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, October 4, 2021

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,

The emergence of large technology firms (big techs) represents a major source of disruption to the financial system and the economy.

These are the first words in the new paper with title "*Big tech regulation: what is going on?*" (Financial Stability Institute (FSI), Insights on policy implementation No 36). The FSI is one of the bodies hosted by the Bank of International Settlements at its headquarters in Basel, Switzerland.

The paper continues: "Big techs have expanded the available range of financial products and services, often with enhanced customer experience. However, the ease and speed with which these companies can scale up their activities and expand into finance may generate pronounced concentration dynamics.
This could significantly affect the adequate functioning of the financial system and may damage market contestability and eventually increase

operational vulnerabilities due to the excessive reliance of market players on the services provided by big techs."

The paper continues: "*Different jurisdictions have moved to adjust their policy frameworks to cope with the risks presented by big techs.*

In particular, a number of policy initiatives have emerged in China, the European Union (EU) and the United States over the last few years in the areas of competition, data protection and data-sharing, operational resilience, conduct of business and financial stability.

These initiatives generally seek to achieve a balance between addressing the different risks posed by big techs and preserving the benefits they bring in terms of market efficiency and financial inclusion."

To achieve this balance is not going to be easy, especially when China becomes an example. But as Albert Einstein has said, *life is like riding a bicycle. To keep your balance, you must keep moving.*

There are some interesting parts in the paper, where China looks more advanced than the States. For example, I was surprised (a polite expression) with the following Table, with sources including "authors' compilation":

Data protection and data-sharing approaches in the EU, US and China — Table 2

	EU	US	China
Data protection			
Collection and use of personal data			
Of which: Lawfulness, fairness and transparency	√	√	√
Purpose specification	√	*	√
Security	√	√	√
Users' data rights			
Of which: Consent and access	√	*	√
Rectification and deletion	√	*	√
Data portability	√	*	√
Data-sharing			
Open banking			
*Approach: prescriptive, facilitative**, market-driven****	Prescriptive	Market	Market

Legend: Comprehensive | Partial | Early stages

* While there is no federal law addressing these elements at present, they are subject to ongoing debate.

** Under a facilitative approach, jurisdictions issue guidance and recommended standards, and release open API standards and technical specifications.

*** No explicit rules or guidance that either require banks or prohibit them to share customer-permissioned data with third parties.

Sources: BCBS (2019) and authors' compilation.

According to the paper, the "proposed data protection frameworks in the US and the finalised framework in China show a high degree of alignment with the EU's GDPR".

We also read: "Chinese authorities have engaged in a number of ex post supervisory actions against big techs. The initial public offering (IPO) of Ant Group rapidly unravelled after regulators blocked it for not complying with listing criteria and disclosure requirements.

In April 2021, the group was forced to restructure and its affiliate, Alibaba, was fined RMB 18.23 billion ($2.8 billion) – the biggest antitrust fine levied in China to date. Additionally, regulators ordered 34 Chinese internet companies to undergo rectification of their business models for potential anticompetitive practices.

A week later, the China Securities Regulatory Commission (CSRC) issued new rules aimed at restricting the listing of fintech and "model innovation enterprises" on the Shanghai Stock Exchange Science and Technology Innovation Board."

I am not sure I understand perfectly what is going on. It looks like China is becoming a role model in regulation worthy of imitation. I am surprised, and I disagree.

Read more at number 2 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 7)

Inthanon-LionRock to mBridge: Building a multi CBDC platform for international payments

Joint report by the BIS Innovation Hub Hong Kong Centre, the Hong Kong Monetary Authority, the Bank of Thailand, the Digital Currency Institute of the People's Bank of China, the Central Bank of the United Arab Emirates.

Number 2 (Page 10)

FSI Insights on policy implementation No 36

Big tech regulation: what is going on?

By Juan Carlos Crisanto, Johannes Ehrentraud, Aidan Lawson and Fernando Restoy

BIS

Number 3 (Page 13)

Moving forward in securing Online Trust via the Digital Wallets

The 2021 Trust Service Forum allows stakeholder communities to engage in open discussions on securing trust services online and on the future of the EU Digital Identity Framework.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Number 4 (Page 16)

Methodology for a Sectoral Cybersecurity Assessment

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Number 5 (Page 20)

Jens Weidmann: Exploring a digital euro

Dr Jens Weidmann, President of the Deutsche Bundesbank and Chair of the Board of Directors of the Bank for International Settlements, at the digital conference "Fintech and the global payments landscape – exploring new horizons".

Number 6 (Page 21)

Rule governing Board determination under the Holding Foreign Companies Accountable Act

Number 7 (Page 23)

Statement in Support of Adoption of PCAOB Rule 6100, Board Determinations Under the Holding Foreign Companies Accountable Act

Duane M. DesParte, Acting Chairperson - PCAOB Open Board Meeting

Number 8 (Page 25)

"We expect to let certain exemptions expire at the end of the year"

Raimund Röseler, Chief Executive Director of Banking Supervision, on the current state of the banks

Number 9 (Page 31)

Conti Ransomware Attacks Impact Healthcare and First Responder Networks

Number 10 (Page 33)

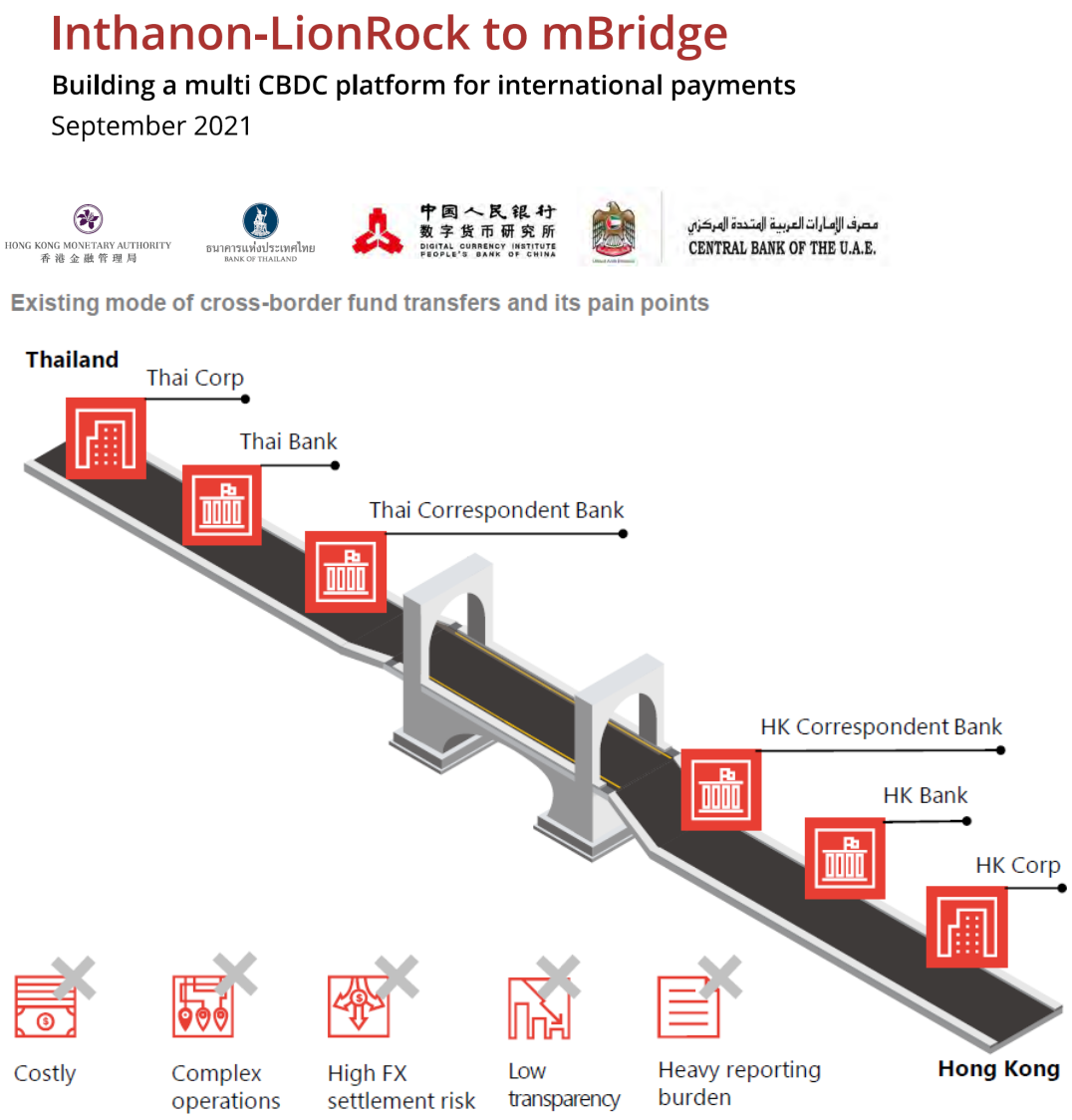
Disrupting Exploitable Patterns in Software to Make Systems Safer

Program pushes secure system design by developing ways to stop cyber attackers' from executing unintended computations on critical systems

Number 1

Inthanon-LionRock to mBridge: Building a multi CBDC platform for international payments

Joint report by the BIS Innovation Hub Hong Kong Centre, the Hong Kong Monetary Authority, the Bank of Thailand, the Digital Currency Institute of the People's Bank of China, the Central Bank of the United Arab Emirates.



In the absence of multilateral solutions for cross-border payments, correspondent banks currently act as bridges, moving payments from one jurisdiction to another.

To achieve this, they have built extensive correspondent banking networks and arrangements.

While serving a critical economic role, these networks and arrangements also introduce more intermediary steps in the system, as correspondent

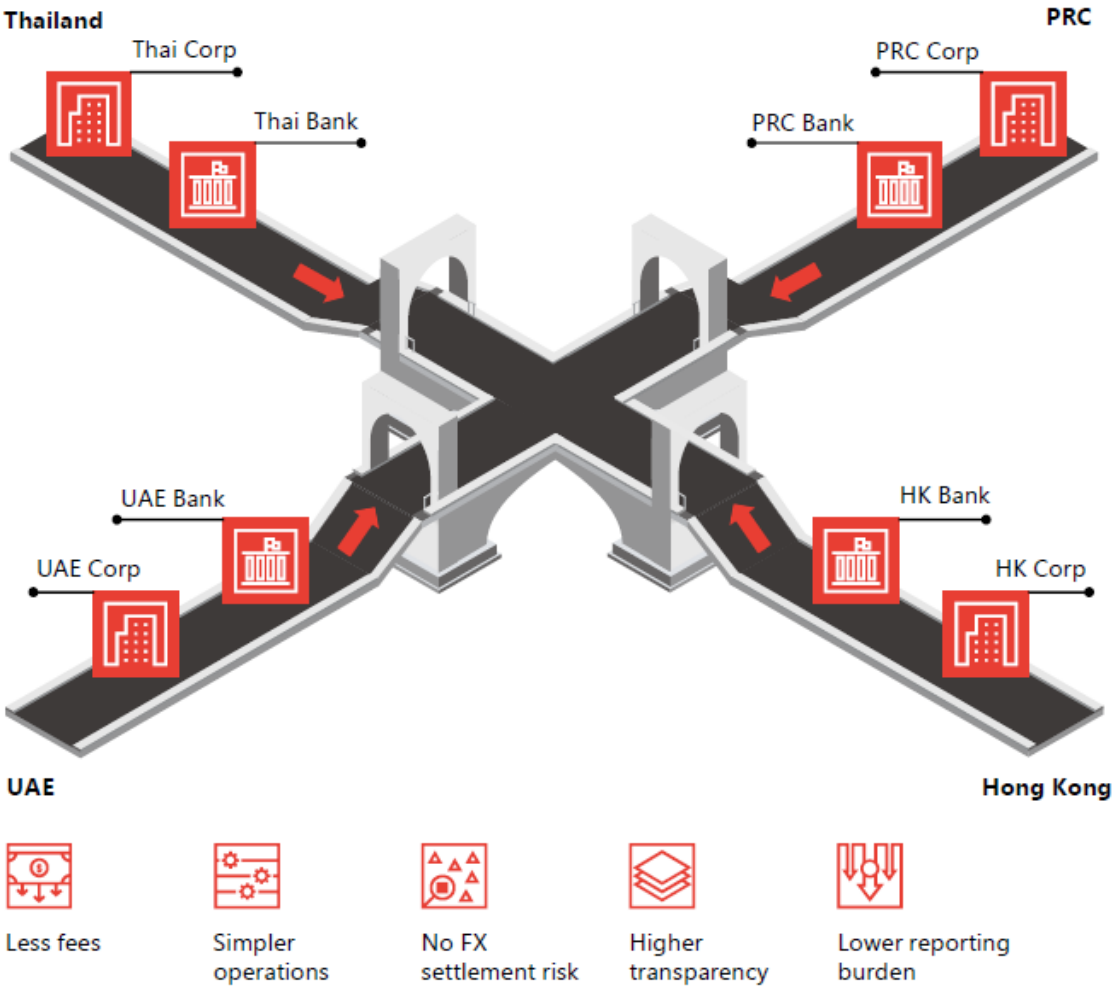
banks are spread out across multiple time zones and different operating hours.

This leads to increased operational complexity, possible bottlenecks and duplication. For example, know-your-customer (KYC) processes are repeated by every bank in the correspondent banking process flow.

As illustrated in the published report of Inthanon-LionRock Phase 1 this in turn leads to higher cost and slower speed of cross-border payments.

This process complexity also is paired with high FX settlement risk, low transparency and a high reporting burden.

Inthanon-LionRock and mBridge Model



Source: Adapted from Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020

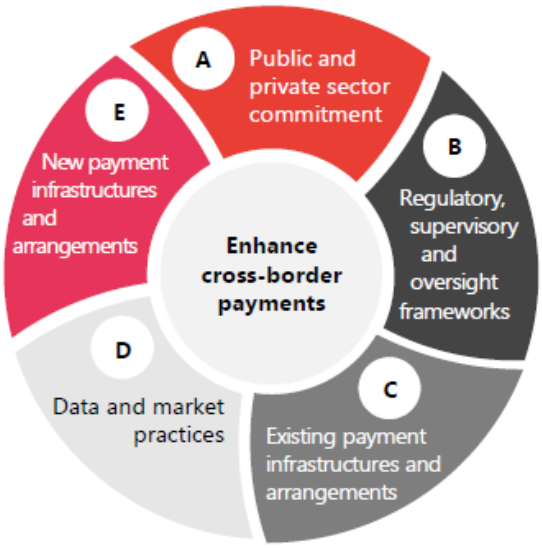
Roadmap to enhancing cross-border payments

1. Develop common cross-border payments vision and targets
2. Implement international guidance and principles
3. Define common features of cross-border payment service levels

A

4. Align regulatory, supervisory and oversight frameworks
5. Apply AML/CFT consistently and comprehensively
6. Review interaction between data frameworks and cross-border payments
7. Promote safe payment corridors
8. Foster KYC and identity information-sharing

B



C

9. Facilitate increased adoption of PvP
10. Improve (direct) access to payment systems
11. Explore reciprocal liquidity arrangements
12. Extend and align operating hours
13. Pursue interlinking of payment systems

D

14. Adopt a harmonised version of ISO 20022 for message formats
15. Harmonise API protocols for data exchange
16. Establish unique identifiers with proxy registries

E

17. Consider the feasibility of new multilateral platforms and arrangements for cross-border payments
18. Foster the soundness of global stablecoins arrangements
19. Factor an international dimension into CBDC designs

Source: Enhancing cross-border payments: building blocks of a global roadmap Stage 2 report to the G20, July 2020[18]

To read more: https://www.bis.org/publ/othp40.htm

Number 2

FSI Insights on policy implementation No 36

Big tech regulation: what is going on?

By Juan Carlos Crisanto, Johannes Ehrentraud, Aidan Lawson and Fernando Restoy

BIS

The emergence of large technology firms (big techs) represents a major source of disruption to the financial system and the economy.

Big techs have expanded the available range of financial products and services, often with enhanced customer experience. However, the ease and speed with which these companies can scale up their activities and expand into finance may generate pronounced concentration dynamics.

This could significantly affect the adequate functioning of the financial system and may damage market contestability and eventually increase operational vulnerabilities due to the excessive reliance of market players on the services provided by big techs.

Different jurisdictions have moved to adjust their policy frameworks to cope with the risks presented by big techs.

In particular, a number of policy initiatives have emerged in China, the European Union (EU) and the United States over the last few years in the areas of competition, data protection and data-sharing, operational resilience, conduct of business and financial stability.

These initiatives generally seek to achieve a balance between addressing the different risks posed by big techs and preserving the benefits they bring in terms of market efficiency and financial inclusion.

Thus far, competition has been the policy area where the most initiatives have been conducted and a paradigm shift is emerging.

Given the large potential for big techs to abuse their technological and data superiority to quickly dominate different market segments and adopt anticompetitive practices, preserving market contestability has become a top priority for authorities in China, the EU and the US.

Competition policy proposals include not only the augmentation of traditional ex post enforcement tools but also the creation of new big tech-specific ex ante regulatory regimes.

A number of data protection and data-sharing initiatives have been proposed.

Policy initiatives across the three jurisdictions place special emphasis on personal data use and data protection.

Moreover, there are relevant initiatives, particularly in China and the EU, with respect to users' data portability.

This, together with emerging policy and market developments on data-sharing, seems to be paving the way to a generalised use of personal data for the provision of financial services by different types of entities.

Policy initiatives are addressing the operational resilience of big tech firms.

These typically apply to big techs either as providers of financial services2 or as third-party service providers of financial firms.

The operational resilience requirements in both cases intend to capture all sources of operational risk (in particular, information and communication technology risks) and expect adoption of sound risk management practices, swift response in case of disruption and continuity of critical services.

Some jurisdictions have taken meaningful policy efforts to address potential conduct issues and financial stability challenges but they do not follow an homogeneous pattern.

A key development in the conduct of business area is the EU's proposed Digital Services Act (DSA). This establishes extensive requirements for very large online platforms connected with the functioning and use of their services.

As such, the DSA represents a comprehensive effort to deal with how big techs treat their customers and the information they receive.

Regarding financial stability, the main regulatory development is the China financial holding company (FHC) regime.

This requires all entities holding two or more types of financial institutions to be structured and licenced as FHCs (if size thresholds or other conditions are met).

This effectively mandated big techs to reorganise their financial business and represents a novel entity-based regulatory approach that entails a

comprehensive oversight of the activities performed by big techs through all their financial subsidiaries.

Additional regulatory responses might be needed to comprehensively address big tech risks and achieve policy consistency at the international level.

Recent initiatives in China, the EU and the US constitute important steps in addressing risks posed by big techs. However, if big techs continue to gain prominence in the financial system, additional policy responses might be necessary.

It is also very likely that new policy actions will largely need to follow an entity-based approach and require close cooperation between competition, data and financial authorities. Moreover, given the cross-border scope of big tech activities, enhanced international regulatory cooperation is essential.

To read more: https://www.bis.org/fsi/publ/insights36.pdf

Number 3

Moving forward in securing Online Trust via the Digital Wallets

The 2021 Trust Service Forum allows stakeholder communities to engage in open discussions on securing trust services online and on the future of the EU Digital Identity Framework.

Electronic signatures, electronic seals and other online trust services have become a staple in the life of many Europeans.

In light of the COVID-19 pandemic, a key aspect to ensure a viable business model for qualified trust service providers was an increasing usage of online trusted services among European citizens, businesses and public administrations in an online mode.

This new reality across the EU has highlighted the security concerns of remote identification and authentication processes.

The necessity for a new framework for EU digital identity became apparent.

The European Commission presented last June a new framework for the EU digital identity by offering to citizens and businesses the digital wallets that will allow EU citizens to retain their documents such as national digital identities, licences, diplomas and bank credentials securely in their smartphone.

The wallet should also allow them to log in to online services across the EU and to electronically sign their documents.

On September 21st, the European Union Agency for Cybersecurity (ENISA) in collaboration with the European Commission delivered the 7th consecutive ‘’Trust Service Forum’’.

It attracted over to 1000 participants and brought more than forty experts, service providers, conformity assessment, supervisory bodies and national authorities together, to discuss the online trust market and its emerging issues under the European Commission’s Regulation 910/2014, on electronic identification and trusted services for electronic transactions in the internal market (eIDAS Regulation).

On 22nd September, D-TRUST in cooperation with TÜViT and the European School of Management and Technology (ESMT), held the 13th CA-Day.

Both conferences were held in a hybrid format, with physical presence for the panellists at the ESMT premises in Berlin and virtually for the participants.

The forum was jointly opened by the European Commission's Director of Digital Society, Trust and Cybersecurity Ms. Lorena Boix Alonso and ENISA's Head of Policy Development and Implementation Unit Mr. Evangelos Ouzounis and it was consisted of three main distinct blocks.

In the first one, the panellists discussed the new ''EU Digital Identity Framework- bringing opportunity to wider use of online trust solutions across the EU''.

The concept of decentralised online identity, that gives back control to users over their personal data and leverages the use of an identity wallet, was additionally discussed.

Second block focused on certification and standardisation efforts and the third one on the trust service market – current state of play, opportunities and outlook.

Panellists had also the opportunity to further elaborate on the upcoming revisions of the eIDAS Regulation that proposes to further extend its application to the private sector and to promote trusted digital identities across the EU.

Background

The Trust Services Forum acts as a platform for participants to share their good practices on the implementation of trust services; review the standards, implementing acts and technical guidelines within the eIDAS; and discuss strategies to promote the adoption of qualified trust services.

The EU Agency for Cybersecurity supports the Commission on the implementation of the eIDAS by providing security recommendations for the implementation of trust services, mapping technical and regulatory requirements, promoting the deployment of qualified trust services in Europe and raising awareness among users on securing their e-transactions.

Under the EU Cybersecurity Act of 2019, the Agency gained an extended mandate to explore the area of electronic identification (eIDs) included in the regulation.

EU's Digital Wallet's proposal

The Commission on the 3rd June 2021 proposed a framework for a European Digital Identity which will be available to all EU citizens, residents, and businesses in the EU. Citizens will be able to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phone.

They will be able to access online services with their national digital identification, which will be recognised throughout Europe. Large platforms are proposed to accept the use of European Digital Identity wallets upon request of the user, for example to prove their age. Use of the European Digital Identity wallet will always be at the choice of the user.

The new European Digital Identity Wallets will enable all Europeans to access services online without having to use private identification methods or unnecessarily sharing personal data. With this solution they will have full control of the data they share.

Number 4

Methodology for a Sectoral Cybersecurity Assessment

Cybersecurity certification under the European Union Cybersecurity Act (CSA) is intended to increase trust and security for European consumers and businesses and help to achieve a genuine digital single market.

This requires that all relevant levels of the ICT market, from sectoral ICT services and systems via ICT infrastructures to ICT products and ICT processes, will be addressed and that the related cybersecurity certification schemes are well accepted by the market.

The CSA stipulates specific requirements, which target efficiency and coherence between schemes of the CSA's cybersecurity certification framework.

These requirements include:

– The security and assurance requirements for ICT services, ICT processes or ICT products should be defined based on the risk associated with their intended use.

– Assurance levels should be implemented consistently across schemes.

– Support for security-by-design.

The methodology for sectoral cybersecurity assessments described in this document (hereinafter called SCSA Methodology) addresses these objectives in the context of drafting sectoral cybersecurity certification schemes, which address ICT services in individual market sectors.

It is designed to be used as a preparatory step for the definition of a candidate scheme involving sectoral stakeholders.

A basic principle of the proposed methodology is to establish a sound understanding of the sectoral ICT services and system as a foundation for all other functions:
– A cybersecurity assessment at the sectoral level will provide information about the objectives of the sectoral stakeholders and will identify the primary assets and related risks.

As an enhancement of the typical risk assessment procedure, a 'deep dive' to gain detailed information about the intended use of relevant subsystems, products or services will be conducted.

In addition, cyberthreat intelligence (CTI) will be employed to provide information on potential attackers, their motivation and capabilities.

This adds an important parameter to the risk analysis and contributes to the information needed to assign security and assurance requirements to ICT subsystems, ICT products or ICT services based on risk.

– The SCSA Methodology provides the option to integrate sectoral, product, process and potentially also ISMS-based cybersecurity certification schemes.

It offers a concept of internal risk, security and assurance reference levels.

If these are commonly used, they will support consistency in the definition of risk, security and assurance across schemes.

The SCSA Methodology is designed to address a wide range of certification schemes, beyond Common Criteria or other ISO/IEC 15408-based schemes.

Optionally other types of certification schemes can be integrated in order to establish consistency across the various types of schemes that support the proposed methodology.

– A link between the ISO/IEC 270xx series of standards and ISO/IEC 15408 is needed to allow information to be exchanged between the outcome of risk assessment and the specification of security and assurance of products.

The expert team has developed a mapping approach that addresses existing divergences of terminology between these standards and allows the transfer of the information that is required.

– The introduction of a common, scalable approach to risk-based security and assurance supports the definition of scaled controls.

These controls are associated with clear security levels which are defined in accordance with their ability to treat risk and protect against known attack potentials.

The expert team has drafted a sample list of scaled controls and has described how these controls can be used in a coordinated way.

Based on these properties and functions, the SCSA Methodology has the potential to fully support the aforementioned requirements stipulated by the CSA and to promote the market acceptance of cybersecurity certification in the following ways:

– The SCSA Methodology supports the identification of risk associated with the intended use of ICT systems, ICT services and ICT processes at any level of the sectoral architecture.

In applying the methodology, relevant stakeholders will be responsible for the identification of risks and they will be involved in the definition of security and assurance requirements.

This will allow them to balance their view of risks against the investment needed to mitigate these risks by introducing appropriate levels of security and assurance.

It can be expected that this transparent, cooperative approach will contribute significantly to the market acceptance of schemes under the CSA.

– As required by the CSA, consistency in the implementation of assurance levels can be achieved across schemes. This will allow the re-use of certificates issued by one scheme in other schemes, thus providing an important benefit both to the business interests of product and infrastructure service providers and to their customers.

At the same time, the methodology's approach to consistency is also flexible enough to support the integration of new types of cybersecurity certification schemes, which may emerge as a result of specific requirements from different markets.

– Introducing a common concept for security levels facilitates the definition of controls which can be commonly used across participating schemes. This provides a sound basis for the introduction of libraries of such controls.

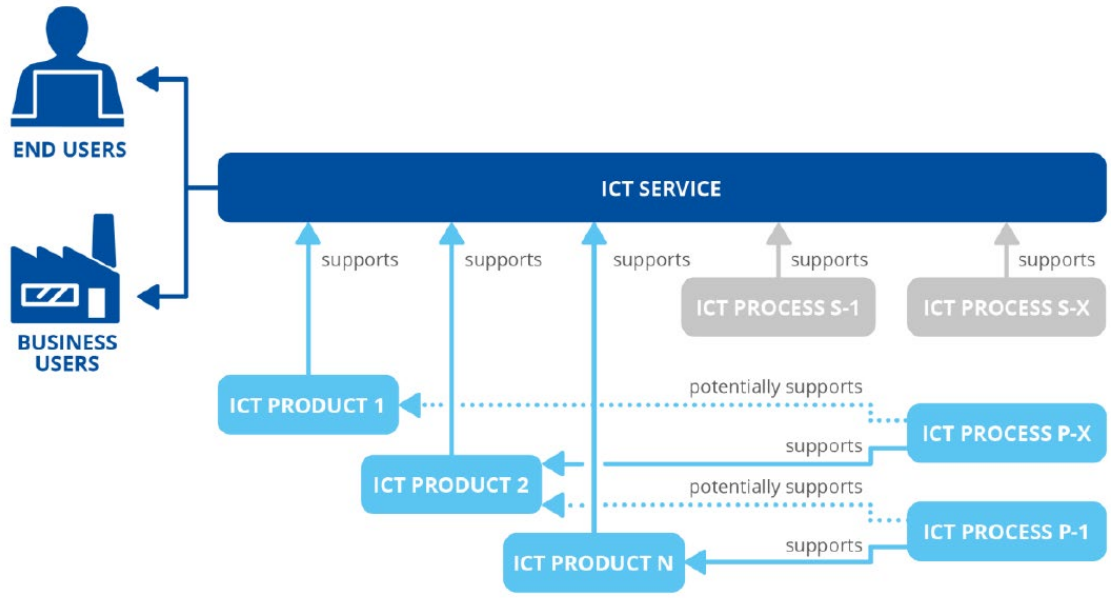
The availability of those could significantly promote the introduction of security-by-design, as well as the implementation of defined security levels in ICT products, ICT processes and also in ICT systems.

Applying the SCSA Methodology will generate sound information about the sectoral system and defined relationships between the stakeholders involved, which may enable additional tangible benefits, including:

– Product and service providers will benefit from reliable information about the intended use of their products and services, as well as sectoral security and assurance requirements. This will allow them to optimize their products and their market reach.

– The defined relationships between risk, security and assurance proposed by this methodology support the definition of horizontal products and services, which can serve various sectors.

Figure 1: CSA-defined elements and their relations



To read more:
https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment

Number 5

Jens Weidmann: Exploring a digital euro

Dr Jens Weidmann, President of the Deutsche Bundesbank and Chair of the Board of Directors of the Bank for International Settlements, at the digital conference "Fintech and the global payments landscape – exploring new horizons".

A very warm welcome to this joint symposium of the Bundesbank and the People's Bank of China. The main theme of our conference is "Fintech and the global payments landscape – exploring new horizons."

I am delighted that we have brought together such a wealth of experts in this field, with representatives of academia, fintech companies, commercial banks, central banks, government and supervisory authorities amongst our number. Sharing our respective thoughts and experiences is to the benefit of all parties involved. I would also like to thank the People's Bank of China for co-hosting this conference.

Unfortunately, the pandemic forces us to hold it as a digital event. If we had been able to meet here in person, I would have recommended a visit to the Bundesbank's Money Museum and the current numismatic special exhibition on the topic of "Money Creators. Who decides what's money?" In the dawning age of digital currencies, that is a highly relevant question indeed. Crypto tokens and other innovations in finance are challenging established views on what constitutes money.

To read more: https://www.bis.org/review/r210923a.htm

Number 6

Rule governing Board determination under the Holding Foreign Companies Accountable Act

The Public Company Accounting Oversight Board (the "PCAOB" or the "Board") is adopting a new rule, PCAOB Rule 6100, Board Determinations Under the Holding Foreign Companies Accountable Act, to provide a framework for its determinations under the Holding Foreign Companies Accountable Act (the "HFCAA") that the Board is unable to inspect or investigate completely registered public accounting firms located in a foreign jurisdiction because of a position taken by one or more authorities in that jurisdiction.

The rule establishes the manner of the Board's determinations; the factors the Board will evaluate and the documents and information the Board will consider when assessing whether a determination is warranted; the form, public availability, effective date, and duration of such determinations; and the process by which the Board will reaffirm, modify, or vacate any such determinations.

Executive summary

The Sarbanes-Oxley Act of 2002 (the "Act") mandates that the Board inspect registered public accounting firms and investigate possible statutory, rule, and professional standards violations committed by those firms and their associated persons.

That mandate applies with equal force to the Board's oversight of registered firms in the United States and in foreign jurisdictions.

Over the course of more than a decade, the Board has worked effectively with authorities in foreign jurisdictions to fulfill its mandate to oversee registered firms located outside the United States.

With rare exceptions, foreign audit regulators have cooperated with the Board and allowed it to exercise its oversight authority as it relates to registered firms located within their respective jurisdictions.

The norms of international comity have guided those efforts and allowed the Board to work cooperatively across borders, to resolve conflicts of law, and to overcome other potential obstacles.

The Board benefits greatly from cross-border cooperation with its international counterparts and has built constructive relationships that facilitate meaningful oversight.

Authorities in a limited number of foreign jurisdictions, however, have taken positions that deny the Board the access it needs to conduct its mandated oversight activities.

Recognizing the ongoing obstacles to Board inspections and investigations in certain foreign jurisdictions, Congress enacted the HFCAA.

The HFCAA requires that the Board determine whether it is unable to inspect or investigate completely registered public accounting firms located in a foreign jurisdiction because of a position taken by one or more authorities in that jurisdiction.

The HFCAA, among other things, also mandates that, after the Board makes such a determination, the U.S. Securities and Exchange Commission (the "Commission") shall require covered issuers who retain such firms to make certain disclosures in their annual reports and, eventually, if certain conditions persist, shall prohibit trading in those issuers' securities.

Following public comment, the Board is adopting a new rule, PCAOB Rule 6100, Board Determinations Under the Holding Foreign Companies Accountable Act, as proposed with some modifications after consideration of comments, to establish a framework for the Board to make its determinations under the HFCAA.

The final rule establishes the manner of the Board's determinations; the factors the Board will evaluate and the documents and information it will consider when assessing whether a determination is warranted; the form, public availability, effective date, and duration of such determinations; and the process by which the Board will reaffirm, modify, or vacate any such determinations.

To read more:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/rulemaking/docket048/2021-004-hfcaa-adopting-release.pdf?sfvrsn=f6dfb7f8_4

Number 7

Statement in Support of Adoption of PCAOB Rule 6100, Board Determinations Under the Holding Foreign Companies Accountable Act

Duane M. DesParte, Acting Chairperson - PCAOB Open Board Meeting

I fully support adoption of PCAOB Rule 6100, Board Determinations Under the Holding Foreign Companies Accountable Act (HFCAA), as set forth before us today.

Robust inspections and investigations of registered public accounting firms auditing U.S. public companies are core to the PCAOB's mandate under the Sarbanes-Oxley Act. This is true whether such firms are located inside or outside of the United States.

Through the passage of the HFCAA, Congress reaffirmed the importance of our oversight activities in providing protection for investors in all U.S. public companies, regardless of where the companies' audit firms are located or their audits are performed.

Rule 6100 establishes a framework for the determinations we are required to make under the HFCAA. This framework will help to promote consistency in our determinations and to provide transparency to investors, firms, issuers, foreign authorities, and other market participants as to the factors the Board will consider and the processes it will use in making and publicly reporting its determinations.

Furthermore, the framework includes a mechanism whereby the Board will reassess its determinations every year, which will provide increased clarity and certainty to market participants over time.

Transparency of the Board's framework is particularly important given the potential consequences that might follow Board determinations under the HFCAA for issuers, investors, and the broader capital markets.

In addition to setting forth the key factors the Board will assess in making determinations, the rule promotes transparency by requiring the Board to describe in a public report its assessment and the basis for its conclusion for any determination it makes.

The rule also requires the Board to reassess and publicly report on its determinations at least annually, which will help ensure market

participants remain timely informed of the status of our ability to inspect or investigate completely audit firms in the covered foreign jurisdictions. In this way, the final rule provides more certainty to market participants than was provided by the two-step reassessment approach set forth in the proposal.

I therefore support the rule before us. It provides the Board a clear and consistent approach for making its determinations and for keeping all interested market participants well informed through timely public reporting.

In closing, I want to thank all those at the PCAOB who have contributed to developing today's final rule; including our staff in the Offices of International Affairs, General Counsel, and Economic and Risk Analysis and with special recognition for Liza McAndrew Moberg, Beth Hilliard Colleye, Ken Lench, Drew Dropkin, and Damon Andrews. I also want to thank the Commission's staff for their support and assistance.

Number 8

"We expect to let certain exemptions expire at the end of the year"
Raimund Röseler, Chief Executive Director of Banking Supervision, on the current state of the banks

The pandemic, landmark rulings, catastrophic flooding: these are turbulent times for the banking sector.

Chief Executive Director Raimund Röseler sat down with BaFinJournal to discuss how the measures to stop the spread of the coronavirus have impacted the banks' books, what additional burdens are expected to result from recent court decisions on cum/ex transactions, premium-aided savings agreements and changes to standard terms and conditions, as well as the extent to which recent catastrophic floods might affect institutions. He also talked about the outcome of the recent Europe-wide stress test.

Mr Röseler, with the delta variant spreading, the pandemic appears to be entering yet another new phase. How long do you want to maintain the supervisory exemptions for the institutions?

Although the pandemic isn't over yet, it hasn't had an inordinate impact on the banks' books so far. So we expect to let the exemptions relating to the liquidity coverage and leverage ratios expire at the end of the year.

We will also be gradually withdrawing other exemptions, including administrative ones. However, we will of course continue to keep a close eye on events as they develop so as not to overburden the banks.

What are the plans for the countercyclical capital buffer?

We will discuss that within the Financial Stability Committee. I suspect that we won't raise the capital buffer until the economic situation permits it.

You've just said that the pandemic hasn't hit the banks' books as hard as originally feared. How are German banks faring, then?

They are well capitalised, as ever. The German institutions have surplus capital in excess of 150 billion euros, and the actual write-downs required have been significantly lower than projected.

Germany's SIs budgeted for six billion euros in write-downs for this year, and only recognised a few hundred million in the first five months. And the situation has been similar for our LSIs .

Most of them have thus far not reported any increased impairments or any significant rises in defaults. We expect that impairments might rise for LSIs and certain risk metrics might deteriorate in some instances. However, on the whole, we believe that Germany's banks remain sound.

What will happen when the various state support measures run out? We can assume that those measures are still distorting the actual picture somewhat at the moment.

State aid really has cushioned much of the blow to the German economy. Now that insolvency law applies again in its old form, insolvencies in certain sectors are on the rise. However, this has yet to directly hit the banks' books so far.

While individual institutions are giving us cause for concern, it is mainly those which were on shaky ground already before the pandemic. Germany's banking sector as a whole has weathered the crisis well so far and we currently believe it will continue to do so.

How are the banks' loan portfolios looking? Do they hold many non-performing loans?

Those are currently at a low level. If NPL ratios were to rise, this would necessitate higher provisions and could weaken the German institutions' profitability further, thereby eroding their solvency.

However, we do not anticipate any wide-scale problems as they are unlikely to rise so drastically.

There are also loans for which the banks have granted forbearance measures, which might also need to be taken into account.

The NPL ratio for the SIs is currently 1.3 percent. If every loan in forbearance were to default, that ratio would climb above 2 percent. Now, that's a lot. But it's a worst-case scenario.

What should institutions do to keep the issue of non-performing loans in check?

Two things: Firstly, institutions need to keep an eye on their borrowers, and act early if need be. And secondly, they need to set aside enough capacities

to deal with defaults – possibly more than in the past. That's because while they might not be dramatic, a number of defaults will undoubtedly occur.

The way banks handle credit risk is also a question of risk management. How are the banks doing on that front?

We believe there is room for improvement at a number of institutions at any rate. The pandemic has shown us that certain banks are experiencing greater problems than others as far as management and organisation are concerned.

As for dealing with defaults: there have been extremely few in the past. Some institutions thus have only little experience in handling NPLs. It is important for banks to be prepared and to set aside capacities for risk management.

The ECB has decided to discontinue its dividend recommendation from October and you have expressed your view on the matter. In your opinion, has BaFin's case-by-case approach been proven effective?

Yes, I believe it has. It was not and is not possible for us to ban dividend distributions wholesale. We will therefore continue to examine each case on its own. However, we will rescind our announcement of December 2020 on the matter.

We will no longer require institutions to notify us in advance of their dividend distribution plans. However, we continue of course to expect them to distribute dividends only if they can afford it.

So you don't expect a wave of distributions.

Correct. Many institutions have already distributed dividends over the course of the year, but at a very prudent level. I assume that this will remain the case. I don't expect that institutions will be trying to make up for lost time, as it were.

Will you be monitoring the institutions?

Yes, we will of course look at each one individually. Ongoing supervision provides us a window into how banks are approaching the issue. If we see that an institution isn't doing well and still pays out dividends or excessive distributions, we will intervene. We have already done so in the past.

Mr Röseler, what do you make of the German banks' results in the current EBA and ECB stress tests?

The German banks have shown that they are sufficiently capitalised even in an adverse stress scenario. That's good news. Particularly as this scenario was no walk in the park, since it included a prolonged economic downturn resulting from persistent uncertainty due to the coronavirus crisis.

Although some German institutions use up portions of their capital buffer in the stress scenario, these are mainly the capital conservation buffer and the buffer for global or other systemically important institutions.

There are two things to keep in mind here: The institutions remained above the minimum capital requirements we supervisory authorities have imposed.

This means they would still have more CET1 capital than we require. And these additional buffers are expressly intended to ensure that the banks have reserves which they can tap in a crisis in order to absorb shocks and continue to lend.

It was just like in the actual coronavirus crisis: the stress test once again showed us how important it is to have sufficient and sound capital resources.

By that I'm referring to both the quality and the quantity of capital. The combination of Tier 1 capital and additional buffers for crises has proven itself. We require this combination as one of the lessons learnt after the 2007/2008 financial crisis.

What will the recent cum/ex ruling by the Federal Court of Justice mean for banks?

The cum/ex ruling did not come as a surprise. It would have been surprising had the Federal Court of Justice ruled differently. And I think the ruling was also in line with most banks' expectations.

That's why the majority of banks likely also recognised sufficient risk provisions. Now we need to see whether there remains room for improvement here and there, including with respect to the provisions.

The Federal Court of Justice has also recently issued two other landmark decisions: one on premium-aided savings agreements and one on changes to standard terms and conditions. How are the banks coping?

The cum/ex ruling really only affects a relatively small number of institutions. The decisions on premium-aided savings agreements and standard terms and conditions are relevant to a large number of banks.

I would even go so far as to say that the terms and conditions decision affects every bank, albeit to varying degrees since not all banks are active in the retail business to the same extent.

The decision took many institutions by surprise. Quite in contrast to the cum/ex ruling. Nobody truly believed it was legal to pay taxes once and have them reimbursed twice.

Are the banks prepared to bear the burdens arising from the terms and conditions decision?

I don't think the costs of reimbursements will be as staggering as originally feared. What is more significant is the question as to how this will affect the future.

What price level will the affected institutions return to in immediate reaction to the decision? The one from three years ago? Or the one in effect when the account was opened? And which price level do they hope to achieve in the long run? What options and processes will the banks have at their disposal for future price hikes?

You said the cost would not be staggeringly expensive. What scale are we talking about here?

Due to limitation rules, reimbursements are expected to be kept to a reasonable amount. However, we don't have any reliable estimates as of yet. We have surveyed 100 banks on the matter and are currently working with ten institutions to figure out how expensive this can get. We are also in close dialogue with the relevant industry associations.

Is BaFin considering issuing a general administrative act regarding changes to standard terms and conditions? Or have the discussions with the institutions and associations been so fruitful that this won't be necessary?

Let's see how the banks get on, first. We've got to bear in mind that the decision caught the institutions off guard. We will also take a close look the next time account management fees are charged at the end of the quarter. We expect the banks to reach valid agreements with their customers as soon as possible. If not, we have every option at our disposal, of course.

A quick look at the Federal Court of Justice's ruling on premium-aided savings agreements: So far, BaFin has received 1.100 objections to the general administrative act.

These objections are not surprising, and do not worry us. We will examine every one of them and every institution will receive a formal objection notice from us.

Some banks will then no doubt turn to the administrative court. This is the usual procedure in a state governed by the rule of law, and that procedure cannot be rushed. I have utmost confidence that our general administrative act will become legally effective. We would not have proceeded in this manner had we not been confident of this.

The consumers are likely less sanguine in this regard.

Understandably. We want to require banks to inform their customers if their premium-aided savings agreements contain invalid interest rate adjustment clauses.

And to let them know whether or not they short-changed them on interest on the basis of those clauses. If so, they have to irrevocably promise their customers an interest recalculation or offer them an amending agreement containing a valid interest rate adjustment clause.

To the extent banks fail to approach customers on their own – as we intended – those customers will have to wait until our general administrative act becomes legally effective. Or they will have to dispute their interest calculations through the civil courts – potentially with assistance from consumer protection associations.

Mr Röseler, we'd like to close with a question regarding the devastation in certain regions of Germany in the wake of July's severe storms. How will this affect the banks?

Some local banks were badly hit by the storms. And in more than one respect: branch offices have been destroyed and employees have been affected. That has an immediate impact on institutions. And the banks' customers also suffered severe losses. The extent to which this will affect loan portfolios, for instance, will surely depend on the scope of state support measures. We will of course keep a close eye on developments. And we will of course exercise our supervisory responsibilities with a sense of proportion.

Mr Röseler, thank you for sitting down to talk with us.

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2021/fa_bj_2108_Interview_EDBA_Lage_Banken_en.html

Number 9

Conti Ransomware Attacks Impact Healthcare and First Responder Networks

The FBI identified at least 16 Conti ransomware attacks targeting US healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year.

These healthcare and first responder networks are among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim.

The ransom letter instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors.

Ransom amounts vary widely and we assess are tailored to the victim. Recent ransom demands have been as high as $25 million.

Cyber attacks targeting networks used by emergency services personnel can delay access to real-time digital information, increasing safety risks to first responders and could endanger the public who rely on calls for service to not be delayed.

Loss of access to law enforcement networks may impede investigative capabilities and create prosecution challenges.

Targeting healthcare networks can delay access to vital information, potentially affecting care and treatment of patients including cancellation of procedures, rerouting to unaffected facilities, and compromise of Protected Health Information.

Technical Details

Conti actors gain unauthorized access to victim networks through weaponized malicious email links, attachments, or stolen Remote Desktop Protocol (RDP) credentials. Conti weaponizes Word documents with embedded Powershell scripts, initially staging Cobalt Strike via the Word

documents and then dropping Emotet onto the network, giving the actor access to deploy ransomware.

Actors are observed inside the victim network between four days and three weeks on average before deploying Conti ransomware, primarily using dynamic-link libraries (DLLs) for delivery.

The actors first use tools already available on the network, and then add tools as needed, such as Windows Sysinternals and Mimikatz to escalate privileges and move laterally through the network before exfiltrating and encrypting data.

In some cases where additional resources are needed, the actors also use Trickbot. Once Conti actors deploy the ransomware, they may stay in the network and beacon out using Anchor DNS.

If the victim does not respond to the ransom demands two to eight days after the ransomware deployment, Conti actors often call the victim using single-use Voice Over Internet Protocol (VOIP) numbers. The actors may also communicate with the victim using ProtonMail, and in some instances victims have negotiated a reduced ransom.

To read more:
https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf

Number 10

Disrupting Exploitable Patterns in Software to Make Systems Safer

Program pushes secure system design by developing ways to stop cyber attackers' from executing unintended computations on critical systems

While much attention is paid to detecting and remedying flaws or vulnerabilities in software, the way a system is designed can also create large opportunities for attackers.

System designers primarily focus on ensuring a program is adept at executing a specific task, focusing on how a design can best support intended features and behaviors and on how they will be implemented within the design.

Attackers have also discovered that these design structures and implementation behaviors can be repurposed for their own malicious purposes.

Unexpected – or emergent – behaviors that these features could exhibit are not often taken into consideration at the time of design.

As a result, attackers often find that they can generate emergent behaviors by using what's already built into a system, providing a way to exploit flaws that are several layers down.

In other words, systems are unknowingly being designed in ways that support adversarial programmability and combinations of features and unprotected abstractions.

These amount to embedded exploit execution engines – creating what is colloquially known as "weird machines."

"When it comes to exploits, the common thinking is that there is a flaw in the program and then there is a crafted input that can trigger the flaw resulting in the program doing something it shouldn't like crashing or granting privileges to an attacker," said Sergey Bratus, a program manager in DARPA's Information Innovation Office (I2O).

"Today, the reality is somewhat different as those existing flaws aren't immediately exposed, so an attacker needs help getting to them. This help is unwittingly provided by the system's own features and design.

Attackers are able to make use of these features and force them to operate in ways they were never intended to."

This challenge becomes increasingly problematic when observing a class of systems that rely on similar features. When an attacker discovers an exploit on one system, this can give a big hint on how to find similar exploits for other systems that have been developed independently by different vendors but make use of similar mechanisms.

This creates persistent exploitable patterns that can be used across a whole host of programs.

The Hardening Development Toolchains Against Emergent Execution Engines (HARDEN) program seeks to give developers a way to understand emergent behaviors and thereby create opportunity to choose abstractions and implementations that limit an attacker's ability to reuse them for malicious purposes, thus stopping the unintentional creation of weird machines.

HARDEN will explore novel theories and approaches and develop practical tools to anticipate, isolate, and mitigate emergent behaviors in computing systems throughout the entire software development lifecycle (SDLC).

Notably, the program aims to create mitigation approaches that go well beyond patching. At present, patches tend to only address a particular exploit and do not disrupt the underlying exploit execution engine residing at the design-level.

HARDEN will also focus on validating the generated approaches by applying broad theories and generic tools to concrete technological use cases of general-purpose integrated software systems.

Potential evaluation systems include the Unified Extended Firmware Interface (UEFI) architecture and boot-time chain of trust, as well as integrated software systems from the Air Force and Navy domains, such as pilots' tablets.

"There are many ways to theorize about addressing these challenges, but the test of the theory is how it will apply to an actual integrated system that we base trust on, or want to base trust on. We want to ensure we're creating models that will be of actual use to critical defense systems," noted Bratus.

To learn more:
https://sam.gov/opp/76520ba476714e04a6349578a763120c/view

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.

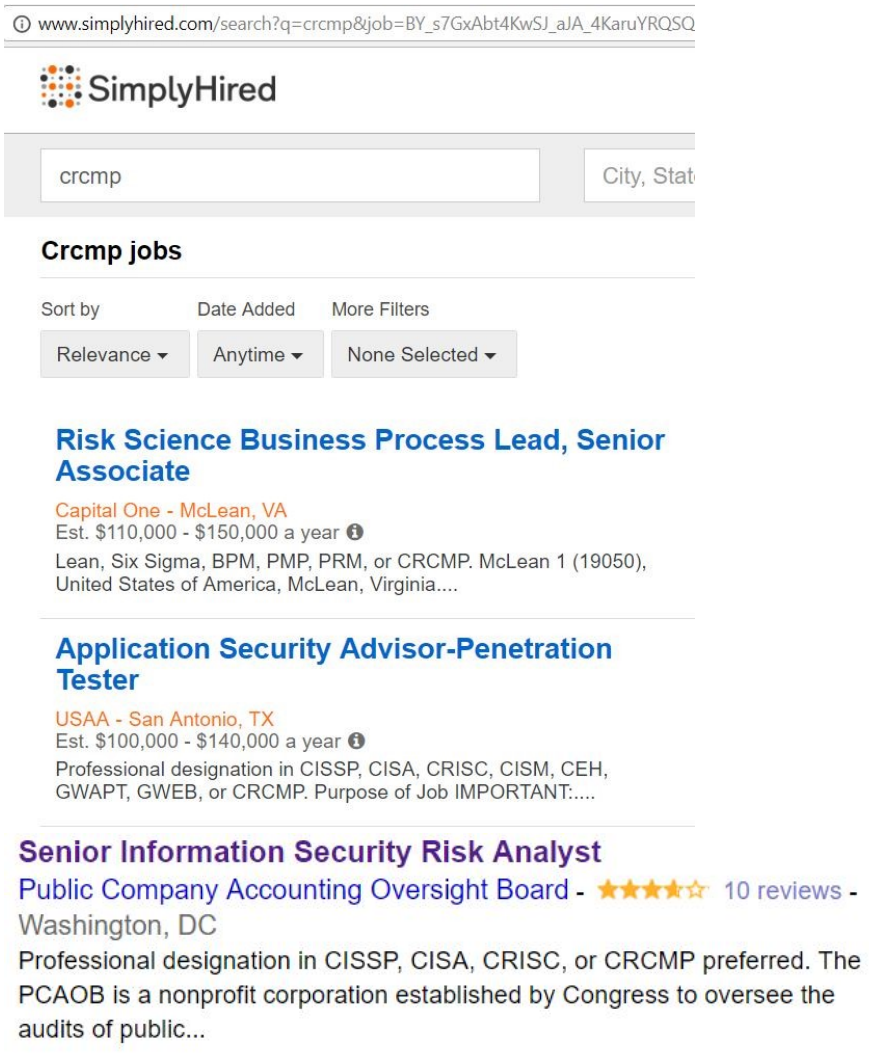
International Association of Risk and Compliance Professionals

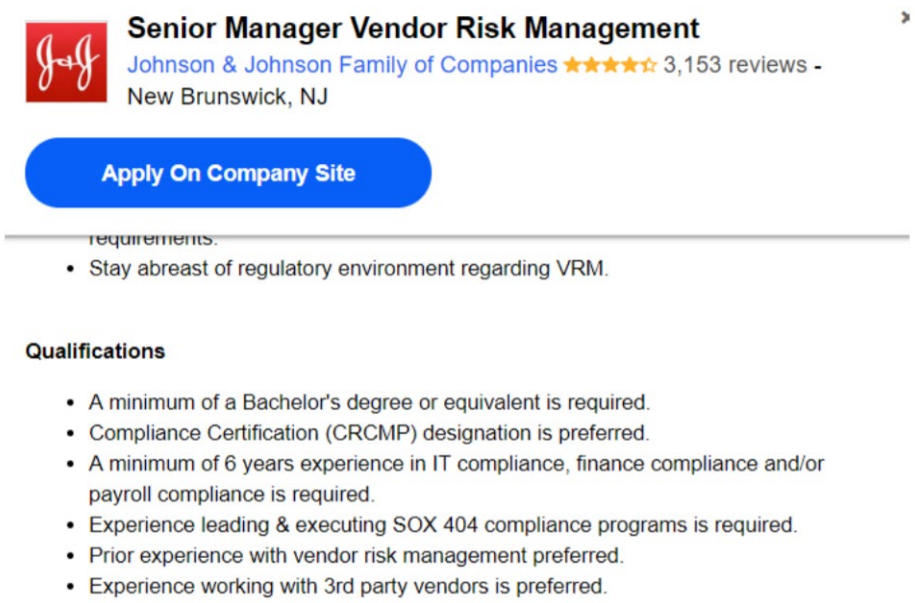
You can explore what we offer to our members:

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





Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews -
New Brunswick, NJ

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

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