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, May 30, 2022

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

Dear members and friends,

Which is the emerging field at the intersection of *cybersecurity* and *biosecurity?* It is called *cyberbiosecurity*.

Cyberbiosecurity aims to identify and mitigate security risks fostered by the digitisation of biology and the automation of biotechnology.

Several areas in Biotech are of particular concern for cyberbiosecurity. *Gene editing tools* are used worldwide for rapid and precise gene editing. In healthcare, the digitisation of biology and metabolic engineering is accelerating the development of new vaccines, drugs and painkillers.

These new possibilities bring a whole new category of vulnerabilities and risks. In the last five years, the technological barriers to acquiring and using biological weapons have been significantly lowered.

The security implications of biotechnological advances extend beyond bioweapons. For example, developments in metabolic pathway engineering also offer ways to produce illicit drugs such as heroin.

To mitigate these risks, the culture of the life sciences community must change from *blind trust* to a *highly aware and educated* community.

We can read more at the new *Annual Report on Cybersecurity Research and Innovation Needs and Priorities,* from the European Network and Information Security Agency (ENISA).

So, why cybersecurity is different in these fields?

The importance of reviewing cybersecurity related issues in life sciences, and in biotechnology in particular, is *no different* from many other critical infrastructures (e.g. the chemical industry, nuclear physics, etc.).

However, the *lack of awareness* and of specific cybersecurity controls to address the risks and the long term implications that may have implications for life itself lends a sense of urgency to the need to review this topic from a research perspective. When it comes to cybersecurity, innovation is quickly becoming a double-edged sword for life sciences customers.

Read more at number 3 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 5)

Green Swan 2022

Number 2 (Page 7)

United States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime

Number 3 (Page 9)

RESEARCH AND INNOVATION BRIEF, MAY 2022

Annual Report on Cybersecurity Research and Innovation Needs and Priorities

Number 4 (Page 17)

Remarks at Securities Enforcement Forum West 2022

Gurbir S. Grewal, Director, SEC Division of Enforcement

Number 5 (Page 20)

Thematic Review on Out-of-Court Corporate Debt Workouts (OCW) - Peer Review Report

Number 6 (Page 23)

Strengthening EU-wide cybersecurity and resilience – provisional agreement by the Council and the European Parliament

European Council
Council of the European Union

Number 7 (Page 26)

Fighting child sexual abuse: European Commission proposes new rules to protect children

European Commission

Number 8 (Page 29)

Global experts examine the changing face of match-fixing

INTERPOL

Number 9 (Page 31)

Joint Statement of the 25th ASEAN+3 Finance Ministers' and Central Bank Governors' Meeting

MAS Monetary Authority of Singapore

Number 10 (Page 39)

New Guidance – Biometric authentication in Automatic Access Control Systems (AACS)

Designing, building and operating AACS that include biometric authentication

CPNI
Centre for the Protection of National Infrastructure

Number 1

Green Swan 2022

A virtual conference co-organised by the Bank for International Settlements, the European Central Bank, the Network for Greening the Financial System and the People's Bank of China.

Building on the foundation of the inaugural Green Swan Conference in 2021, which brought together a wide range of high-calibre policymakers, experts and practitioners from different sectors, Green Swan 2022 offers a deeper dive into the topics of:

(i) monetary policy setting and operations in the context of climate change, and

(ii) the role of finance in the climate transition, including transparency and disclosures, transition plans and financing green innovation.

The conference will be fully livestreamed. Join the conversation on social media using #GreenSwanConference

Opening event

09:30 - 09:35 **Welcome remarks**

Luiz PEREIRA DA SILVA
(Bank for International Settlements)

09:35 - 10:05 **Opening address**

Ravi MENON
(Monetary Authority of Singapore; NGFS)

Session 1: The role of finance in climate transition

11:20–11:35 **Keynote speech**

ZHOU Xiaochuan
(China Society for Finance and Banking; former Governor of the People's Bank of China)

11:00–12:30 **Roundtable: What can the public and private sectors do to turn transition finance framework to actions?**

Chair: MA Jun
(G20 Sustainable Finance Working Group; China Green Finance Committee)

Masyita CRYSTALLIN
(Indonesia Ministry of Finance)

Paulina DEJMEK HACK
(European Commission)

Emmanuel FABER
(International Sustainability Standards Board)

Daniel HANNA
(Standard Chartered Bank)

Kamran KHAN
(Deutsche Bank)

Vivek PATHAK
(IFC - International Finance Corporation)

Nicolas STERN
(London School of Economics)

To read more:
https://www.bis.org/events/green_swan_2022/overview.htm

Agenda:
https://www.bis.org/events/green_swan/green_swan_2022_agenda.pdf

Number 2

United States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime

At the Council of Europe (COE) headquarters in Strasbourg, France, on May 12, Deputy Assistant Attorney General (DAAG) Richard Downing of the U.S. Department of Justice's Criminal Division signed the *Second Additional Protocol to the Convention on Cybercrime* on enhanced cooperation and disclosure of electronic evidence on behalf of the U.S. government.

This strengthening and expansion of the multilateral international treaty commonly called the *Budapest Convention* is part of the United States' steadfast commitment to helping nations, including the United States, fight cybercrime by obtaining access to needed electronic evidence.

The Second Additional Protocol to the Budapest Convention will accelerate cooperation among parties to protect our citizens from cybercrime and hold criminals accountable.

As cybercrime proliferates, electronic evidence is increasingly stored in different jurisdictions.

The Second Additional Protocol is specifically designed to help law enforcement authorities obtain access to such electronic evidence, with new tools including direct cooperation with service providers and registrars, expedited means to obtain subscriber information and traffic data associated with criminal activity, and expedited cooperation in obtaining stored computer data in emergencies. All these tools are subject to a system of human rights and rule of law safeguards.

At the signing, DAAG Downing said, "The Budapest Convention is a truly remarkable international instrument. Its technology-neutral approach to cybercrime has created an enduring framework for cooperation that ensures law enforcement has the tools they need to respond to new criminal methods."

He noted that 66 countries are currently party to the Convention and more accede every year.

Today's signing, which took place within the framework of an international conference on enhanced cooperation and disclosure of electronic evidence held in cooperation with the Italian Presidency of the COE Committee of Ministers, was the culmination of nearly four years of negotiation by the U.S. delegation, composed of U.S. Department of Justice and Department of State representatives.

The U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs is a leading donor to the Council of Europe Cybercrime Program, which provides crucial advice and technical assistance to help countries join and implement the Budapest Convention.

The United States remains committed to the Budapest Convention as the premier international legal instrument for fighting cybercrime. As DAAG Downing said today, "It is our collective vision that every country that is serious about fighting cybercrime and that provides for the protection of human rights should become party to the Budapest Convention. The Convention strikes the right balance between imposing obligations on nations to have robust laws and capabilities and providing the flexibility necessary for nations with different legal systems to join."

Additional information about the Second Additional Protocol to the Budapest Convention may be found at:
https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention

To read more:
https://www.justice.gov/opa/pr/united-states-signs-protocol-strengthen-international-law-enforcement-cooperation-combat

https://rm.coe.int/1680081561

Number 3

RESEARCH AND INNOVATION BRIEF, MAY 2022

Annual Report on Cybersecurity Research and Innovation Needs and Priorities

The future of the European Union (EU) in the digital age depends on the choices made today and the ability of individuals, businesses and organisations to address challenges and seize opportunities.

While Europe and the world recover from a public health crisis, it is vitally important to identify future challenges and opportunities. This decade, the EU will increase investment in research and innovation (R&I).

One of the focus areas will be the digital transformation of the economy and society that works for people by promoting the European way of life, supporting democracy and values, and protecting its strategic autonomy.

In this context, the work of the research community is crucial in creating the knowledge necessary to understand what lies ahead.

The EU is a strong player in knowledge and innovation: it accounts for almost 20% of global research and development, publishing and patenting activities.

This document offers a forward-looking perspective on some of these challenges and opportunities. It recognises the importance of key structural trends with major implications for the EU's digital ambitions to 2030 and beyond.

The multidisciplinary nature of these trends led to the selection of four main themes that form the structure adopted for this report: hyperconnected world, intelligent systems, cybersecurity in life sciences (biotechnology), and computational security.

Digital hyperconnectivity is a trigger for all other trends and is independent of any particular technology.

Ubiquitous connectivity will increase the convergence of industries, products, technologies and services, driven by the accelerated datafication of everything.

The growing appetite for data will help make technology smarter as the next frontrunner in the race for greater automation and optimisation in everyday life.

In addition, hyperconnectivity, datafication and intelligent automation also contribute to research in the life sciences.

This decade, as a result of the pandemic and the efficiency of biotechnology, the EU will increase investment in the research and development of new technologies for the pharmaceutical and health sectors.

However, hyperconnectivity and intelligent automation do not come without challenges. While the benefits are well known, the challenges and risks are yet to be fully recognised.

Cybersecurity is crucial to ensure that EU citizens, businesses and organisations can enjoy the promised benefits in a reliable and trustworthy environment.

This report also aims to identify some of the future needs in protecting data and securing authentication, by creating knowledge in computational security.

A summary of the findings across all the thematic areas is presented in Table 1 below.

	HYPERCONNECTED WORLD	COMPUTATIONAL SECURITY	INTELLIGENT SYSTEMS	CYBERSECURITY IN LIFE SCIENCES (CYBERBIOSECURITY)
NOTEWORTHY CHALLENGES AND GAPS	1. Generating a broader understanding on how hyperconnectivity may influence humanity and the social and political dimensions.	1. Lack of skills in cryptography; 2. Reduced number of market opportunities; 3. The need for standardisation; 4. Efficient support for developers working in the field; 5. Moving of cryptography research from communication fields to being embedded within hardware.	1. Better understating of socio-economic implications with Artificial Intelligence (AI) applied to cybersecurity; 2. Develop technical and regulatory excellence; 3. The need for foresight and development of institutional capacity to deal with AI.	1. Defining the security implications of life science technologies for cybersecurity research; 2. Skills and training for life science researchers; 3. Generating a broader understanding of the implications of cybersecurity for life sciences research.
RELEVANT FUTURE RESEARCH NEEDS AND PRIORITIES	1. The redefinition of the boundaries of human-computer interaction, and the concomitant security risks that are associated with this; 2. Cybersecurity in the context of new generations of mobile communications and data collection or processing methods (evolution from 5G to 6G).	1. Efficient implementation of symmetric key schemes at higher security levels; 2. Planning and preparation for the transition to the Post Quantum era of cryptographic systems; 3. Secure implementations of cryptographic systems are needed that resist side channel attacks; 4. New assumptions and seemingly-impossible results for future cryptographic components that derive from mathematics, physics or hardware limitations; 5. Standards for new quantum resilient safe algorithms and protocols.	1. Linking vertical and horizontal views on AI research (across research teams but also from design to implementation); 2. Design of approaches for monitoring large-scale and possibly interconnected systems; 3. Exploration of biomimetic cybersecurity algorithms; 4. Inclusion of context awareness in machine learning (ML) in order to boost resiliency.	1. The evolving risks and the threat landscape in biotechnology R&I. 2. Risk management framework in the field of public health microbiology (e.g. modern DNA sequencing); 3. Categories of bio vulnerabilities in the context of cyber; 4. Identification of processes and routines throughout the life science fields that require cyber-interfaces and reliance on automation; 5. Pursuit of various activities and initiatives to establish cyberbiosecurity guides and standards.

During 2022, ENISA will promote several initiatives with stakeholders and the community to discuss the challenges and corresponding research needs outlined in this report.

These findings will also be used by ENISA to identify funding priorities for the Strategic Agenda and for the work programme of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC).

CYBERSECURITY IN LIFE SCIENCES (BIOTECHNOLOGY)

Governments and security experts have identified the life sciences sector as *particularly vulnerable* to cybercrime.

The importance of reviewing cybersecurity related issues in life sciences, and in biotechnology in particular, is no different from many other critical infrastructures (e.g. the chemical industry, nuclear physics, etc.).

However, the lack of awareness and of specific cybersecurity controls to address the risks and the long term implications that may have implications for life itself lends a sense of urgency to the need to review this topic from a research perspective.

When it comes to cybersecurity, innovation is quickly becoming a double-edged sword for life sciences customers.

Recently, a cybersecurity researcher uncovered the threat posed by two Advance Persistent Threat (APT) groups that gained access to a leading pharmaceutical company's environment for up to three years before being discovered.

They stole IP and business data from the victim, information on bio culture products, cost reports and other details related to the company's overseas operations.

There is nothing more important to a pharmaceutical company than the formula for one of its new drugs.

THE URGENCY OF CYBERBIOSECURITY

Most broadly, cyberbiosecurity aims to identify and mitigate security risks fostered by the digitisation of biology and the automation of biotechnology. What exactly is meant by this needs to be explained further.

Cyberbiosecurity was first defined as understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of commingled life and medical sciences, cyber-physical dimension, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate and attribute such threats as they pertain to security, competitiveness and resilience.

We have reached new milestones in our understanding of how biological systems work and have also found ways to manipulate these systems to our advantage or needs in meaningful ways.

Biotech tools such as gene editing can intentionally introduce heritable genetic traits into wild populations, offering a new way to escape certain vector-borne diseases.

Several areas in Biotech are of particular concern for cyberbiosecurity. Gene editing tools such as CRISPR-CAS939 (Clustered Regularly Interspaced Short Palindromic Repeats associated protein-9 nuclease) for example, are used worldwide for rapid and precise gene editing.

Researchers like to use computers to analyse Deoxyribonucleic acid (DNA), operate lab machines and store genetic information.

In healthcare, the digitisation of biology and metabolic engineering is accelerating the development of new vaccines, drugs and painkillers.

Agriculture is becoming smarter and digital, with farmers relying on data-driven decisions gained from sensors implanted in the soil, satellites controlling tractor movements and other new practices.

But these new possibilities also bring a whole new category of vulnerabilities and risks.

In the last five years, the technological barriers to acquiring and using biological weapons have been significantly lowered.

The security implications of biotechnological advances extend beyond bioweapons. For example, developments in metabolic pathway engineering also offer ways to produce illicit drugs such as heroin.

Scientists have already figured out how to make the active ingredients in other narcotics, such as cannabis and precursors to Lysergic acid diethylamide (LSD).

What if a terrorist group or despotic regime tries to spread modified organisms aimed at attacking troops, scaring civilians, or throwing food production into disarray?

Recently, researchers outlined in a study the risks of using gene sequencing technologies to corrupt databases by altering sequences or annotations.

In this article, computer scientists designed a DNA sample that, when sequenced, resulted in a file that allowed the hacker to remotely control the sequencing computer and make changes to DNA sequences.

These changes could delay a research program, resulting in capital and labour losses, or could be used in a terrorist act to produce toxins or infectious agents in an uncontrolled manner.

To mitigate these risks, the culture of the life sciences community must change from blind trust to a highly aware and educated community.

This also requires intricate relationships between the computational and experimental dimensions of product development workflows.

The multiplicity of pathogens and toxins with their potential to be used as bioweapons (BW) agents could be due to several factors.

These include infectivity (the number of organisms required to cause disease), virulence (the severity of the disease caused), transmissibility (the ease of spread from person to person) and incubation time (the time from exposure to a biological agent to a disease outbreak).

All these attributes are manageable by modern biotechnology, and information about such experimental series is key to any covert attack that uses them as bioweapons.

Similarly, in cyberspace, there are a variety of malicious codes. These include viruses (programs that replicate in target machines); worms (self-sustaining programs); and carriers such as a Trojan horse that perform a legitimate function combined with malicious activity.

Additionally, botnets or networks of computers infected with malicious code can be coordinated to perform distributed denial-of-service attacks.

For biological weapons, means of delivery range from advanced aerial spraying to contamination of food or water, while malicious code can be transmitted in cyberspace through user portals, email, web browsers, chat clients, web-enabled applications, and updates.

The cyberthreat has expanded dramatically in recent years through a series of damaging incidents.

Bioinformatics software is still not hardened against cyberattacks. There is a need to promote the widespread adoption of standard software best practices for security, such as input sanitisation, use of memory-safe languages or bounds checking on buffers and regular security audits.

Patching remains a challenge because analytics software often resides in individually managed repositories and is not regularly updated.

A MAPPING OF KNOWN CYBERBIOSECURITY CHALLENGES AND EXISTING GAPS

Exploitable technology and a range of (still under-assessed) attack vectors include:

- (a) databases (including genomic, list of dangerous genes or organisms), design-build-test libraries and rules, simulations, test data, sample records,

- (b) individual personal computers, lab equipment and processes, mission-critical devices and hardware (e.g. assemblers, synthesisers, sensors),

- (c) mission-critical software (e.g. workflow controls, process controls),

- (d) local and remote networks, and

- (e) raw materials, supplies and actual biomatter.

Notably, many of the devices used throughout the biotech sector are portable, and most are connected to the internet.

Challenges arise not only at the level of application but even during research as well as at the design, build and test level.

Thanks to the inherent vast variation in nature, biological processes are difficult to grasp. Computerised or automated results (e.g. molecular diagnostic tests) are next to impossible to verify with the naked eye. Yet more traditional tests and processes throughout the life-science fields have been replaced by computer technology.
Practical skill and hands-on experience are no longer the focus.
Furthermore, more credence is often given to a computerised output (e.g. in diagnostics) than to clinical observations.

While biological or medical decision making was traditionally based on consensus and expert opinion, computer simulations or automated processes could easily be distorted and manufactured without anyone being able to tell the difference.

Examples of known attacks show how easy it is to compromise sensors and protocols and to, for example, achieve misdiagnosis of skin cancer, referable diabetic retinopathy and pneumonia by automated processes.

A LARGELY UNRECOGNISED BIOTECH THREAT LANDSCAPE

The most studied cyberbiosecurity danger probably involves pathogenic databases. Several studies have shown extensive cybersecurity vulnerabilities which are exacerbated by the human interface (errors and social engineering attacks).

The danger is not only that bad actors could 'create' dangerous microorganisms from unsecured digital information. Just as concerning is the fact that erroneous or manipulated data can compromise international research activities and public health responses during outbreaks of disease (e.g. when trying to understand, model and detect new pathogens).

More generally, cyberbiosecurity vulnerabilities can lead to disruption of CIA at all levels (including biosynthetic pathways and processes, software, hardware, mission-critical devises etc.) and scales (from biological processes at the molecular level to genetically-modified plants, microbes or animals).

Notably, as biotech is only able to work with small biological snippets (e.g. 'marker genes' or 'DNA signatures', which are believed to represent the whole organism), establishing genuine 'integrity' of biological entities or processes (e.g. genuine GMOs versus illicit or manipulated ones) is in many cases technically impossible.

Impairment of the confidentiality of biologic data can, for example, leak pathogenic data. Illicit access to, for example, synthetic processes or critical biomatter can result in the hazardous distribution of biological agents with a potential global impact.

Making only manipulated devices or processes available can lead to erroneous medical treatment or misdetection attacks - whereby the device or service could appear to be functioning while it actually provides false results. For example, with modern sequencing technologies, this could lead to false diagnostics.

Such attacks could even have a global impact when no other molecular tests are available, as is often the case with novel pathogens.

On the other hand, lack of availability (including supply chain attacks) can result in shortages of drugs, medical supplies, food, knowledge and others.

To read more:
https://www.enisa.europa.eu/publications/research-and-innovation-brief

Number 4

Remarks at Securities Enforcement Forum West 2022

Gurbir S. Grewal, Director, SEC Division of Enforcement

Good afternoon everyone.

Thank you to Bruce Carton for the invitation to speak today and to Professor Joe Grundfest for the very kind introduction.

As is customary, my remarks today express my views, and don't necessarily reflect those of the Commission, the Commissioners, or other members of staff.

Ordinarily at an event like this one, I'd speak about all that ways in which we are working to protect investors, including our increased focus on the private fund space, the additional resources we've committed to our Crypto Assets and Cyber Unit, and other enforcement priorities.

And I'd likely close by reassuring each of you in the defense bar that we're not doing away with the White Paper and Wells processes, but rather streamlining them. But I'd like to take a different approach today given some recent experiences and observations.

An animating principle for me in this role has been to increase public confidence in our markets and in government—to counter the declining trust in our institutions that we are experiencing.

There is a perception among large segments of the population that corporate wrongdoers are not being held accountable and that there are two sets of rules: one for the big and powerful and another for everyone else. While there are many reasons for these beliefs and trends, delayed accountability does not help.

That's why, since day one, I've been asking staff to look for ways in which to push the pace of our investigations. The public needs to know when they read a news story about corporate malfeasance that we will move quickly to investigate what happened and hold wrongdoers accountable, even in the most complex cases. You saw an example of that recently in our actions against Archegos Capital Management, its founder Bill Hwang, and others.

But one thing I hear frequently from staff is how the conduct of defense counsel in some cases frustrates and delays our truth-seeking mission. For example, I recently learned about a document production in an investigation concerning an entity with billions in assets that it would be overly generous to refer to as a rolling production.

Despite our best efforts, we've received a little over 200 documents over the course of the last six months, including a single page recently produced in response to requests for U.S. customer account and trading data. One page. Needless to say, that makes it difficult for us to assess whether there's been a violation of the securities laws.

None of this is new. About a decade ago, one of my predecessors—Rob Khuzami—gave a speech about questionable behavior by defense counsel in SEC investigations.

From slow-rolling document productions as I just described—to representing multiple witnesses with adverse interests in the same matter—to kicking witnesses during testimony to get them to answer questions a certain way, Director Khuzami catalogued many ways in which defense counsel undermined the SEC's investigative process.

Unfortunately ten years on from that speech, we continue to see some of these behaviors, as well as newer forms of the same tactics. In other words, while defense counsel may have stopped kicking witnesses under the table, they've moved to more subtle behaviors.

To be clear, I fully appreciate and welcome zealous advocacy. After all, good defense lawyers help ensure that our enforcement decisions are fair and informed. But dilatory or obstructive conduct is not zealous advocacy. It is behavior that frustrates our processes, puts investors at risk, and contributes to that declining trust I described.

Delay, for example, may enable a fraudster to dissipate assets or place them beyond our reach. A needlessly lengthy accounting fraud investigation could mean that markets lack accurate information about a public company for an extended period. And advisory clients unaware of a potential conflict may keep money invested with a firm, when, given full information, they would choose another money manager.

Protracted investigations also impose costs on the individuals and firms involved. Most obviously, there are the reputational costs that an issuer might incur after disclosing an investigation but before its delayed resolution. Those reputational costs may, in turn, impose economic costs

on shareholders. There are also, of course, the legal bills incurred as a result of unduly extended negotiations or needless disputes over routine investigatory issues.

And, finally, there are the psychological or emotional costs for witnesses involved in investigations. When counsel decide to dispute plainly reasonable requests, delay productions, prolong testimony, or otherwise frustrate our investigations, it can exacerbate all of these costs.

For these reasons and others, it's in our collective interest to ensure that our investigations move quickly and efficiently.

To read more:
https://www.sec.gov/news/speech/grewal-remarks-securities-enforcement-forum-west-051222

Number 5

Thematic Review on Out-of-Court Corporate Debt Workouts (OCW) - Peer Review Report

Financial Stability Board (FSB) member jurisdictions have committed, under the FSB Charter and in the FSB Framework for Strengthening Adherence to International Standards, to undergo periodic peer reviews.

To fulfil this responsibility, the FSB has established a regular programme of country and thematic peer reviews of its member jurisdictions.

Thematic reviews focus on the implementation and effectiveness across the FSB membership of international financial standards developed by standard-setting bodies and policies agreed within the FSB in a particular area important for global financial stability.

Thematic reviews may also analyse other areas important for global financial stability where international standards or policies do not yet exist.

The objectives of the reviews are to encourage consistent cross-country and cross-sector implementation; to evaluate (where possible) the extent to which standards and policies have had their intended results; and to identify gaps and weaknesses in reviewed areas and to make recommendations for potential follow-up (including through the development of new standards) by FSB members.

This report describes the findings of the peer review on out-of-court corporate debt workouts, including the key elements of the discussion in the FSB Standing Committee on Standards Implementation (SCSI).

It is the sixteenth thematic review conducted by the FSB and is based on the objectives and guidelines for the conduct of peer reviews set forth in the Handbook for FSB Peer Reviews.

The analysis and conclusions of this peer review reflect information as of mid-February 2022 unless otherwise noted.

The draft report for discussion by SCSI was prepared by a team chaired by Tomoko Amaya (since November 2021, Japan Financial Services Agency) and previously by Juan Pablo Graf Noriega (until November 2021, Comisión Nacional Bancaria y de Valores, Mexico). The team comprised Qin Liu (People's Bank of China), Eva-Maria Luedemann (Deutsche Bundesbank), Shashank Saksena (Ministry of Finance, India), Federico

Fornasari (Banca d'Italia), Tomio Mizutani (Japan Financial Services Agency), Cayetana Lado (Instituto de Crédito Oficial, Spain), Paul Bannister (Insolvency Service, United Kingdom), Lisa Kraidin (Federal Reserve Bank of New York), Adam Schupack (Department of the Treasury, United States), José M. Garrido (International Monetary Fund), Mahesh Uttamchandani (World Bank), Kristine Drevina (European Central Bank) and Miriam Parmentier (European Commission). Michael Januska and Marianne Klumpp (FSB Secretariat), José Manuel Portero (Comisión Nacional del Mercado de Valores, Spain) and Harry Lawless (World Bank) provided support to the team and contributed to the preparation of the report.

Table of Contents

Out-of-court workout (OCW)	A privately negotiated debt restructuring between the debtor and all or some of its creditors. Examples of OCWs show a vast array of negotiated restructurings along a continuum of increasing formality, reflecting broadly the extent of institutional involvement. • On the informal side of the continuum are purely informal OCWs, which basically do not follow formal requirements, but may be based on (non-binding) common principles or practices. • Enhanced OCWs are in the middle of the spectrum. They do not involve courts, but benefit from other features such as third-party coordination or a dedicated process or incentives framework. • Hybrid OCWs are on the formal end of this spectrum as they involve courts at limited points in the process and for limited tasks. This report uses these categories to provide structure and orientation. A specific framework or procedure may not clearly fall into one category as opposed to another or be regarded as falling into a different category than that described here.
Enhanced OCW	A privately negotiated debt restructuring between the debtor and all or some of its creditors, which does not involve courts, but benefits from other supporting features, such as third party (possibly administration or authority) coordination or a dedicated process or incentives framework. In some variants, participants are bound by law or contract to follow restructuring-specific standards introduced by an administrative authority, in accordance with an expectation or requirement set out by that authority. In the context of this report, codes of conduct, debt restructuring schemes, master restructuring agreements and alternative dispute resolution are considered a modality of enhanced OCW.

To read more: https://www.fsb.org/wp-content/uploads/P090522.pdf

Number 6

Strengthening EU-wide cybersecurity and resilience – provisional agreement by the Council and the European Parliament

The Council and the European Parliament agreed on measures for a high common level of cybersecurity across the Union, to further improve the resilience and incident response capacities of both the public and private sector and the EU as a whole.

Once adopted, the new directive, called 'NIS2', will replace the current directive on security of network and information systems (the NIS directive).

Stronger risk and incident management and cooperation

NIS2 will set the baseline for cybersecurity risk management measures and reporting obligations across all sectors that are covered by the directive, such as energy, transport, health and digital infrastructure.

The revised directive aims to remove divergences in cybersecurity requirements and in implementation of cybersecurity measures in different member states. To achieve this, it sets out minimum rules for a regulatory framework and lays down mechanisms for effective cooperation among relevant authorities in each member state. It updates the list of sectors and activities subject to cybersecurity obligations, and provides for remedies and sanctions to ensure enforcement.

The directive will formally establish the European Cyber Crises Liaison Organisation Network, EU-CyCLONe, which will support the coordinated management of large-scale cybersecurity incidents.

Widening of the scope of the rules

While under the old NIS directive member states were responsible for determining which entities would meet the criteria to qualify as operators of essential services, the new NIS2 directive introduces a size-cap rule. This means that all medium-sized and large entities operating within the sectors or providing services covered by the directive will fall within its scope.

While the agreement between the European Parliament and the Council maintains this general rule, the provisionally agreed text includes

additional provisions to ensure proportionality, a higher level of risk management and clear-cut criticality criteria for determining the entities covered.

The text also clarifies that the directive will not apply to entities carrying out activities in areas such as defence or national security, public security, law enforcement and the judiciary. Parliaments and central banks are also excluded from the scope.

As public administrations are also often targets of cyberattacks, NIS2 will apply to public administration entities at central and regional level. In addition, member states may decide that it applies to such entities at local level too.

Other changes introduced by the co-legislators

The European Parliament and the Council have aligned the text with sector-specific legislation, in particular the regulation on digital operational resilience for the financial sector (DORA) and the directive on the resilience of critical entities (CER), to provide legal clarity and ensure coherence between NIS2 and these acts.

A voluntary peer-learning mechanism will increase mutual trust and learning from good practices and experiences, thereby contributing to achieving a high common level of cybersecurity.

The two co-legislators have also streamlined the reporting obligations in order to avoid causing over-reporting and creating an excessive burden on the entities covered.

Member states will have 21 months from the entry into force of the directive in which to incorporate the provisions into their national law.

Next steps

The provisional agreement concluded today is now subject to approval by the Council and the European Parliament.

On the Council's side, the French presidency intends to submit the agreement to the Council's Permanent Representatives Committee for approval soon.

To read more:
https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/r

enforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

NOTE	
From:	General Secretariat of the Council
To:	Council
No. prev. doc.:	9583/2/21, 11724/21
No. Cion doc.:	14150/20
Subject:	Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148 *- General Approach*

Number 7

Fighting child sexual abuse: European Commission proposes new rules to protect children

European Commission

The Commission is proposing new EU legislation to prevent and combat child sexual abuse online.

With 85 million pictures and videos depicting child sexual abuse reported worldwide in 2021 alone, and many more going unreported, child sexual abuse is pervasive.

The COVID-19 pandemic has exacerbated the issue, with the Internet Watch foundation noting a 64% increase in reports of confirmed child sexual abuse in 2021 compared to the previous year.

The current system based on voluntary detection and reporting by companies has proven to be insufficient to adequately protect children and, in any case, will no longer be possible once the interim solution currently in place expires.

Up to 95% of all reports of child sexual abuse received in 2020 came from one company, despite clear evidence that the problem does not only exist on one platform.

To effectively address the misuse of online services for the purposes of child sexual abuse, clear rules are needed, with robust conditions and safeguards.

The proposed rules will oblige providers to detect, report and remove child sexual abuse material on their services.

Providers will need to assess and mitigate the risk of misuse of their services and the measures taken must be proportionate to that risk and subject to robust conditions and safeguards.

A new independent EU Centre on Child Sexual Abuse (EU Centre) will facilitate the efforts of service providers by acting as a hub of expertise, providing reliable information on identified material, receiving and analysing reports from providers to identify erroneous reports and prevent them from reaching law enforcement, swiftly forwarding relevant reports for law enforcement action and by providing support to victims.

The new rules will help rescue children from further abuse, prevent material from reappearing online, and bring offenders to justice. Those rules will include:

- **Mandatory risk assessment and risk mitigation measures:** Providers of hosting or interpersonal communication services will have to assess the risk that their services are misused to disseminate child sexual abuse material or for the solicitation of children, known as grooming. Providers will also have to propose risk mitigation measures.

- **Targeted detection obligations, based on a detection order:** Member States will need to designate national authorities in charge of reviewing the risk assessment. Where such authorities determine that a significant risk remains, they can ask a court or an independent national authority to issue a detection order for known or new child sexual abuse material or grooming. Detection orders are limited in time, targeting a specific type of content on a specific service.

- **Strong safeguards on detection:** Companies having received a detection order will only be able to detect content using indicators of child sexual abuse verified and provided by the EU Centre. Detection technologies must only be used for the purpose of detecting child sexual abuse. Providers will have to deploy technologies that are the least privacy-intrusive in accordance with the state of the art in the industry, and that limit the error rate of false positives to the maximum extent possible.

- **Clear reporting obligations:** Providers that have detected online child sexual abuse will have to report it to the EU Centre.

- **Effective removal:** National authorities can issue removal orders if the child sexual abuse material is not swiftly taken down. Internet access providers will also be required to disable access to images and videos that cannot be taken down, e.g., because they are hosted outside the EU in non-cooperative jurisdictions.

- **Reducing exposure to grooming:** The rules require app stores to ensure that children cannot download apps that may expose them to a high risk of solicitation of children.

- **Solid oversight mechanisms and judicial redress:** Detection orders will be issued by courts or independent national authorities. To minimise the risk of erroneous detection and reporting, the EU Centre will verify reports of potential online child sexual abuse made by providers before sharing them with law enforcement authorities and

Europol. Both providers and users will have the right to challenge any measure affecting them in Court.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down rules to prevent and combat child sexual abuse

(Text with EEA relevance)

{SEC(2022) 209 final} - {SWD(2022) 209 final} - {SWD(2022) 210 final}

Article 1

Subject matter and scope

1. This Regulation lays down uniform rules to address the misuse of relevant information society services for online child sexual abuse in the internal market.

It establishes, in particular:

(a) obligations on providers of relevant information society services to minimise the risk that their services are misused for online child sexual abuse;

(b) obligations on providers of hosting services and providers of interpersonal communication services to detect and report online child sexual abuse;

(c) obligations on providers of hosting services to remove or disable access to child sexual abuse material on their services;

(d) obligations on providers of internet access services to disable access to child sexual abuse material;

(e) rules on the implementation and enforcement of this Regulation, including as regards the designation and functioning of the competent authorities of the Member States, the EU Centre on Child Sexual Abuse established in Article 40 ('EU Centre') and cooperation and transparency.

To read more:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472

Number 8

Global experts examine the changing face of match-fixing

ABU DHABI, United Arab Emirates – The 12th meeting of INTERPOL's Match-Fixing Task Force (IMFTF) has concluded with a call to harmonize global efforts to curb competition manipulation.

The three-day (10-12 May) meeting brought together integrity and intelligence specialists from some 50 countries, representing law enforcement, public authorities, sports federations, anti-doping organizations and betting monitoring services.

It was the first major event held under the banner of INTERPOL's newly-created Financial Crime and Anti-Corruption Centre (IFCACC), which provides a coordinated global response against the exponential growth in transnational financial crime and corruption.

Discussions focused on mechanisms to boost intelligence sharing and close legislative and institutional gaps, such as the establishment of National Platforms, as outlined in the Macolin Convention, which centralize and analyse information on irregular and suspicious trends.

With criminal organizations increasingly operating across betting and sports markets, participants discussed the emerging uses of technology, big data and social media. They also acknowledged that match-fixers are still very much relying on tried and true methods of manipulation, such as targeting the entourage of athletes and grooming young players, pointing to a continued need for education.

INTERPOL provided an overview on the specific tools available to law enforcement dedicated to data collection on sport corruption (project ETICA) and financial crimes analysis (FINCAF). A number of countries presented recently issued INTERPOL Purple Notices providing information on modus operandi linked to social media, identity theft, ghost and fake matches.

The meeting included a closed-door session for specialized investigators to share case studies, discuss emerging match-fixing tactics and hold multi and bilateral meetings to coordinate active international cases.

Exchanges revealed that while betting intelligence remained important to investigations, other sources of intelligence also needed to be exploited. For

example, although doping has traditionally been viewed through a drug-enforcement lens, participants heard that positive doping tests and alerts could be a valuable source of intelligence for integrity investigations, notably on the criminal organizations behind competition manipulation.

INTERPOL and the International Olympic Committee (IOC) held a side event dedicated to stakeholders in the United Arab Emirates, in order to raise awareness, build capacity and enhance national mechanisms to prevent, detect and sanction competition manipulation.

The IMFTF was created in 2011 to support member countries with investigations and law enforcement operations in all sports, and maintain a global network of investigators for the sharing of information, intelligence and best practices. It now includes 100 member units, with more than 150 National Points of Contact worldwide.

To read more:
https://www.interpol.int/News-and-Events/News/2022/Global-experts-examine-the-changing-face-of-match-fixing

Number 9

Joint Statement of the 25th ASEAN+3 Finance Ministers' and Central Bank Governors' Meeting

Monetary Authority of Singapore

I. Introduction

1. The 25th ASEAN+3 Finance Ministers' and Central Bank Governors' Meeting (AFMGM+3) was convened on 12 May 2022 under the co-chairmanship of H.E. Dr. Aun Pornmoniroth, Deputy Prime Minister and Minister of Economy and Finance of the Kingdom of Cambodia, H.E. Sum Sannisith, Deputy Governor of the National Bank of Cambodia and H.E. Liu Kun, Minister of Finance of the People's Republic of China, H.E. Chen Yulu, Deputy Governor of the People's Bank of China.

The meeting was held in virtual format under the extraordinary circumstances due to the COVID-19 pandemic. The Vice President of the Asian Development Bank (ADB), the Director of the ASEAN+3 Macroeconomic Research Office (AMRO), the Deputy Secretary-General of ASEAN, and the Deputy Managing Director of the International Monetary Fund (IMF) were also present at the meeting.

2. We exchanged views on current developments and the outlook for the global and regional economies, as well as policy responses to risks and challenges. In view of the challenges ahead, we recognize that ASEAN+3 financial cooperation has a more essential role to play in supporting regional economies to navigate these obstacles.

In this regard, we agree to further deepen our collaboration to enhance regional financial cooperation, including through the Chiang Mai Initiative Multilateralisation (CMIM), AMRO, Asian Bond Markets Initiative (ABMI), and ASEAN+3 Future Initiatives.

II. Recent Economic and Financial Developments in the Region

3. The ASEAN+3 economies have remained steadfast in weathering the challenges posed by the COVID-19 pandemic. Since early 2021, we have focused on ramping up the vaccination rates to protect our populations and have adopted more targeted containment measures to minimize the impact on our economies and to support recovery.

As a result, the region saw robust growth of around 6 percent in 2021. Looking ahead, given the strong protection afforded by high vaccination

rates in the region, the region can look forward to further opening-up and stronger economic recovery this year.

However, the sharper-than-expected monetary policy normalization in some major advanced economies, continuing supply chain disruptions, and rising food and energy prices aggravated by the current Russia-Ukraine conflict may pose downside risks to the outlook for the region's trade and investment, growth, and inflation.

4. We recognize that continuing supportive policies are crucial in alleviating the impact of the pandemic and strengthening a sustained economic recovery.

At the same time, we acknowledge the importance of avoiding misallocation of resources and ensuring support for new and growing sectors.

We will calibrate policy measures introduced in response to the pandemic as the economic recovery gains traction, preserve monetary and financial stability and long-term fiscal sustainability, and safeguard against downside risks and negative spillovers.

5. The pandemic has caused scarring effects in various extent to the ASEAN+3 economies. However, it has also provided a strong boost for digitally supplied services such as e-commerce, digital financial services, and telehealth.

Closer intra-regional cooperation—in the areas of trade and investment, supply chain logistics and resilience, customs systems inter-connectivity, cross-border flows, sustainable and green infrastructure, and digital integration—will further expand the region's opportunities to secure post-pandemic growth, minimize scarring, and prepare for future shocks.

In this regard, we remain firmly committed to an open and rules-based multilateral trade and investment system and resolve to further strengthen intra-regional ties. We welcome and fully support the coming into force of the Regional Comprehensive Economic Partnership.

We also recognize that the long-term growth outlook for the region is contingent on how the region manages climate-related risks.

With these in mind, we acknowledge the merits of collaborating towards strong and inclusive recovery and making continued progress in the 2030 Agenda for Sustainable Development to achieve stronger, greener and more balanced global development.

III. Strengthening Regional Financial Cooperation

Chiang Mai Initiative Multilateralisation (CMIM)

6. The COVID-19 pandemic, its economic impact, and the uncertainties surrounding the global economy have highlighted the importance of further strengthening the CMIM. In this regard, we welcome the adoption of a new reference rate for CMIM liquidity support arrangements, which will align CMIM reference rate with global financial market conventions.

We also welcome the updated CMIM Operational Guidelines (OG) on the use of each member's own local currency for CMIM arrangements, which took effect in January 2022. We appreciate members' efforts in strengthening accessibility of CMIM arrangements, by allowing requesting members to prepare medium term economic targets and policy plans with more flexibility.

7. We are pleased with the progress made in further developing the CMIM OG to enable a member to provide a local currency of another member (third-party local currency), in addition to its own domestic currency, for CMIM liquidity support. Going forward, we task the Deputies to continue discussing local currency procedural arrangements, with a view towards finalizing the OG by the end of 2022.

8. We note the efforts undertaken to review the CMIM margin structure and task the Deputies to continue the discussions with the aim of concluding the review by the end of this year. This is an important step in improving CMIM's accessibility and reliability while ensuring that CMIM will be an effective financing option for members in times of need.

We commend members for adopting an indicative work plan to discuss the CMIM medium- to long-term future direction and other related issues in the context of the second periodic review, which is to be completed by 2024. Hence, we task the Deputies, with AMRO's support, to continue relevant discussions on CMIM future direction.

9. We also welcome the successful completion of the 12th Test Run, which was conducted in 2021. The test run assessed the eligibility of a requesting member to access the facility, by using the Economic Review and Policy Dialogue (ERPD) matrix framework, and demonstrated the operational readiness of the CMIM-Precautionary Line IMF de-linked portion.

We are confident that the 13th Test Run, to be conducted jointly with the IMF later this year, will further enhance the operational readiness of the

CMIM and better support its members by ensuring the procedures for smooth and timely transition from the CMIM IMF de-linked portion to the IMF-linked portion.

We encourage AMRO to continue strengthening coordination with the IMF and other regional financing arrangements, to support ASEAN+3 members to tap the full strength and scale of the global financial safety net when needed.

ASEAN+3 Macroeconomic Research Office (AMRO)

10. Since its establishment in 2011, AMRO has played an important role in helping to safeguard macroeconomic and financial stability in the ASEAN+3 region through robust surveillance and strong technical support to the CMIM. We congratulated AMRO on its ten-year anniversary celebration in December 2021 for its achievements in the past decade.

11. Given the fast-changing external environment and increasing demands from ASEAN+3 members, we support the initiative to review AMRO's Strategic Direction (SD) and identify new areas where AMRO may provide support to members in addressing the challenges ahead. We also support the proposal to develop a detailed implementation plan, including the build-up of a regional think-tank network to strengthen AMRO's role as a Regional Knowledge Hub (RKH).

We look forward to the finalization and approval of AMRO's updated SD, which will include the implementation plan of the RKH, by the end of this year. We look forward to consequent updates to other AMRO strategies and policies including the Performance Evaluation Framework and building a competent staff team based on merit and geographical balance, especially from developing member countries, for better alignment with AMRO's updated SD.

12. We encourage AMRO to play a larger role in supporting the ASEAN+3 Finance Process by providing thought-leadership, and serving as a knowledge sharing platform for key issues that will impact the region. In this regard, we welcome AMRO's inaugural participation as an Observer at the ASEAN+3 Leaders' Summit in 2021 and affirm our full support for AMRO's continued participation at future Leaders' Summits.

13. We welcome the consistent progress in AMRO's surveillance capacity and AMRO's continued efforts in this regard. We encourage AMRO to establish itself as the authoritative regional voice on ASEAN+3 macro-economic and financial stability issues on the global stage, including

through enhancing partnerships with international organizations and research institutions.

We welcome AMRO's publication of its policy position paper on capital flow management and macroprudential policy measures in the ASEAN+3 region. We also appreciate AMRO's efforts in developing more analytical tools and making them available to the members.

We encourage AMRO to mainstream emerging and structural issues, such as financial digital transformation, climate change, population aging, and supply chain reconfiguration in its surveillance work, and to strengthen its role as a trusted advisor by providing members with targeted and pragmatic policy advice aimed at maintaining macroeconomic and financial stability, advancing economic transformation, and pursuing sustainable development.

We encourage AMRO to conduct more in-depth surveillance and give policy advice independently, and to tailor its work perspectives based on the characteristics of the ASEAN+3 region and member economies to ensure that its recommendations are applicable.

14. We appreciate AMRO's support to the CMIM's operational readiness and welcome the expansion of its Technical Assistance (TA) team and enhancement of its TA activities.

We commend China's, Japan's and Korea's continued financial contributions to AMRO to strengthen its TA function, as well as continued participation and support from ASEAN members in AMRO's TA work.

We welcome the Medium-term Implementation Plan 2022-2026 as endorsed by the Deputies and encourage AMRO to continue to strengthen its accountability through the Integrated Evaluation Cycle.

15. We welcome AMRO's support in launching the ASEAN+3 Finance Process Online Repository in August 2021. The repository has proven to be a valuable resource for knowledge management within the ASEAN+3 finance track.

As ASEAN+3 continues to expand and deepen the regional financial collaboration, we encourage the Deputies to explore ways to further strengthen the effectiveness and efficiency of the ASEAN+3 finance process going forward, with greater support from AMRO.

16. We express our deep appreciation to the outgoing AMRO Director, Mr. Doi Toshinori, for his excellent stewardship of AMRO over the past

three years. Despite the uncertainty and disruptions caused by the COVID-19 pandemic, Mr. Doi competently steered AMRO through these challenges to continue providing timely, robust and relevant analyses to help the region navigate these challenging times.

We welcome the incoming Director, Dr. Li Kouqing, and look forward to working with him fruitfully in the next three years. We expect continued efforts in improving AMRO's inclusiveness and diversity with support from all ASEAN+3 members.

Asian Bond Markets Initiative (ABMI)

17. We acknowledge the ABMI's continued progress toward implementing the ABMI Medium-Term Road Map 2019-2022, which aims to strengthen support for infrastructure finance, create an ecosystem for sustainable bond market development, promote regulatory standardization and harmonization, improve bond market infrastructure to facilitate cross-border transactions, and foster collaboration among regional initiatives.

We appreciate the ADB's work in this regard and look forward to more tangible achievements in further deepening the development of the local currency bond market.

18. We commend the Credit Guarantee and Investment Facility (CGIF)'s on-going efforts to expand and innovate the issuance of local currency bonds despite the difficulties under the pandemic.

We support regional efforts to develop green, social, and sustainability bonds, and look forward to the report on sustainable finance in ASEAN+3 being published.

We welcome the continued enhancements to AsianBondsOnline (ABO) and the progress of ongoing research to assess the status of the "double mismatch problem" under the ASEAN+3 Bond Market Forum (ABMF), which will provide recommendations and suggestions for the next round of the ABMI Medium-Term Road Map.

We take note of the study under the Cross-Border Settlement Infrastructure Forum (CSIF) which assesses the recent technological advances in the ASEAN+3 region and the Asia Prime Collateral Forum (APCF)'s efforts to advance collateral utilization in the ASEAN+3 region. We look forward to more capacity building through the Technical Assistance Coordination Team (TACT).

ASEAN+3 Future Initiatives

19. We welcome the substantial progress made in deepening and broadening ASEAN+3 financial cooperation, including those made by the four Working Groups (WGs).

We acknowledge the recommendations of WG1 to explore the pilot usage of standardized core project finance loan documents and partner with the ADB to draft a report on regional post-COVID infrastructure priorities. We are pleased with the progress made by WG2 in developing the ASEAN+3 Macro-structural Framework with the support of AMRO.

We acknowledge the concept paper prepared by WG3 to conduct a detailed study among ASEAN+3 members with the aim to launch a new ASEAN+3 initiative on Disaster Risk Financing building on the existing regional initiatives such as the ASEAN Disaster Risk Financing and Insurance (ADRFI) and the Southeast Asia Disaster Risk Insurance Facility (SEADRIF).

We welcome WG4's work on improving regional policy coordination on fintech and introducing Open Banking System as one of the areas for technical cooperation in the region. We encourage the four WGs to make further progress, with concrete outcomes to deepen the cooperation in these areas.

20. We welcome the proposal and discussion on the two new initiatives of Financial Digitalization and Transition Finance, which are well-aligned with the development trend within the region.

We acknowledge the importance of opportunities and challenges of financial digitalization from the perspective of regional financial cooperation, and look forward to the assessment of its potential implications on Regional Financing Arrangements (RFAs) for forward-looking recommendations on potential adjustments of RFAs. We welcome AMRO's initial research on this new agenda and look forward to its further support.

We recognize the role of transition finance in facilitating low carbon transition of carbon-intensive sectors in ASEAN+3 economies, and welcome the work plan on transition finance as a good starting point to better understand members' needs, concerns, and potential recommendations. This will contribute towards more sustainable development in the region and complement relevant global work. We encourage the Deputies to continue the work on the two new initiatives and

come up with concrete proposals to contribute to the future ASEAN+3 finance process.

ASEAN+3 Financial Cooperation in Disaster Risk Financing and Insurance

21. We continue to support the efforts of the SEADRIF in strengthening the financial resilience of ASEAN member countries against disaster risks, with support from the ASEAN Secretariat and the World Bank. We welcome the membership expansion of SEADRIF and the progress of the Public Asset Financial Protection Program. We also welcome the remaining ASEAN+3 member countries to join SEADRIF, and for donor partners beyond the ASEAN+3 region to support this initiative.

IV. Conclusion

22. We express our appreciation to the governments of the Kingdom of Cambodia and the People's Republic of China for their excellent arrangements as the Co-chairs of the ASEAN+3 Finance Ministers' and Central Bank Governors' Process in 2022. We agreed to meet in Incheon, Korea in 2023, and look forward to working with Indonesia and Japan as the Co-chairs of the ASEAN+3 Finance Ministers' and Central Bank Governors' Process in 2023.

To read more:
https://www.mas.gov.sg/news/media-releases/2022/joint-statement-of-the-25th-asean-plus-3-finance-ministers-and-central-bank-governors-meeting

Number 10

New Guidance – Biometric authentication in Automatic Access Control Systems (AACS)

Designing, building and operating AACS that include biometric authentication

CPNI
Centre for the Protection of National Infrastructure

Overview

The purpose of any access control system is, quite simply, to control who goes where and when. The person in question maybe an employee, a contractor or a visitor.

The level of access can and will vary depending on their status and access requirements or the location they are entering.

The access control "system" can be seen in different ways. For example: the door, the lock, the access control panel and the method of entry (e.g. token and reader) can be seen as a "system".

For the purposes of clarity, CPNI group the "system" into the following sub categories:

AACS

Automatic Access Control System (AACS) – this is the control panel, the decision maker. It is on this panel, or software, that the decision to allow entry is made. It is here that permissions are granted, where individuals are enrolled onto the system and given the rules of entry; for example, where they are allowed to enter and when.

Token & Readers

Token, Reader, Keypad – this is effectively the "key" to the door. The token is generally (not necessarily) a card. This card will be held to the reader. If the card has been activated and is a valid credential, then access will be granted.

The token and reader alone will offer "single factor authentication". For additional security, a keypad is connected. This requires a Personal Identification Number (PIN) to be used alongside the token and reader – Multi-factor authentication.

BAACS

Biometric Automatic Access Control Systems (BAACS) – this uses a particular biometric (e.g. fingerprint) to gain access.

Biometric authentication can be single factor (biometric only) or multi-factor) token and biometric. There are a number of biometric 'modalities' which can be used for access control (see CPNI BAACS Guidance).

To read more:
https://www.cpni.gov.uk/automatic-access-control-systems-0

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,

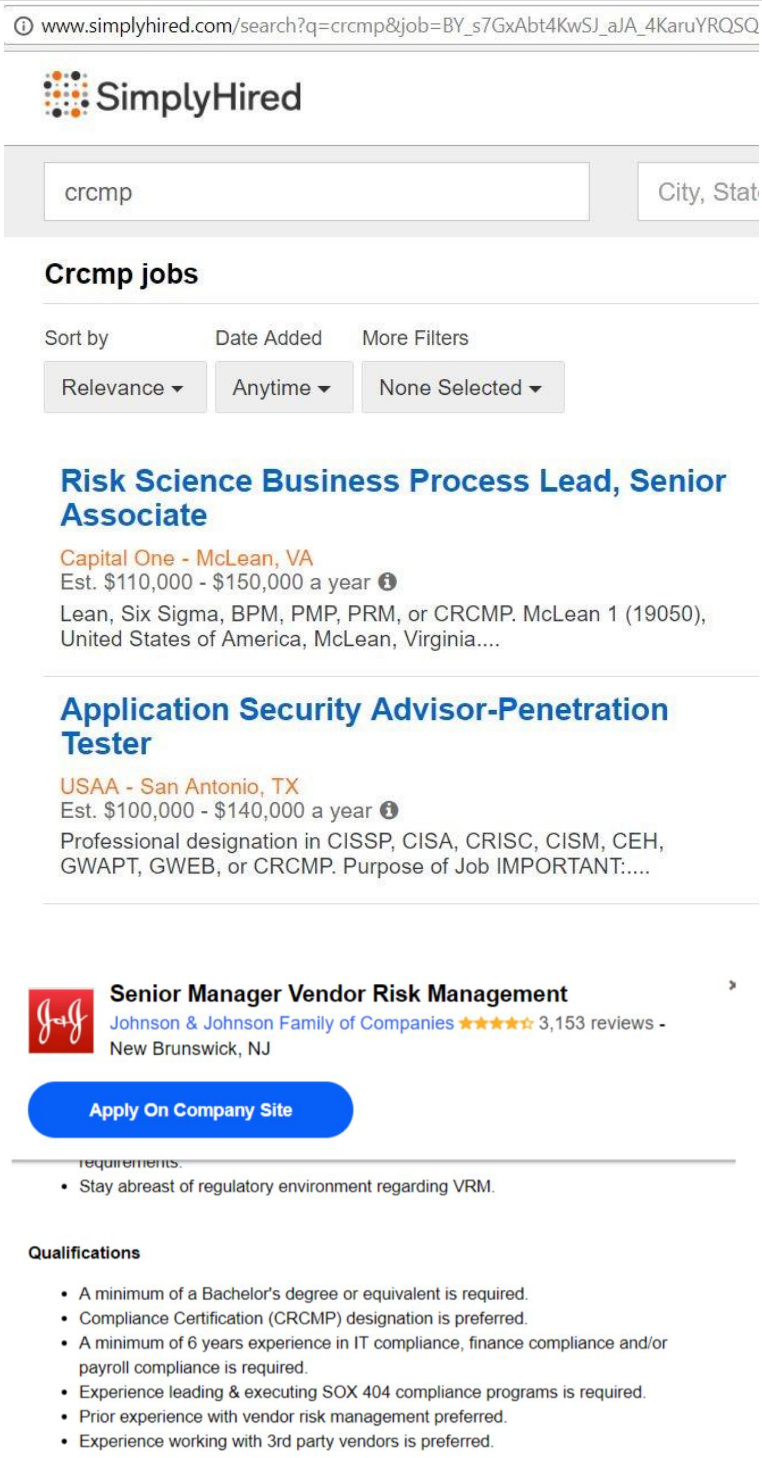
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.