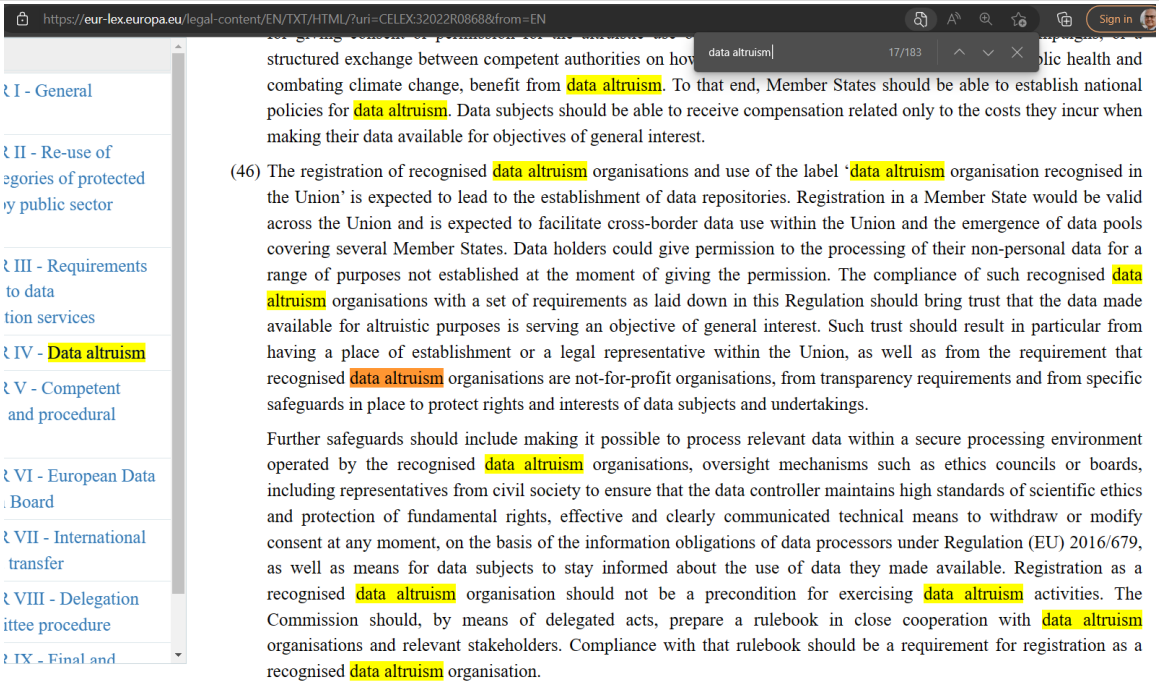
I prepare a presentation for a Board of Directors on the European Data Governance Act (DGA) - Regulation (EU) 2022/868. A very difficult part is the unbelievable concept of "data altruism".

Why is it difficult? Because the phrase "data altruism" is repeated 183 times in 44 pages.



enable data analytics and machine learning, including across … data altruism 16/183 … achieve that objective, Member States should be able to have in place organisational or technical arrangements, or both, which would facilitate data altruism. Such arrangements could include the availability of easily useable tools for data subjects or data holders for giving consent or permission for the altruistic use of their data, the organisation of awareness campaigns, or a structured exchange between competent authorities on how public policies, such as improving traffic, public health and combating climate change, benefit from data altruism. To that end, Member States should be able to establish national policies for data altruism. Data subjects should be able to receive compensation related only to the costs they incur when making their data available for objectives of general interest.

(46) The registration of recognised data altruism organisations and use of the label 'data altruism organisation


https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0868&from=EN

Sign in

data altruism 17/183

I - General

II - Re-use of egories of protected y public sector

III - Requirements to data tion services

IV - Data altruism

V - Competent and procedural

VI - European Data Board

VII - International transfer

VIII - Delegation ittee procedure

IX - Final and

structured exchange between competent authorities on how lic health and combating climate change, benefit from data altruism. To that end, Member States should be able to establish national policies for data altruism. Data subjects should be able to receive compensation related only to the costs they incur when making their data available for objectives of general interest.

(46) The registration of recognised data altruism organisations and use of the label 'data altruism organisation recognised in the Union' is expected to lead to the establishment of data repositories. Registration in a Member State would be valid across the Union and is expected to facilitate cross-border data use within the Union and the emergence of data pools covering several Member States. Data holders could give permission to the processing of their non-personal data for a range of purposes not established at the moment of giving the permission. The compliance of such recognised data altruism organisations with a set of requirements as laid down in this Regulation should bring trust that the data made available for altruistic purposes is serving an objective of general interest. Such trust should result in particular from having a place of establishment or a legal representative within the Union, as well as from the requirement that recognised data altruism organisations are not-for-profit organisations, from transparency requirements and from specific safeguards in place to protect rights and interests of data subjects and undertakings.

Further safeguards should include making it possible to process relevant data within a secure processing environment operated by the recognised data altruism organisations, oversight mechanisms such as ethics councils or boards, including representatives from civil society to ensure that the data controller maintains high standards of scientific ethics and protection of fundamental rights, effective and clearly communicated technical means to withdraw or modify consent at any moment, on the basis of the information obligations of data processors under Regulation (EU) 2016/679, as well as means for data subjects to stay informed about the use of data they made available. Registration as a recognised data altruism organisation should not be a precondition for exercising data altruism activities. The Commission should, by means of delegated acts, prepare a rulebook in close cooperation with data altruism organisations and relevant stakeholders. Compliance with that rulebook should be a requirement for registration as a recognised data altruism organisation.

I must explain to the Board of Directors of the US organization (the client) that "a data intermediation services provider that is not established in the European Union, but which offers the data intermediation services within the Union, shall designate a legal representative in one of the Member States in which those services are offered".

But what exactly is the 'legal representative', according to the European Data Governance Act (DGA)?

According to the DGA, "legal representative means a natural or legal person established in the Union explicitly designated to act on behalf of a data intermediation services provider or an entity that collects data for objectives of general interest made available by natural or legal persons on the basis of data altruism not established in the Union, which may be addressed by the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations in addition to or instead of the data intermediation services provider or entity with regard to the obligations under this Regulation, including with regard to initiating enforcement proceedings against a non-compliant data intermediation services provider or entity not established in the Union".

This is one sentence, and I have to explain it. I would prefer to explain Quantum Steganography in a Board, it would be easier. Socrates believed that the poets are only the interpreters of the gods. Perhaps I must follow this approach.

Read more at number 1 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 6)

Regulation (EU) 2022/868 (Data Governance Act)

Official Journal

of the European Union

Number 2 (Page 10)

US Federal Reserve Banks, Combined Financial Statements

Number 3 (Page 13)

BIS's Project Nexus prototype successfully links Eurosystem, Malaysia and Singapore payments systems.

Partners in Indonesia, Malaysia, the Philippines, Singapore and Thailand to work towards wider payments connectivity

Number 4 (Page 19)

Current challenges facing the European Monetary Union

Dr Joachim Nagel, President of the Deutsche Bundesbank, at King's College, London.

Number 5 (Page 28)

Development of a National Spectrum Strategy

National Telecommunications and Information Administration, Department of Commerce - Request for comments.

National Telecommunications and Information Administration

United States Department of Commerce

Number 6 (Page 31)

Is Your Cybersecurity Strategy Falling Victim to These 6 Common Pitfalls?

NIST research reveals misconceptions that can affect security professionals — and offers solutions.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Number 7 (Page 35)

Ransomware Vulnerability Warning Pilot (RVWP)

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Number 8 (Page 37)

Joint communication on the update of the EU Maritime Security Strategy and its Action Plan

An enhanced EU Maritime Security Strategy for evolving maritime threats

EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Number 9 (Page 41)

DNS data shows one in ten organisations have malware traffic on their networks

National Cyber Security Centre

Number 10 (Page 43)

Preventing the Improper Use of CHIPS Act Funding

NATIONAL ARCHIVES

FEDERAL REGISTER
The Daily Journal of the United States Government

Number 1

Regulation (EU) 2022/868 (Data Governance Act)

Official Journal

of the European Union

Action at Union level is necessary to increase trust in data sharing by establishing appropriate mechanisms for control by data subjects and data holders over data that relates to them, and in order to address other barriers to a well-functioning and competitive data-driven economy.

That action should be without prejudice to obligations and commitments in the international trade agreements concluded by the Union.

A Union-wide governance framework should have the objective of building trust among individuals and undertakings in relation to data access, control, sharing, use and re-use, in particular by establishing appropriate mechanisms for data subjects to know and meaningfully exercise their rights, as well as with regard to the re-use of certain types of data held by the public sector bodies, the provision of services by data intermediation services providers to data subjects, data holders and data users, as well as the collection and processing of data made available for altruistic purposes by natural and legal persons.

In particular, more transparency regarding the purpose of data use and conditions under which data is stored by undertakings can help increase trust.

The idea that data that has been generated or collected by public sector bodies or other entities at the expense of public budgets should benefit society has been part of Union policy for a long time.

Directive (EU) 2019/1024 and sector-specific Union law ensure that the public sector bodies make more of the data they produce easily available for use and re-use.

However, certain categories of data, such as commercially confidential data, data that are subject to statistical confidentiality and data protected by intellectual property rights of third parties, including trade secrets and personal data, in public databases are often not made available, not even for research or innovative activities in the public interest, despite such availability being possible in accordance with the applicable Union law, in

particular Regulation (EU) 2016/679 and Directives 2002/58/EC and (EU) 2016/680.

Due to the sensitivity of such data, certain technical and legal procedural requirements must be met before they are made available, not least in order to ensure the respect of rights others have over such data or to limit the negative impact on fundamental rights, the principle of non-discrimination and data protection. The fulfilment of such requirements is usually time- and knowledge-intensive. This has led to the insufficient use of such data.

While some Member States are establishing structures, processes or legislation to facilitate that type of re-use, this is not the case across the Union. In order to facilitate the use of data for European research and innovation by private and public entities, clear conditions for access to and use of such data are needed across the Union.

There are techniques enabling analyses on databases that contain personal data, such as anonymisation, differential privacy, generalisation, suppression and randomisation, the use of synthetic data or similar methods and other state-of-the-art privacy-preserving methods that could contribute to a more privacy-friendly processing of data.

Member States should provide support to public sector bodies to make optimal use of such techniques, thus making as much data as possible available for sharing.

The application of such techniques, together with comprehensive data protection impact assessments and other safeguards, can contribute to more safety in the use and re-use of personal data and should ensure the safe re-use of commercially confidential business data for research, innovation and statistical purposes.

Article 1, Subject matter and scope

1. This Regulation lays down:

(a) conditions for the re-use, within the Union, of certain categories of data held by public sector bodies;

(b) a notification and supervisory framework for the provision of data intermediation services;

(c) a framework for voluntary registration of entities which collect and process data made available for altruistic purposes; and

(d) a framework for the establishment of a European Data Innovation Board.

2. This Regulation does not create any obligation on public sector bodies to allow the re-use of data, nor does it release public sector bodies from their confidentiality obligations under Union or national law.

This Regulation is without prejudice to:

(a) specific provisions in Union or national law regarding the access to or re-use of certain categories of data, in particular with regard to the granting of access to and disclosure of official documents; and

(b) the obligations of public sector bodies under Union or national law to allow the re-use of data or to requirements related to processing of non-personal data.

Where sector-specific Union or national law requires public sector bodies, data intermediation services providers or recognised data altruism organisations to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union or national law shall also apply. Any such specific additional requirements shall be non-discriminatory, proportionate and objectively justified.

3. Union and national law on the protection of personal data shall apply to any personal data processed in connection with this Regulation. In particular, this Regulation is without prejudice to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directives 2002/58/EC and (EU) 2016/680, including with regard to the powers and competences of supervisory authorities.

In the event of a conflict between this Regulation and Union law on the protection of personal data or national law adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data shall prevail.

This Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligations set out in Regulations (EU) 2016/679 or (EU) 2018/1725 or Directives 2002/58/EC or (EU) 2016/680.

4. This Regulation is without prejudice to the application of competition law.

5. This Regulation is without prejudice to the competences of the Member States with regard to their activities concerning public security, defence and national security.

The Act:
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0868&from=EN

Number 2

US Federal Reserve Banks, Combined Financial Statements

The Federal Reserve Board on Friday released the 2022 combined annual audited financial statements for the Reserve Banks.

An independent public accounting firm engaged by the Board issued unqualified opinions, asserting that its audit found the financial statements for the Board and the Reserve Banks to be free of material misstatements in accordance with the applicable auditing standards.

The Board released preliminary income and expense data earlier this year.

Additionally, the Board released individual statements for the 12 Federal Reserve Banks, the Board, and 3 limited liability companies (LLCs) related to lending facilities established to support the Federal Reserve's pandemic response.

The audited financial statements provide information about the assets, liabilities, and earnings of the Federal Reserve Banks, the Board, and the LLCs as of December 31, 2022.

The Federal Reserve Act requires the Reserve Banks to remit excess earnings to the U.S. Treasury after providing for operating costs, payments of dividends, and any amount necessary to maintain surplus at the statutory limit.

During a period when earnings are less than these costs, a deferred asset is recorded, representing a shortfall in earnings from the most recent point that remittances to the Treasury were suspended.

During 2022, the Reserve Banks transferred $76.0 billion from weekly earnings as compared to $109 billion in 2021, and in the fall, they first suspended weekly remittances to the Treasury and began accumulating a deferred asset, which totaled $16.6 billion by the end of the year.

A deferred asset has no implications for the Federal Reserve's conduct of monetary policy, its operations, or its ability to meet its financial obligations.

Additional information in the audited financial statements of the Reserve Banks includes:

- Earnings were approximately $58.8 billion in 2022, representing a decrease of $49.1 billion from 2021;
- Interest income on securities acquired through open market operations totaled $170.0 billion in 2022, an increase of $47.6 billion from 2021;
- Interest expense on depository institutions' reserve balances was $60.4 billion in 2022, an increase of $55.1 billion from 2021;
- Interest expense on securities sold under agreements to repurchase was $42.0 billion in 2022, an increase of $41.6 billion from 2021.
- Net income from facilities related to the Federal Reserve's pandemic response was $108.0 million in 2022; and
- Operating expenses were $9.2 billion in 2022, including assessments of $2.8 billion for Board expenses, currency costs, and the operations of the Consumer Financial Protection Bureau.

Total assets of the Reserve Banks as of December 31, 2022, were approximately $8.6 trillion, a decrease of $187.0 billion from the previous year.

Total assets were composed primarily of $8.4 trillion of U.S. Treasury securities, and federal agency and government-sponsored enterprise mortgage-backed securities acquired through open market operations.

The Federal Reserve Bank of New York provides additional detailed information about open market operations and securities holdings on an ongoing basis on its website.

The Board engaged KPMG LLP to audit the financial statements of the Reserve Banks and the LLCs in accordance with standards issued by the American Institute of Certified Public Accountants and the Public Company Accounting Oversight Board, and the audit of the Board's financial statements was also conducted in accordance with the Generally Accepted Government Auditing Standards. KPMG also conducted audits of internal controls over financial reporting for the 12 individual Reserve Banks and the Board.

The Federal Reserve System financial statements are available on the Federal Reserve Board's website.

To read more:
https://www.federalreserve.gov/aboutthefed/files/combinedfinstmt2022.pdf

Number 3

BIS's Project Nexus prototype successfully links Eurosystem, Malaysia and Singapore payments systems.

Partners in Indonesia, Malaysia, the Philippines, Singapore and Thailand to work towards wider payments connectivity

BIS

To enhance cross-border payments, the BIS Innovation Hub Singapore Centre developed the Nexus concept of a first-of-its-kind multilateral network connecting multiple domestic instant payment systems (IPS).

Nexus prototype successfully connected the test IPS of the Eurosystem, Malaysia and Singapore, allowing payments to be sent across the three using only mobile phone numbers.

In the next phase, BIS and the central banks of Indonesia, Malaysia, the Philippines, Singapore and Thailand will jointly work towards connecting their domestic IPS through Nexus.

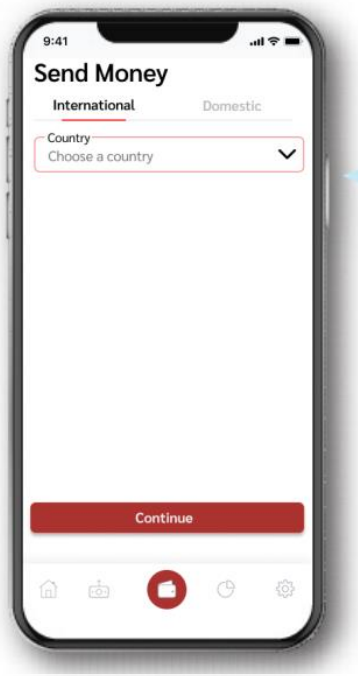
The BIS Innovation Hub Singapore Centre and partners today announced the successful connection of the test versions of three established IPS using the Nexus model and outlined the next phase of the project to work on the real-world potential of a multilateral network that could be scaled up across more countries.

The year-long collaboration included the Bank of Italy, Central Bank of Malaysia (BNM) and Monetary Authority of Singapore (MAS), plus the payment systems operators PayNet and Banking Computer Services (BCS).

Test payments were initiated using only the mobile phone numbers or the recipients' company registration numbers via the Eurosystem's TARGET Instant Payment Settlement (TIPS), Malaysia's Real-time Retail Payments Platform (RPP) and Singapore's Fast and Secure Transfers (FAST) payment system.

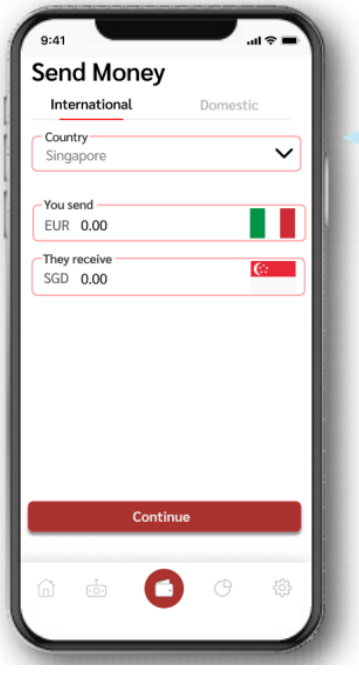
The Nexus report, published today, provides details on the early experiments and technical specifications for the multilateral interlinking of payment systems.

The success of the experiment paves the way for the BIS Innovation Hub Singapore Centre to explore the practical applications of a distributed multilateral network.



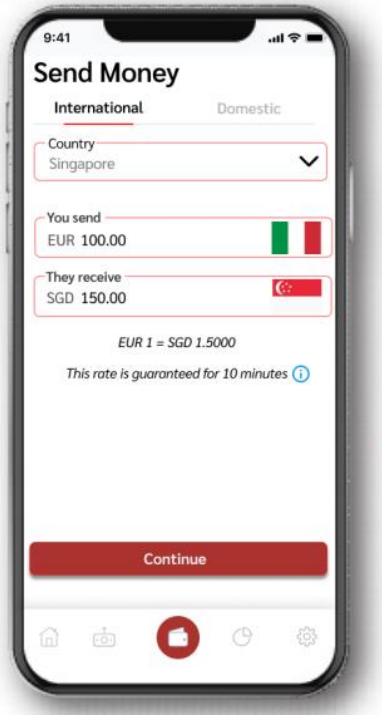
The sender logs in to their bank or PSP's existing app. (There is no separate Nexus app.)

The sender selects the Destination Country.



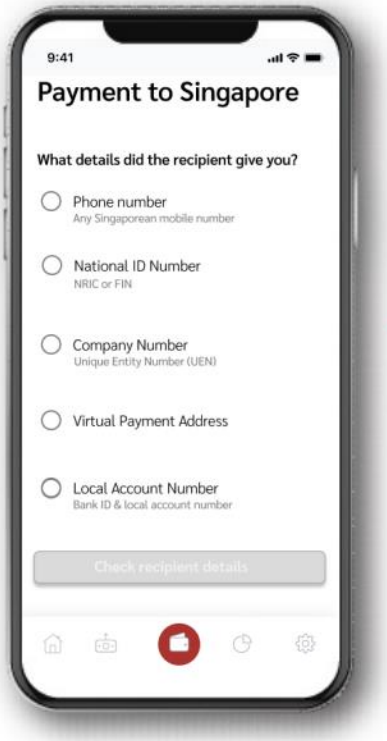
The sender enters EITHER the amount they wish to send, in their own currency OR the amount they wish the recipient to receive, in the recipient's currency.

The recipient will receive exactly the amount shown, without deductions. If the Destination PSP charges the recipient any fees for processing the payment, these must be charged as a separate line item.



Nexus retrieves a list of quotes. The sender's PSP (Source PSP) will also ask Nexus for available quotes for payments to the Destination Country. Nexus returns a list of quotes from different FXPs. The Source PSP selects the quote and FX Provider that it wishes to use. The Source PSP can also choose to add a markup to the FX rate before it displays the final rate to the sender.

If the sender accepts the rate, they click "Continue". If they change either amount, the rate will be refreshed (as larger payments may be eligible for better rates).

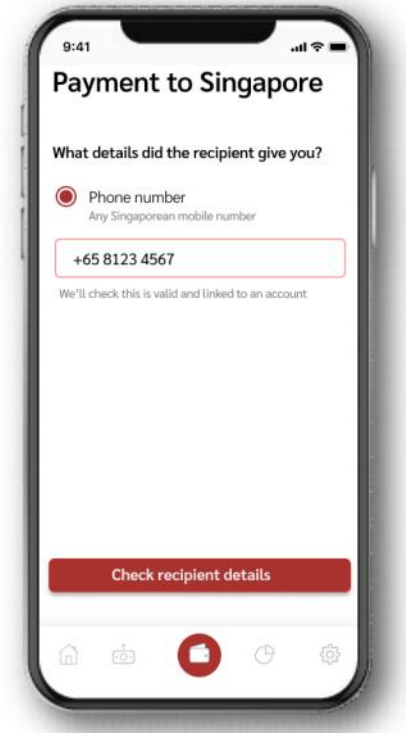


The Source PSP uses the Nexus API to request the full list of proxy formats that can be used to address payments to the Destination Country. It uses this information to dynamically create a list of proxy formats in the app.

The sender then selects the type of proxy or account details that the recipient has provided to them.

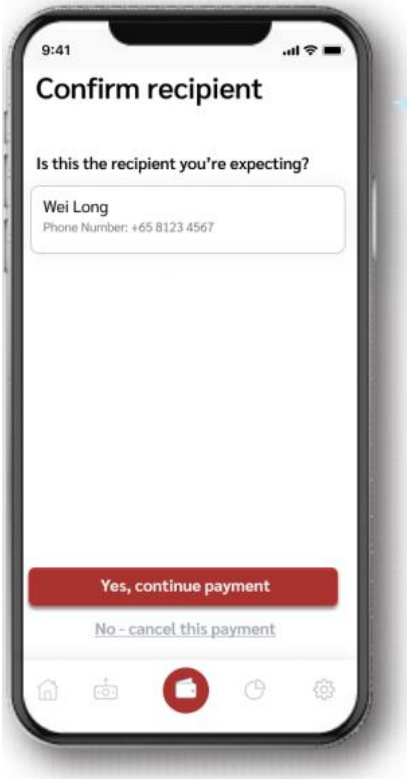
The sender can select a proxy (such as a mobile phone number). Any alias that is valid in the Destination Country will also be valid through Nexus.

The sender can alternatively enter a domestic account number and PSP identifier (such as a BIC) or an International Bank Account Number, where these are accepted in the Destination Country.



If a sender enters a proxy, the Source PSP will send this information to Nexus. Nexus will then contact the proxy resolution service in the Destination Country. If the proxy is registered to an account, it will respond to Nexus with the associated account details and the name of the recipient, along with a display name that can be shown to the sender.

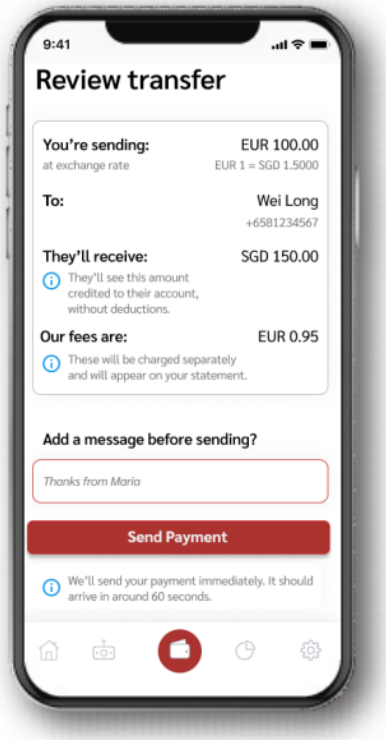
Nexus will then use the account details to confirm that the recipient's PSP is onboarded with Nexus and able to receive cross-border payments.



Now the sender is shown the name of the recipient, as provided by the proxy resolution service, where available.

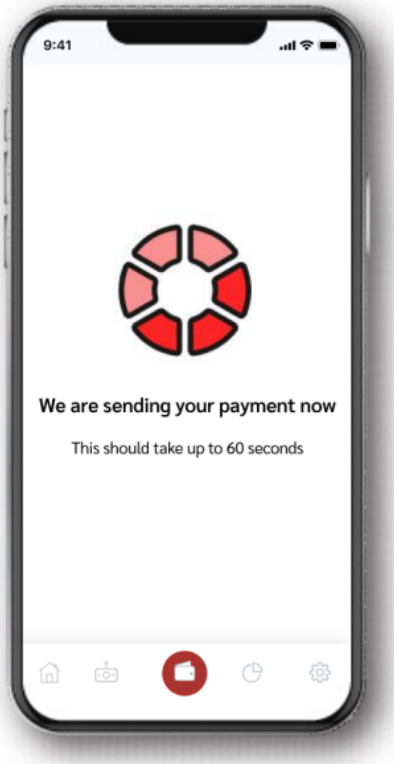
Depending on the country's requirements, they may see the full name or the name partially obscured.

The sender confirms the name. (If they don't recognise the name, they can cancel the payment).



The sender is given a chance to confirm all details. They are shown exactly what will be deducted from their account, exactly what will be credited to the recipient, the final exchange rate that applies and any fees that the sender's PSP or bank will charge the sender.

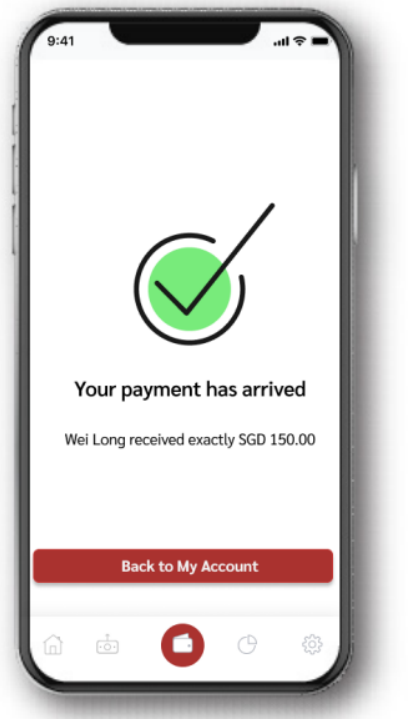
The sender clicks "Send Payment".



Final payment instruction – the payment instruction can now be sent from the Source PSP to the Source IPS.

Once the payment is complete in the Source IPS, the Nexus Gateway will communicate with the Nexus Gateway in the Destination Country, which will trigger the second stage of the process in the destination IPS.

The payment should be processed within 60 seconds in most cases.



Once the final payment stage is complete, the recipient will be credited and notified, and the sender will be notified that their payment was successful.

In some cases, the payment will trigger an alert against any sanctions lists. If the PSP in question does not have a highly automated screening process, it may need extra time to process the payment. In this case, the payment will still successfully reach the recipient's PSP, but the PSP will have extra time (defined in the Nexus Scheme Rulebook) to review the payment before crediting it to the recipient.

To read more: https://www.bis.org/press/p230323.htm

https://www.bis.org/publ/othp62.pdf

Project Nexus

Enabling instant cross-border payments

Conclusions from a technical proof of concept between the Eurosystem, Malaysia and Singapore

March 2023

BANCA D'ITALIA EUROSISTEMA

BANK NEGARA MALAYSIA CENTRAL BANK OF MALAYSIA

MAS Monetary Authority of Singapore

PayNet PAYMENTS NETWORK MALAYSIA

Banking Computer Services Private Limited
A Subsidiary of NETS

Number 4

Current challenges facing the European Monetary Union

Dr Joachim Nagel, President of the Deutsche Bundesbank, at King's College, London.

1. Introduction

Ladies and gentlemen,

I am very pleased to be with you today and to speak in these beautiful and history-filled surroundings.

We are living in turbulent times – once again. I guess almost everyone can name factors currently adding to overall uncertainty: the Russian war of aggression against Ukraine, the comeback of high inflation, high public debt levels and, most recently, financial market tensions as well. In such times, it is especially difficult to prioritise actions that need to be taken.

In my speech today, I will focus on a number of issues that I deem important right now. I will shed some light on current economic developments. Then I will of course, comment on inflation and monetary policy. And I will focus especially on fiscal developments and the discussion surrounding fiscal rules which – as you may know, is a particular obsession of central bankers.

One topic that is probably of particular interest to you is the most recent developments in financial markets. Whenever banks get in distress or fail, questions inevitably pop up: about proper risk management, about sufficient regulation, about contagion risks. And rightly so. It is our duty as central banks to probe the stability of our corners of the global financial system.

As far as I can see, the majority of risk managers in banks have done a decent job of coping with today's challenges. Regulation in the euro area is far stricter now than it was 15 years ago. The euro area banking sector is resilient, with strong capital and liquidity positions. And despite the events that we have witnessed in the past 15 days, contagion risks to euro area banks appear to be low. We will continue to monitor closely the developments in financial markets. And we are ready to act, if need be.

With that, I would like to move to issues more important in the long run. In my speech today, I will elaborate on some of the current challenges facing the European Monetary Union, with special focus on the two public sector agents influencing the macroeconomy – monetary and fiscal policies. I will draw particular attention to the ongoing debate about reforming European fiscal rules.

But every speech on general issues is naturally held in specific times and circumstances. So, let me begin with a few words about the economic and inflation outlook in Europe as well as about our latest monetary policy decisions.

2. The macroeconomic environment

Last year, the euro are saw an expansion of 3.5% in economic activity. The main factor behind the economic expansion in Europe was the lifting of COVID-related restrictions. However, high inflation dampened private consumption. This was, to some extent, due to the energy crisis caused by the Russian war of aggression against Ukraine.

Initially, during the late summer, there were deep concerns that a cut in the Russian energy supply would cause a severe recession, at least in some euro area countries. Fortunately, European countries and Germany in particular made considerable progress in finding alternative gas suppliers and in filling gas storage facilities before the winter. Thus, the most negative scenario was avoided.

Nevertheless, the energy crisis provoked not only surging energy retail prices and higher production costs for firms. It also created considerable uncertainty and made production planning for firms more difficult, especially for those with high energy consumption. These dampening factors had an effect in the second half of the year especially, while the growth effects of the lifting of COVID restrictions petered out.

For this winter, we expect economic activity in the euro area to increase marginally. According to the ECB's economic projections published last week, GDP in the euro area will grow only by 1% this year. It should be taken into account though, that the current financial market tensions imply greater uncertainty around projected figures.

One of the most striking economic features of the recent past is the comeback of high inflation. To be fair, the high inflation did not emerge only because of the energy crisis caused by the war in Ukraine. The inflation rate had already accelerated in the summer of 2021.

As the world recovered from the unprecedented economic slump caused by the pandemic, supply chains were under stress. Together with expansive monetary and fiscal policies, the rapid recovery pushed up energy prices. Moreover, demand for certain goods and services increased strongly. Supply bottlenecks and price increases were the result.

With the Russian invasion of Ukraine in February 2022, energy prices skyrocketed. Furthermore, the war and its consequences disrupted some other supply chains. In particular, the energy price shock heated up inflation even more.

The figures clearly demonstrate how exceptional last year was. According to the IMF, 2022 consumer prices in advanced economies rose by 7.3%. That was the highest increase in almost four decades. In the UK, the consumer price index even rose by more than 9%. In the euro area, the Harmonised Index of Consumer Prices rose by 8.4% on an annual average for 2022.

Initially, high inflation rates were driven mainly by energy and food prices. Energy prices recently decreased, and with them headline inflation rates. However, inflation keeps becoming more broad-based. We can see this from core inflation, which excludes energy and food prices. Core inflation keeps rising in the euro area. In February, it stood at 5.6%.

Overall, inflation rates will remain high in the near term. According to the ECB's economic projections, the inflation rate will average 5.3% this year. This is more than double our medium-term inflation target of 2%. According to the projection, we will have to wait until 2025 to see inflation approach our target by decreasing to 2.1%.

Moreover, the projection still contains significant uncertainty, and in particular upside risks. For example, high commodity and production prices could be passed on to consumers to a greater extent than previously expected. Wages may increase even more strongly than assumed in the projections.

3. Current monetary policy issues

Given this outlook, the Governing Council of the ECB could not simply assume that high inflation will return to the target level of 2% on its own. On the contrary, monetary policy has to act decisively. That's why the Governing Council of the ECB delivered six interest rate increases over the last eight months. Monetary policy rates increased by 350 basis points – the largest hike sequence ever in the euro area.

However, increasing the policy rates is not the only instrument we have at our disposal. In the first half of 2022, we discontinued net purchases under our PEPP and APP asset purchase programmes. This meant that security holdings under these programmes remained largely constant.

From this month on until June, we are reinvesting only about 50% of maturing assets under the APP. So our balance sheet is starting to shrink gradually, phasing out one additional component of the previous expansive monetary policy. From July onwards, reinvestments in the APP could be further reduced. This would support the tight monetary policy needed to rein in inflation.

With our monetary policy actions, we are dampening economic activity. This is not an unwanted side effect, but an important link in the causal chain of our monetary policy tightening. We have to tame inflation, and to do so, we have to be bold and decisive. In my view, our job is not done yet. If inflation develops as projected, further interest rate hikes have to follow in upcoming meetings.

In the event that financial market tensions continue or spread to the euro area, we are prepared to respond to preserve financial stability in the euro area. The monetary policy of the Eurosystem will do what is necessary to ensure a timely return to price stability.

But it is not monetary policy alone that influences the inflation outcome. The former Governor of the Bank of England Mervyn King once said: "If central bankers are the only game in town, I'm getting out of town!". So let's have a look at the other important player of the public sector – fiscal policy.

4. Current fiscal policies

Before touching on some general aspects of the discussion on fiscal rules, let us take a quick look at the current policy mix in the euro area. Last year, we went through tough times. Fiscal policy action was needed. Huge increases in energy prices and high inflation severely affected households and businesses. It was right to use fiscal policies to help those people who were hit hardest and could not help themselves. It was right to support viable businesses that otherwise would not have made it through the particularly difficult times.

Fiscal policy has delivered quite forcefully. Sizeable temporary measures were taken, and the fiscal support was, for the most part, relatively broad and untargeted. And the measures were mainly financed through additional deficits.

However, while expansionary fiscal measures are appropriate to restore stability in the case of a demand shock, this is not so much the case in today's circumstances. The current situation is characterised to a large extent by supply-side effects and, of particular relevance for monetary policy, by high inflationary pressures.

In such a situation, expansionary fiscal measures risk fuelling inflation further. There is a risk that monetary and fiscal policies will work against each other. Therefore, looking ahead, it is important that in the euro area, the size of fiscal policy support is reduced as soon as possible. Any further support should be well-targeted.

The easing of tension in the energy market will assist in the reduction of fiscal support. And some measures, such as the German gas and electricity price brakes, will be less costly than initially planned. It would be highly advisable not to use this kind of fiscal relief for other purposes like other expenditure or tax cuts. They should instead contribute to lowering the high deficits. In this way, fiscal policy in the euro area can support the Eurosystem's monetary policy by reducing the fiscal stimulus and by putting public finances on a more sustainable path.

5. Fiscal rules in the euro area

In general, and not just in today's specific circumstances, fiscal policy is a major factor influencing how effectively the Eurosystem fulfils its mandate of price stability. Monetary and fiscal policy have their interdependencies. Their policy stances can more or less be in harmony.

In the best case, sound fiscal policy provides the necessary bedrock for monetary policy also in a broader and longer-term perspective. In the worst case, persistently unsound fiscal policy creates significant risks that make it more difficult for central banks to fulfil their mandate. Here, we speak of the risk of fiscal dominance. What does fiscal dominance mean exactly?

The higher the level of public debt becomes, the greater the pressure on central banks to maintain favourable financing conditions in order to prevent the state from experiencing a solvency crisis.

If the central bank gives in to that pressure, it is no longer primarily following the goal of price stability. In an extreme case, the roles of fiscal and monetary policy are reversed: the central bank stabilises government debt, and the level of inflation is determined by fiscal priorities. Or, as the American Economist Michael Woodford puts it: "Fiscal dominance manifests itself through pressure on the central bank to use monetary policy to maintain the market value of government debt".

In the euro area, fiscal soundness is all the more important because a single monetary authority operates amid many sovereign fiscal authorities. Therefore, the architects of Economic and Monetary Union not only relied on market discipline by emphasising the no-bail-out principle. In addition, fiscal rules were established as an important feature of the monetary union to preserve sound public finances and to prevent fiscal pressures on monetary policy.

The fiscal rules are enshrined in the European treaties. They were regularly the subject of controversy and have been repeatedly adapted and reformed over time. A frequent criticism was that the fiscal rules might be an impediment to public investment. Others criticised the rules as being overly complex and opaque.

In my view, the fiscal rules were better than their reputation – at least when we look at their substance. The quantitative budget ceilings were suited to ensuring that high debt ratios fall swiftly. However, they were insufficiently binding and their application was often the result of political negotiations. The results were not convincing either. Highly indebted countries failed to reduce their debt levels even in good economic times.

Currently the rules are still suspended until the end of the year. During the pandemic, the general escape clause from the Stability and Growth Pact was activated. In parallel, a reform process was launched. For that purpose, the Commission initiated a consultation process in 2021. The Bundesbank also contributed its proposals to this process.

Our main recommendations were to make the quantitative targets more binding, with less discretionary exemptions and more stringent implementation. Moreover, we suggested allowing for more deficit-financed investment expenditure when debt ratios are sufficiently low, and national rainy-day funds to enhance flexibility for fiscal authorities. In addition, we proposed making fiscal rules more binding, for example by transferring fiscal surveillance to an independent institution with an exclusive focus on debt sustainability – such as the European Stability Mechanism.

Last year, the Commission presented its first reform proposal, which saw contentious debate among Member States. Last week, the Economic and Financial Affairs Council – ECOFIN – agreed on basic reform principles. I very much welcome its commitment to sustainable public finances and reduction of high debt levels. However, the current agreement appears to be largely based on the Commission's proposals of last November. I have not been convinced by the initial Commission proposals. I have expressed

doubts that such an approach will lead to an improvement in fiscal rules, but instead, I believe it will do the opposite.

The Commission proposes multiannual fiscal adjustment paths. Those paths would have to be agreed by the Commission and every Member State. Individual public debt challenges as well as reform and investment plans would have to be taken into account. In my view, such an approach is hardly compatible with the goal of a common clear, transparent, and binding fiscal framework for all Member States. It implies leeway for Member States as well as a high degree of discretionary judgement by the Commission. Monitoring compliance with fiscal rules would be highly complex, and results of sustainability analyses will crucially depend on initially defined assumptions.

These challenges will be aggravated if the rules take reforms and investment plans into account. Fiscal targets would be mixed with other policy goals. In combination with the multiannual set up, this raises concerns about whether back-loading might become the new standard of fiscal efforts. I am concerned that such a fiscal framework would fail to contribute to a reliable reduction of high sovereign debt levels. And this would be a burden for our monetary policy and would leave us feeling exposed when it comes to dealing with future economic shocks.

However, the discussion on reforming the common fiscal framework is still ongoing between the Commission and the Member States. And similar concerns have been raised, not least by the German Finance Minister Christian Lindner. So we have to wait for the final agreement. In the end, the specific design of the rules and, equally importantly, their implementation, will determine the outcome.

6. Perspectives of the European Monetary Union

Now you may ask: what's next for the euro area? Well, unless there is democratic legitimacy for a European political union, the future of the European monetary union relies on strengthening the existing governance framework.

In general, progress has been made in resolving the well-known drawbacks. The European Stability Mechanism – ESM – was established to provide financial assistance if necessary.

A macroeconomic imbalance procedure has been introduced, and reforms have been implemented to mitigate the mutual reinforcement of problems in the financial sector and public finances. In particular, the Single Supervisory Mechanism and the Single Resolution Mechanism are

designed to forestall financial distress in the banking system. However, further reform progress is needed to contain any detrimental impact of distortions from the government to the banking system.

Ultimately, however, each Member State remains responsible for its fiscal and economic policy. As regards the fiscal governance framework, fiscal rules should become less complex, less discretionary and more binding.

In my view, however, fiscal rules alone cannot ensure, together with monetary policy, price stability. That means financial markets have to play their part by pricing sovereign risks adequately and thereby support fiscal discipline.

Borrowing at European Union level to finance current expenditure, such as with Next Generation European Union transfers, should remain an exception. This guarantees that potentially rising risk premia for government debt constitute a significant incentive for sound fiscal policy. Capital market disciplining would be helpful in this respect.

The debt ratio in the euro area increased rapidly during the pandemic. Politicians have to find a proper way to bring it down. Sustainable public finances secure capital market access and avoid potential conflicts with monetary policy. I hope the current reform of the governance framework will not culminate in a rules-free setting. Sustainable public finances are in the interest of taxpayers as well as fiscal authorities and central banks.

7. Closing remarks

Ladies and gentlemen,
let me conclude.

From a central banker's perspective, fiscal rules are indeed very important. The economist Karl Brunner expressed this with the following words:

"The crucial conclusion from [-] stability analysis suggests that a stable, non-inflationary monetary regime is unlikely to persist in the absence of a fiscal regime effectively containing the average deficit."

In this context, the direction of the current reform process causes me concern. We will see whether the answers to questions still under discussion will improve the outcome. And we will see how any new rules will actually be implemented.

In my view, the European Union weathered the crises of the last few years fairly well. The EU countries reacted responsibly and successfully to the

economic shocks caused by the pandemic and energy crisis. Certainly, we would not have been better off during the crisis had we been dealing with twenty different European currencies. Working together to find a common European response is worth the effort. I am firmly convinced that monetary union is beneficial to all members.

Thank you.

To read more:
https://www.bundesbank.de/en/press/speeches/current-challenges-facing-the-european-monetary-union-906784

Number 5

Development of a National Spectrum Strategy

National Telecommunications and Information Administration, Department of Commerce - Request for comments.

National Telecommunications and Information Administration
United States Department of Commerce

SUMMARY: The National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, seeks public comment on the development and implementation of a National Spectrum Strategy for the United States.

Through this Request for Comments, NTIA seeks broad input from interested stakeholders, including private industry (specifically including developers and end-users of spectrum-based technologies and services, and contractors for federal missions), academia, civil society, the public sector, and others on three proposed pillars of the National Spectrum Strategy set forth below.

DATES: Parties should file their comments no later than April 17, 2023.

ADDRESSES: All electronic comments on this action, identified by Regulations.gov docket number NTIA– 2023–0003, may be submitted through the Federal e-Rulemaking Portal at https://www.regulations.gov.

The docket established for this proceeding can be found at www.Regulations.gov, NTIA– 2023–0003. Click the "Comment Now!" icon, complete the required fields, and enter or attach your comments.

Responders should include a page number on each page of their submissions. Please do not include in your comments information of a confidential nature, such as sensitive personal information.

All comments received are part of the public record and generally will be posted to Regulations.gov and the NTIA website without change. All personally identifiable information (e.g., name, address) voluntarily submitted by the commenter may be publicly accessible.

For more detailed directions regarding the content of comment submissions, please see the "Request for Comments" section below. Those encountering any difficulties with the prescribed formatting and uploading directions should notify Mr. Alden at the contact information listed below at least ten (10) business days before the filing deadline.

NTIA welcomes views on the NSS pillars as detailed in this notice, and these views may be reflected, at the agency's discretion, in the ensuing development of the NSS and implementation plan.

These public comments are being gathered in conjunction with a series of public listening sessions, which will be held concurrently with the comment period of this RFC. Schedules and instructions for attending and speaking at the public listening sessions will be available on NTIA's website at https:// www.ntia.gov.

Background

America is increasingly dependent on secure and reliable access to radio frequency spectrum. Sufficient access to spectrum is vital to national security, critical infrastructure, transportation, emergency response, public safety, scientific discovery, economic growth, competitive next-generation communications, and diversity, equity, and inclusion.

Increased spectrum access will also advance U.S. innovation, connectivity, and competition, create high-paying and highly skilled jobs, and produce improvements to the overall quality of life.

Access to more spectrum, in short, will help the United States continue to lead the world in advanced technology and enhance our national and economic security.

Spectrum access, however, must be managed responsibly and efficiently. NTIA jointly manages the nation's spectrum resources with the Federal Communications Commission.

NTIA is requesting comments from interested parties to help inform the development of a national spectrum strategy, which is needed for the U.S. to plan effectively for its current and future spectrum needs.

As part of this effort, and to support the need for greater spectrum access, NTIA—in collaboration with the Federal Communications Commission and in coordination with its other federal partners—endeavors to identify at least 1,500 megahertz of spectrum for in-depth study to determine whether that spectrum can be repurposed to allow more intensive use.

The Department of Commerce is committed to developing a national spectrum strategy based upon collaboration with both federal and non-federal stakeholders, including Tribes, and on data-driven decision-making, to fully address the needs of spectrum reliant services and missions, including but not limited to:

• Fixed and mobile wireless broadband services;

• Next-generation satellite communications and other space-based systems;
• Advanced transportation technologies;

• Industrial and commercial applications, (i.e., manufacturing, agriculture, and utilities);

• Wireless medical devices and telemedicine;

• Internet of Things (IoT) and smart cities;

• National defense and homeland security;

• Safeguarding the national airspace and ports;

• Securing the Nation's critical infrastructure;

• Earth and space exploration and research; and

• Climate monitoring and forecasting, and other scientific endeavors.

To read more:
https://www.regulations.gov/document/NTIA-2023-0003-0001

Number 6

Is Your Cybersecurity Strategy Falling Victim to These 6 Common Pitfalls?

NIST research reveals misconceptions that can affect security professionals — and offers solutions.

Here's a pop quiz for cybersecurity pros: Does your security team consider your organization's employees to be your allies or your enemies? Do they think employees are the weakest link in the security chain? Let's put that last one more broadly and bluntly: Does your team assume users are clueless?

Your answers to those questions may vary, but a recent article by National Institute of Standards and Technology (NIST) computer scientist Julie Haney highlights a pervasive problem within the world of computer security: Many security specialists harbor misconceptions about lay users of information technology, and these misconceptions can increase an organization's risk of cybersecurity breaches. These issues include ineffective communications to lay users and inadequately incorporating user feedback on security system usability.

"Cybersecurity specialists are skilled, dedicated professionals who perform a tremendous service in protecting us from cyber threats," Haney said. "But despite having the noblest of intentions, their community's heavy dependence on technology to solve security problems can discourage them from adequately considering the human element, which plays a major role in effective, usable security."

The human element refers to the individual and social factors impacting users' security adoption, including their perceptions of security tools. A security tool or approach may be powerful in principle, but if users perceive it to be a hindrance and try to circumvent it, risk levels can increase.

A recent report estimated that 82% of 2021 breaches involved the human element, and in 2020, 53% of U.S. government cyber incidents resulted from employees violating acceptable usage policies or succumbing to email attacks.

Haney, who has a comparatively unusual combination of expertise in both cybersecurity and human-centered computing, wrote her new paper, "Users Are Not Stupid: Six Cyber Security Pitfalls Overturned," to help the security and user communities become allies in mitigating cyber risks.

"We need an attitude shift in cybersecurity," Haney said. "We're talking to users in a language they don't really understand, burdening them and belittling them, but still expecting them to be stellar security practitioners. That approach doesn't set them up for success. Instead of seeing people as obstructionists, we need to empower them and recognize them as partners in cybersecurity."

The paper details six pitfalls that threaten security professionals (also available in this handout), together with potential solutions:

1. **Assuming users are clueless.** Though people do make mistakes, belittling users can result in an unhealthy "us vs. them" relationship between users and cybersecurity professionals. Research on nonexperts reveals that users are simply overwhelmed, often suffering from security fatigue. A potential solution involves building positive relationships with users while empowering them to be active, capable partners in cybersecurity.

2. **Not tailoring communications to the audience.** Security pros often use technical jargon that reduces audience engagement, and they may fail to tailor lessons in ways that appeal to what users care about in their daily lives. Several strategies can help, from focusing on plain-language messages to presenting information in multiple formats to enlisting the help of an organization's public affairs office.

3. **Unintentionally creating insider threats due to poor usability.** Users who are already pushed to their limit by time pressures or other distractions can unwittingly become threats themselves, as they become prone to poor decision making. (As one example, complex password policies can inspire poor decisions, such as using the same password across multiple accounts.)

Offloading the user's security burden can help, such as by exploring whether more mail filtering can be done by the server so that fewer phishing emails get through. Also, when piloting new security solutions, testing the approach first with a small group of users can reveal potential confusion that can be corrected before a wider rollout.

4. **Having too much security.** "Too much" implies that a security solution may be too rigid or restrictive for the specific job context. While always using the most secure tools available sounds wise in principle, some users can find the resulting complexity stifling for daily work, leading them to violate security policies more frequently. Instead of a "one size fits all" stance, performing a risk assessment using a risk management framework

can help determine what level of cybersecurity best fits a given environment.

5. **Depending on punitive measures or negative messaging to get users to comply.** Negative reinforcement is common within organizations today: Examples include disabling user accounts if security training is not completed and publicly shaming individuals who cause cybersecurity incidents.

Whether or not these measures work in the short term, they breed resentment toward security in the long term. Instead, offering positive incentives for employees who respond to threats appropriately can improve attitudes toward security, as can taking a collaborative approach with struggling users.

6. **Not considering user-centered measures of effectiveness.** As employees often find security training to be a boring, check-the-box activity, how much of it are they actually retaining? Without direct user feedback and concrete indicators of behavior, organizations can struggle to answer that question.

It helps to think of concrete metrics as symptom identifiers — such as help desk calls that reveal users' pain points and incidents like phishing clicks that can show where users need more support.

After identifying the symptoms, security teams can use surveys, focus groups or other direct interactions with users to determine the root cause of problems, as well as improve their solutions.

Haney stressed that not all security professionals have these misconceptions; there are certainly security teams and organizations making positive progress in recognizing and addressing the human element of security. However, these misconceptions remain prevalent within the community.

Haney said that though the issue with neglecting the human element has been well known for years — her paper cites evidence from industry surveys, government publications and usable security research publications, as well as her research group's original work — there is a gap between research findings and practice.

"There has been a lot of research into this issue, but the research is not getting into the hands of people who can do something about it. They don't know it exists," she said. "Working at NIST, where we have a connection to

all sorts of IT experts, I saw the possibility of bridging that gap. I hope it gets into their hands."

To read more:
https://www.nist.gov/news-events/news/2023/03/your-cybersecurity-strategy-falling-victim-these-6-common-pitfalls

Number 7

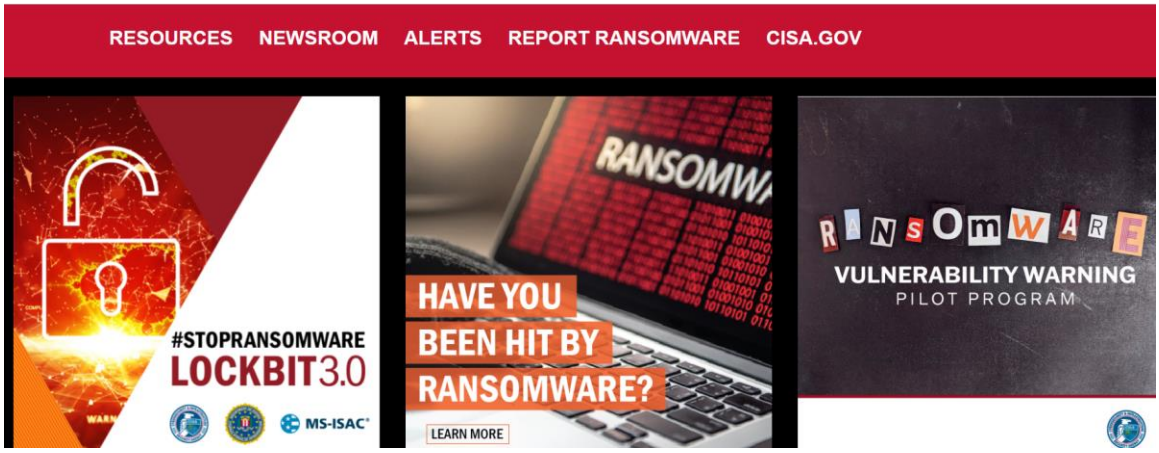
Ransomware Vulnerability Warning Pilot (RVWP)

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which the US President signed into law in March 2022, required CISA to establish the RVWP (see Section 105 [6 U.S.C. § 652 note]).

Organizations across all sectors and of all sizes are too frequently impacted by damaging ransomware incidents. Many of these incidents are perpetrated by ransomware threat actors using known vulnerabilities.

By urgently fixing these vulnerabilities, organizations can significantly reduce their likelihood of experiencing a ransomware event. In addition, organizations should implement other security controls as described on stopransomware.gov.

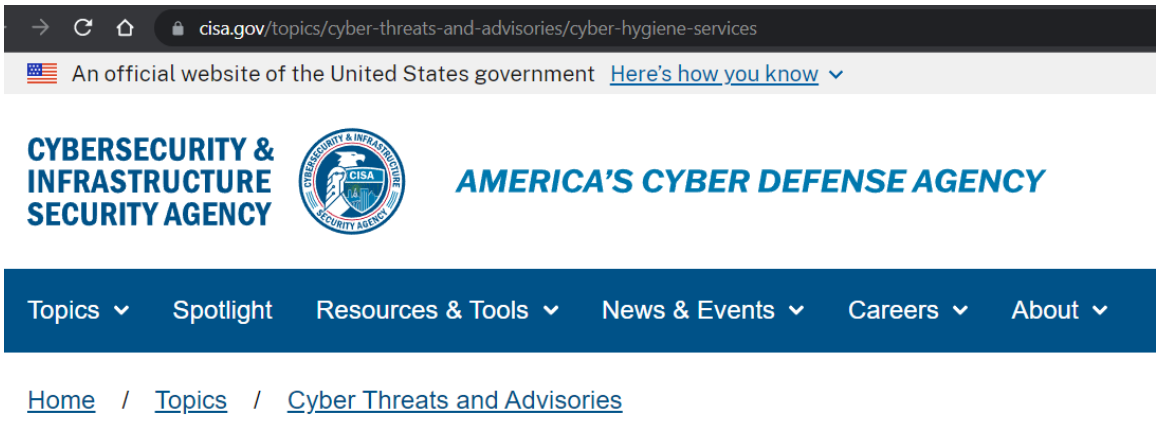


However, most organizations may be unaware that a vulnerability used by ransomware threat actors is present on their network. Through the Ransomware Vulnerability Warning Pilot (RVWP), which started on January 30, 2023, CISA is undertaking a new effort to warn critical infrastructure entities that their systems have exposed vulnerabilities that may be exploited by ransomware threat actors

As part of RVWP, CISA leverages existing authorities and technology to proactively identify information systems that contain security vulnerabilities commonly associated with ransomware attacks.

Once CISA identifies these affected systems, our regional cybersecurity personnel notify system owners of their security vulnerabilities, thus enabling timely mitigation before damaging intrusions occur.

CISA accomplishes this work by leveraging its existing services, data sources, technologies, and authorities, including CISA's Cyber Hygiene Vulnerability Scanning service and the Administrative Subpoena Authority granted to CISA under Section 2209 of the Homeland Security Act of 2002.



You may visit:
https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services

To read more:
https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot

Number 8

Joint communication on the update of the EU Maritime Security Strategy and its Action Plan

An enhanced EU Maritime Security Strategy for evolving maritime threats

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Maritime security is vital to the European Union (EU) and to its Member States. Together, the EU's Member States form the largest combined exclusive economic zone in the world.

The EU economy depends greatly on safe and secure oceans: over 80% of global trade is seaborne, about two-thirds of the world's oil and gas supply is either extracted at sea or transported by sea, and up to 99% of global data flows are transmitted through undersea cables.

To ensure effective ocean governance, to protect our oceans and seabeds, and to unlock the full potential of the sustainable blue economy, the global maritime domain must be secure.

Since 2014, the European maritime security strategy (EUMSS) and action plan have provided the framework for addressing security challenges at sea.

The strategy has stimulated closer cooperation between civilian and military authorities, in particular through information exchange. It has helped promote rules-based governance at sea and has given a boost to international cooperation. It has strengthened the EU's autonomy and capacity to respond to maritime security threats.

The EU plays an increasingly important role as a global maritime security provider, by conducting its own naval operations, e.g. Atalanta and Irini, implementing the Coordinated Maritime Presences (CMP) concept, and promoting maritime situational awareness and cooperating with a wide range of external partners.

In addition, the Copernicus maritime and border surveillance operational systems, implemented by the European Maritime Safety Agency (EMSA) and the European Border and Coast Guard Agency (Frontex), provide spacebased observations, complementing the navigation services of Galileo satellites.

The overall strategic environment is experiencing drastic changes. Reshaped by the climate crisis and environmental degradation and

aggravated by Russia's illegal and unjustified military aggression against Ukraine, it demands more action from the EU as an international security provider. In line with the EU Strategic Compass for Security and Defence, this update of the EUMSS and its action plan aims to respond to the new challenges.

It is an opportunity to drive forward sustainable solutions to maritime security problems. It is also an opportunity to further enhance the EU's role internationally and further secure the EU's access to an increasingly contested maritime domain.

The updated EUMSS is a framework for the EU to take further action to protect its interests at sea, and to protect its citizens, values and economy. The aim is to promote international peace and security while adhering to the principle of sustainability and protecting biodiversity.

The EU and its Member States will implement the updated strategy, in line with their respective competences.

Manage risks and threats

In line with the Strategic Compass, the EU and its Member States will improve their collective ability to defend their security and increase their resilience and preparedness for maritime security challenges, including hybrid and cyber threats.

The EU and its Member States should be able to react quickly, with coordinated civilian and military capabilities. Fighting climate change and environmental degradation are among the EU's top political priorities that are reflected in its external action through many thematic or geographical strategies such as Global Gateway or the Strategy for Cooperation in the Indo-Pacific, as well as through EU diplomatic outreach and EU Climate Diplomacy.

The EU has already taken significant steps to achieve climate neutrality by 2050, and will take further action on problems interlinked with climate change, environmental degradation and security.

The High Representative and the Commission will present a Joint Communication on the nexus between climate change, environmental degradation and security and defence in mid2023.

It will include, inter alia, proposals for tools assessing the causes and consequences of climate change and environmental degradation on the maritime sector, on maritime infrastructure, as well as on natural and

man-made features of coastal areas, including as regards early warning, evidence-based research and satellite imagery (e.g. through Copernicus programme).

In the Arctic, the ice caps are melting, sea ice is receding, new shipping routes are gradually opening up, and the consequent increase in human activities is expected to generate or aggravate threats to the environment and to local communities.

In this regard the Joint Communication on "A stronger EU engagement for a greener, peaceful and prosperous Arctic" must be further operationalised as soon as possible in particular with regard to zero emission shipping in the Arctic Ocean, sustainable mining of critical raw materials, and sustainable development of the Arctic regions.

Protecting critical infrastructure in the maritime domain also remains a key priority. The EU should complement the role of Member States in building up the resilience of critical maritime infrastructure such as pipelines or undersea cables that run across national maritime borders.

It should improve current risk assessments on undersea cables and complement them with response options and mitigating measures building on cross-sectoral expertise and capacities. It is imperative to provide continued support to Member States to develop underwater protective assets and counter-drone solutions.

In addition, the EU should continue to facilitate the coexistence of offshore renewable energy with defence activities, as advocated in the offshore renewable strategy.

With the Directive on the resilience of critical entities and the revised Directive on the security of network and information systems (NIS 2 Directive), the EU is at the forefront of relevant developments, with a comprehensive legal framework allowing it to upgrade both the physical and the cyber resilience of critical entities and infrastructure.

The EU should step up cooperation with key partners and relevant non-EU countries in this area, in particular through the EU-NATO structured dialogue on resilience and the task force on resilience of critical infrastructure.

The EU faces the additional challenge posed by large quantities of unexploded ordnance (UXO) and chemical weapons originating from the First and Second World Wars lying in sea basins around the EU.

This challenge is further exacerbated by Russia's military aggression against Ukraine, resulting in a large number of mines present in the Black Sea.

The type, location and quantity of this ordnance are poorly documented, which poses risks to maritime safety and security, to the environment (due to possible release of chemicals) and to blue economy activities (e.g. the construction of offshore renewable energy sites).

Building on existing successful projects, the EU should address this issue urgently and comprehensively, mitigating the environmental risks associated with UXO and their disposal.

It will also be very important to dispose safely of UXO and mines left in the Black Sea, as soon as security and political conditions allow.

Maritime security is also undermined by foreign actors, both due to risks related to foreign direct investment in critical infrastructure, and to information manipulation and interference by such actors.

These issues will be addressed through relevant instruments and frameworks; e.g. foreign direct investment will be screened in line with the relevant Regulation.

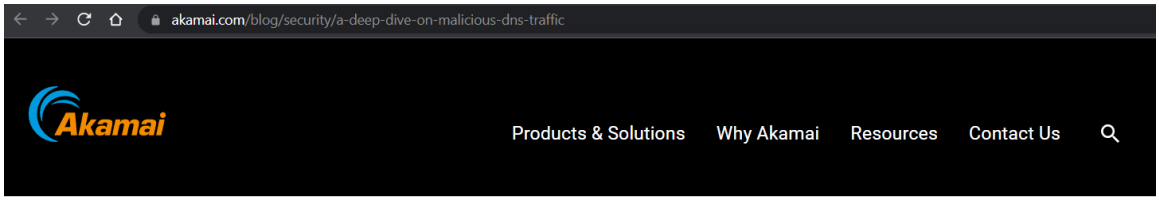
To read more:
https://oceans-and-fisheries.ec.europa.eu/system/files/2023-03/join-2023-8_en.pdf

Number 9

DNS data shows one in ten organisations have malware traffic on their networks

National Cyber Security Centre

An investigation by Akamai has shown that between 10% and 16% of organisations had Domain Name System (DNS) traffic originating on their network towards command-and-control (C2) servers associated with known botnets and various other malware threats.



Attack Superhighway: A Deep Dive on Malicious DNS Traffic

The report also showed that over 9% of devices that generated C2 traffic, did so to domain names associated with known ransomware threats. Of these, REvil and LockBit were the most common ones.

The NCSC has produced guidance on the selection and deployment of protective DNS and there is also the Protective DNS for public sector organisations at:
https://www.ncsc.gov.uk/guidance/protective-dns-for-private-sector

To read more:
https://www.ncsc.gov.uk/report/threat-report-24th-march-2023

https://www.akamai.com/blog/security/a-deep-dive-on-malicious-dns-traffic

Number 10

Preventing the Improper Use of CHIPS Act Funding

The CHIPS Act (the Act) established an incentives program to reestablish and sustain U.S. leadership across the semiconductor supply chain.

To ensure that funding provided through this program does not directly or indirectly benefit foreign countries of concern, the Act includes certain limitations on funding recipients, such as prohibiting engagement in certain significant transactions involving the material expansion of semiconductor manufacturing capacity in foreign countries of concern and prohibiting certain joint research or technology licensing efforts with foreign entities of concern.

The Department of Commerce (Department) is issuing, and requesting public comments on, a proposed rule to set forth terms related to these limitations and procedures for funding recipients to notify the Secretary of Commerce (Secretary) of any planned significant transactions that may be prohibited.

Background

Semiconductors are essential components of electronic devices that enable telecommunications and grid infrastructure, run critical business and government information technology and operational technology systems, and are necessary to a vast array of products, from automobiles to fighter jets. Recognizing the criticality of supply chain security and resilience for semiconductors and related products, the President signed the Executive Order on America's Supply Chains shortly after taking office in February 24, 2021.

This Executive order, among other things, directed several Departments to undertake assessments of critical supply chains; several of the resulting reports address microelectronics and related subcomponent supply chains.

The resulting June 2021 White House Report on Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth highlighted the insufficient domestic manufacturing capacity for semiconductors. The White House Report noted that the United States lacks advanced semiconductor manufacturing capabilities and is dependent on geographically concentrated and in some cases potentially unreliable sources of supply.

It recommended dedicated funding to advance semiconductor manufacturing, and research and development to support critical manufacturing, industrial, and defense applications.

In August 2022, the Congress passed the CHIPS Act of 2022, which amended Title XCIX of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, also known as the Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act.

Together, these statutory provisions (collectively, the CHIPS Act or Act), establish a semiconductor incentives program (CHIPS Incentives Program) that will provide funding, including via grants, cooperative agreements, loans, loan guarantees, and other transactions, to support investments in the construction, expansion, and modernization of facilities in the United States for the fabrication, assembly, testing, advanced packaging, production, or research and development of semiconductors, materials used to manufacture semiconductors, or semiconductor manufacturing equipment.

The CHIPS Incentives Program aims to strengthen the security and resilience of the semiconductor supply chain by mitigating gaps and vulnerabilities. It aims to ensure a supply of secure semiconductors essential for national security and to support critical manufacturing industries. It also aims to strengthen the resilience and leadership of the United States in semiconductor technology, which is vital to national security and future economic competitiveness of the United States.

The CHIPS Incentives Program is administered by the CHIPS Program Office (CPO) within the National Institute of Standards and Technology (NIST) of the United States Department of Commerce. CPO is separately issuing Notices of Funding Opportunity (NOFO) that lay out the procedures by which interested organizations may apply for CHIPS Incentives Program funds, and criteria under which applications will be evaluated.

To protect national security and the resiliency of supply chains, CHIPS Incentives Program funds may not be provided to a foreign entity of concern, such as an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a country that is engaged in conduct that is detrimental to the national security of the United States. This proposed rule incudes a detailed explanation of what is meant by foreign entities of concern, as well as a definition of “owned by, controlled by, or subject to the jurisdiction or direction of.”

In further support of U.S. national security interests, CHIPS Incentives Program recipients (funding recipients) are required by the Act to enter

into an agreement (required agreement) with the Department restricting engagement by the funding recipient or its affiliates in any significant transaction involving the material expansion of semiconductor manufacturing capacity in foreign countries of concern.

In recognition that some potential applicants for CHIPS Incentives may have existing facilities in foreign countries of concern, and to minimize potential supply chain disruptions, the Act includes exceptions for certain transactions involving older (legacy) semiconductor manufacturing in a foreign country of concern.

A funding recipient must notify the Secretary of any planned significant transactions of the funding recipient or its affiliates involving the material expansion of semiconductor manufacturing capacity in a foreign country of concern, including in cases where it believes the transaction is allowed under the exceptions in 15 U.S.C. 4652(a)(6)(C)(ii).

Terms related to this notification requirement are defined in Subpart A of this rule. The Secretary will provide direct notice to the funding recipient that a review of a transaction is being conducted and, later, that the Secretary has reached an initial determination regarding whether the transaction is prohibited. Funding recipients may submit additional information or request that the initial determination be reconsidered, after which the Secretary will provide a final determination.

In making determinations, the Secretary will consult with the Director of National Intelligence and the Secretary of Defense.

The Secretary will initiate review of transactions by funding recipients through self-reported notifications; the Secretary also may initiate a review of non-notified transactions, including based on information provided by other government agencies or information from other sources.

Failure by a funding recipient (or its affiliate) to comply with this restriction on semiconductor manufacturing capacity expansion in foreign countries of concern may result in recovery of the full amount of Federal financial assistance provided to the funding recipient (referred to in the Act as the “Expansion Clawback.”)

The Act also prohibits funding recipients from knowingly engaging in any joint research or technology licensing effort with a foreign entity of concern that relates to a technology or product that raises national security concerns as determined by the Secretary and communicated to the funding recipient before engaging in such joint research or technology licensing. A funding recipient's required agreement will include a commitment that the funding

recipient and its affiliates will not conduct prohibited joint research or technology licensing. Failure to comply with this restriction may also result in recovery of the full amount of Federal assistance (referred to in the Act as the “Technology Clawback.”)

To read more:
https://www.federalregister.gov/documents/2023/03/23/2023-05869/preventing-the-improper-use-of-chips-act-funding

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

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

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

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

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

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

3. *Training and Certification* – Become:

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

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

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

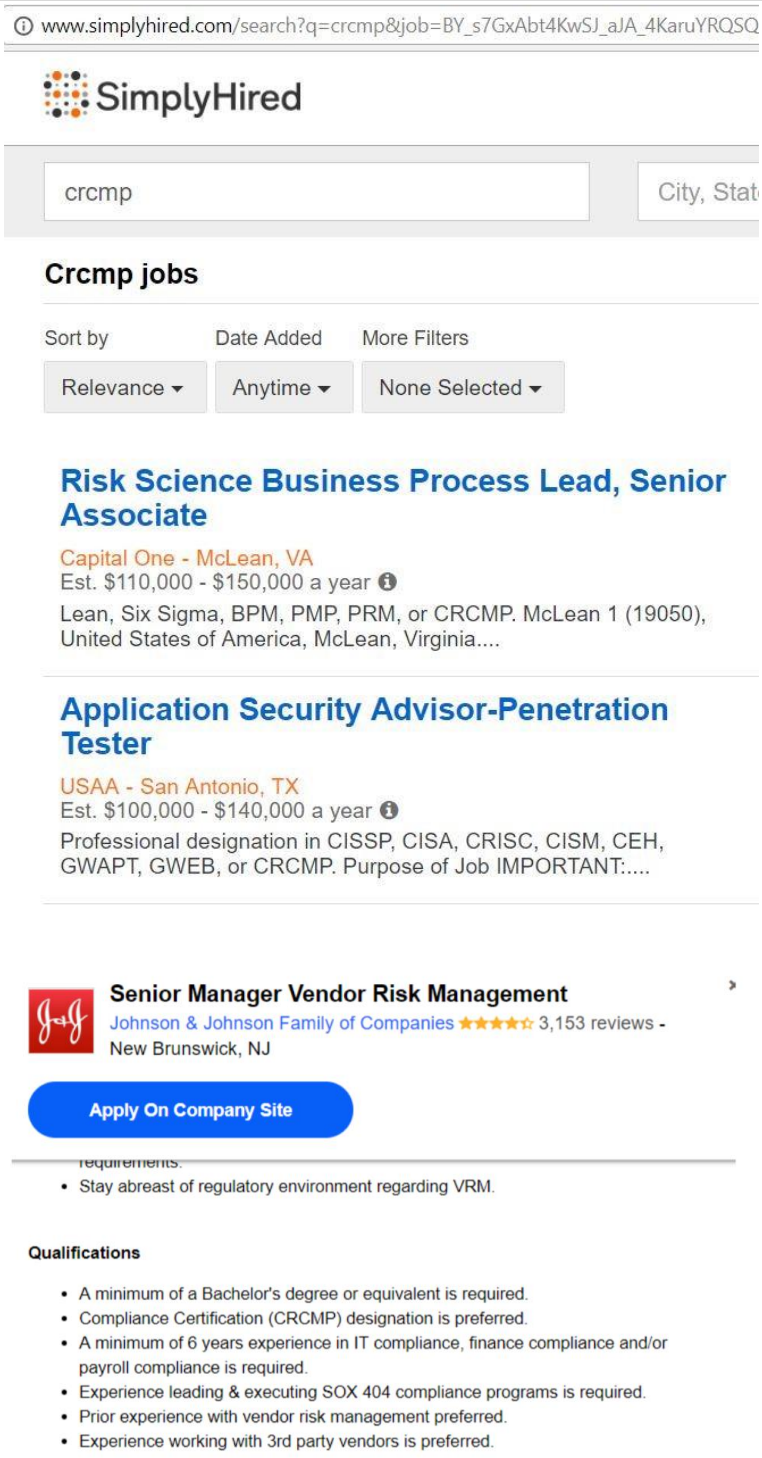
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

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

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

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



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

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

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

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

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

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

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

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

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