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 16, 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,

I loved the question: *What is the best way to regulate machine learning in risk models?*

This is what BaFin and the Deutsche Bundesbank asked, and the findings of the consultation are now available. I was pleased to read responses in another major issue, the difference between *model maintenance* and *model change*.

According to BaFin and the Deutsche Bundesbank, institutions and enterprises are obligated to *inform supervisors* of any changes to Pillar 1 models and, if applicable, only implement these changes after they have been approved.

There is *no clear-cut distinction* between regular model maintenance and model change, which continually leads to discussions with supervisors,

especially as the term “model change” is also dependent on the prevailing supervisory context.

The consultation paper provided multiple examples of this. However, the flexibility and, in some cases, high-frequency adaptivity of Machine Learning (ML) procedures can make it *more difficult* to draw a clear distinction between adjustment and change that would be indispensable for supervisory purposes.

One important area of discussion in the consultation paper concerns the *explainability* of models. As the hypothesis space that can be depicted by the model becomes more complex and more highly dimensional, it also becomes more difficult to describe the functional relationship between input and output verbally or using mathematical formulae, and the details of the calculations are less comprehensible for modellers, users, validators and supervisors. As a result, it is more difficult, if applicable, to *verify* the validity of the model output as well.

This is an interesting approach. 13 years after the de Larosière report, we continue to have the same problems. (The de Larosière Group's mandate covered the issues of how to organize the supervision of financial institutions and markets in the EU; how to strengthen European cooperation on financial stability oversight, early warning and crisis mechanisms; and how EU supervisors should cooperate globally.)

We read in the de Larosière report: “The use by sophisticated banks of internal risk models for trading and banking book exposures has been another fundamental problem.

These models were often not properly understood by board members (even though the Basel 2 rules increased the demands on boards to understand the risk management of the institutions).

Whilst the models may pass the test for normal conditions, they were clearly based on too short statistical horizons and this proved inadequate for the recent exceptional circumstances.

Future rules will have to be better complemented by more reliance on judgement, instead of being exclusively based on internal risk models.

Supervisors, board members and managers should understand fully new financial products and the nature and extent of the risks that are being taken; stress testing should be undertaken without undue constraints; professional due diligence should be put right at the centre of their daily work.”

This is the most important part: Supervisors, board members and managers should *understand* fully new financial products and the nature and extent of the risks that are being taken.

Somebody has to explain the model risk to them. Albert Einstein had said that *if you can't explain it simply, you don't understand it well enough.*

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

Best regards,

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

Number 1 (Page 1)

Machine learning in risk models

BaFin Federal Financial Supervisory Authority

Number 2 (Page 1)

"The Name's Bond:" Remarks at City Week

Gary Gensler, Chair, U.S. Securities and Exchange Commission

Number 3 (Page 1)

Our Strategy 2022-2025

FCA FINANCIAL CONDUCT AUTHORITY

Number 4 (Page 1)

EBA proposes to simplify and improve the macroprudential framework

EBA EUROPEAN BANKING AUTHORITY

Number 5 (Page 1)

Joint Committee, Annual Report 2021

EBA EUROPEAN BANKING AUTHORITY | eiopa European Insurance and Occupational Pensions Authority | esma European Securities and Markets Authority | JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Number 6 (Page 1)

Supply Chain Guidance

CPNI Centre for the Protection of National Infrastructure

Number 7 (Page 1)

Government of Jersey publishes first National Risk Assessment of Non-Profit Organisations

Jersey Financial Services Commission

Number 8 (Page 1)

FINMA Annual Report

finma
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Number 9 (Page 1)

The HKMA launches the Regtech Knowledge Hub

HONG KONG MONETARY AUTHORITY
香港金融管理局

Number 10 (Page 1)

Final Report - Emission allowances and associated derivatives

esma European Securities and Markets Authority

Number 1

Machine learning in risk models

BaFin Federal Financial Supervisory Authority

What is the best way to regulate machine learning in risk models? BaFin and the Deutsche Bundesbank asked the companies for their input. The findings of the consultation are now available – the dialogue continues.

Banks and insurers want to use machine learning (ML) in their risk models; BaFin and the Deutsche Bundesbank see such use intertwined with fundamental supervisory and regulatory issues and want to discuss these issues with the companies and their associations.

The two authorities formulated a number of propositions and published them in a joint consultation paper in July 2021.

You may visit:
https://www.bundesbank.de/resource/blob/598256/5e89d5d7b7cd236ad93ed7581800cea3/mL/2020-11-policy-dp-aiml-data.pdf

DEUTSCHE BUNDESBANK EUROSYSTEM

Policy Discussion Paper
The Use of Artificial Intelligence and Machine Learning in the Financial Sector

The paper is entitled “Machine learning in risk models – Characteristics and supervisory priorities” .

The participants’ responses have now been evaluated and summarised; the results paper is available on the BaFin website at:
https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_Ergebnisse_machinelles_Lernen_Risikomodelle_en.html?nn=8813520

DEUTSCHE BUNDESBANK EUROSYSTEM

BaFin Bundesanstalt für Finanzdienstleistungsaufsicht

Machine learning in risk models – Characteristics and supervisory priorities
Responses to the consultation paper

The consultation specifically dealt with internal models that are used to calculate the regulatory own funds requirements in Pillar I of the regulatory frameworks for banks and insurers.

It also addressed the use of ML methods in risk management of Pillar II of the regulatory frameworks. While algorithms as such are not subject to supervisory approval, internal models must be approved by the supervisors – also if they involve the use of machine learning.

Machine learning in risk management

The consultation revealed that banks and insurers are already using methods of machine learning in many areas, such as money laundering and fraud detection or analyses in credit processes. The companies are also using ML methods in distribution and product pricing.

Though there have been only a few instances of ML technologies being used in Pillar I risk models to date, some banks and insurers consider the technologies to be highly promising. These methods are already being used today to validate internal models, for example as support or challenger tools.

Responses support BaFin and Bundesbank propositions

In their consultation paper, BaFin and the Bundesbank had suggested forgoing a definition of machine learning. Instead, they proposed supervisory practices that involved analysing a specific internal model in terms of certain characteristics and using these characteristics to determine the supervisory steps to be taken. This idea of a technology-neutral

approach met with broad consensus. The figure below illustrates the characteristics-based view, using two internal ratings-based approaches (IRBA) for banks' credit risk.

The consultation also revealed that banks, insurers and their associations consider the existing supervisory regulations to be sufficient, also for ML procedures. From their perspective, there is no need for a reform of the statutory requirements, at least at the fundamental level. The participants also approved the regulators and supervisors' current focus on the volume and suitability of the data basis and on data quality, the importance of which will be growing as the use of ML methods increases.

Methods of machine learning must be explainable

For BaFin, the Bundesbank and the consultation participants, the explainability of ML methods is a central factor for the successful application of machine learning. They all agree that further discussion will be needed to determine the point in time at which a model has changed so extensively due to machine learning that it would have to be approved again. From a supervisory point of view, it is therefore crucial that the development and use of the models remain comprehensible.

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2022/fa_bj_2202_Maschinelles_Lernen_en.html

Number 2

"The Name's Bond:" Remarks at City Week

Gary Gensler, Chair, U.S. Securities and Exchange Commission

Thank you. It's good to be with City Week again. As is customary, I'd like to note that my views are my own, and I am not speaking on behalf of the Commission or SEC staff.

Since we are in London (at least virtually), I wanted to note that this year marks the 60th anniversary of the first James Bond film. I know there are various commemorations of this storied franchise going on in the U.K., but I want to focus my remarks on the lead character's name.

Bond. James Bond.

Ian Fleming, the author of the spy novels, gave an interview with The New Yorker 60 years ago this month — several months before "Dr. No" hit theaters.

It turns out that Fleming wanted 007 to be "an extremely dull, uninteresting man." In fact, he borrowed the name "James Bond" from the author of a beloved childhood book on birds. When he was brainstorming names for his lead character, he thought, "[T]hat's the dullest name I've ever heard."

He added, "Now, the dullest name in the world has become an exciting one."

Fixed Income Markets

That brings me to a different kind of bond: the $50 trillion-plus U.S. bond markets.

The fixed income markets may not, on the surface, seem like the most cinematic part of the financial system. There are no "meme" bonds (at least, not yet). The nightly news is more likely to focus on stocks.

And yet, bonds are far from the "dullest" market in the world. They're incredibly important — to individuals, companies, and governments in the

U.S. and around the world. Fixed income markets, particularly government securities, money markets, and repurchase agreements ("repos"), are integral to how central banks around the globe administer monetary policy. As individual investors start to approach retirement, they often turn to fixed income as a lower-risk investment.

Altogether, the fixed income markets represent about half of the capital markets that the SEC oversees, making them just as big as the equity markets.

The $23 trillion Treasury market is the base upon which so much of our capital markets are built. Treasuries are how we, as the U.S. government and as taxpayers, raise money: We are the issuer.

The non-Treasury fixed income markets also are so critical.

They include the $14 trillion of asset-backed securities, funding our mortgage, auto, and credit card markets.

They include $10 trillion of corporate bonds, enabling companies to raise money for factories, jobs, and innovation.

They include $4 trillion of municipal bonds, allowing local governments to fund essential projects, like bridges, roads, and schools.

Altogether, the non-Treasury fixed income markets are more than 2.5 times larger than the commercial bank lending market. That's right — America turns more to bonds than to banks to fund their projects.

Given the size and importance of these markets, it's worth asking how we can modernize our rules for today's economy and technologies, so these markets can be as fair as possible for investors and as efficient as possible for issuers of all types.

The U.S. Congress and President Franklin Delano Roosevelt understood the importance of these markets when they came together to establish the securities laws in the 1930s. Among the many terms they used to define a security, they included "bond," "note," "debenture" — you get the picture.

Initially, government bonds were exempt from many of the federal securities laws (outside of antifraud provisions).

Then, things changed. New York City almost went bankrupt in 1974; then-unregulated municipal securities dealers were taking advantage of returning Vietnam War veterans; and Congress brought municipal

securities further under our statutory authority. In the 1980s, there were jitters in Treasury markets. After a dozen firms failed, such as Drysdale Government Securities and E.S.M. Government Securities, parts of the Treasury markets were folded into our remit.

In recent decades, bond markets also have evolved in response to new trends.

First, mortgages, credit cards, and other kinds of debt were bundled into tradable securities. Securitization, which started in the 1980s, really took off in the '90s. It shifted the U.S. debt markets even more from the banking sector to the securities sector.

Second, the fixed income markets increasingly have moved to electronic trading, including on platforms. The platforms, whether interdealer brokers or request-for-quote platforms, have a large and growing share of Treasuries, along with other asset classes. The COVID pandemic has only accelerated these trends.

Finally, a greater share of bond ownership has shifted to registered investment companies, like mutual funds, money market funds, exchange-traded funds, and closed-end funds. This shift raises challenges for financial resiliency.

Given these trends, and the sheer size and importance of the fixed income markets, I think we should focus on how we can make improvements to them. Thus, I will discuss some of the policy work at the SEC with respect to strengthening transparency, modernizing our rule sets for electronified platforms, and enhancing financial resiliency.

To read more:
https://www.sec.gov/news/speech/gensler-names-bond-042622

Number 3

Our Strategy 2022-2025

FCA FINANCIAL CONDUCT AUTHORITY

Consistent topline outcomes	For consumers
Fair value	Consumers receive fair prices and quality
Suitability and treatment	Consumers are sold suitable products and services and receive good treatment
Confidence	Consumers have strong confidence and levels of participation in markets, in particular through (1) minimised harm when firms fail and (2) minimised financial crime
Access	Diverse consumer needs are met through (1) high operational resilience and (2) low exclusion

Consistent topline outcomes	For wholesale markets
Fair value	Market participants are able to make well informed assessments of value and risks due to appropriate transparency
Confidence	Markets are (1) resilient to firm failures and (2) clean with low levels of market abuse, financial crime and regulatory misconduct
Access	Markets are orderly in a variety of conditions so that participants are able to access a diverse range of services with minimised operational disruptions

Reducing and preventing financial crime

Financial crime – including fraud, money laundering, sanction evasion and terrorist financing – does enormous damage to society. It undermines market integrity and consumers' and market participants' confidence.

Criminals often attempt to use or impersonate financial services firms to make and launder money, causing loss to consumers, facilitating other crime and reducing confidence in financial services. Stopping financial crime requires a collective effort – from us, regulated firms, Government, law enforcement and our regulatory partners.
Our aim is to measurably reduce financial crime, and the risk of financial crime. We will continue to closely scrutinise firms at the authorisation

gateway so they meet our standards for financial crime systems and controls before they're authorised.

We will be more proactive in our supervision. Where we detect harm or UK-wide financial crime vulnerabilities, we will continue to share intelligence with our partners to enable a system-wide response.

We will continue to monitor social media for suspicious advertising which may indicate fraud. We will also continue our work to take down illegal advertising quickly and warn consumers through our Warning List and ScamSmart campaigns.

We will supervise cryptoasset firm compliance with the Money Laundering Regulations (MLRs). We will intervene where cryptoasset firms are at risk of being used as conduits for illegal activity and where firms pose harm to consumers or market integrity.

We are increasingly data-led, focusing on the effectiveness of systems and controls so we can:

• detect financial crime faster

• disrupt and pursue firms and individuals

• remove FCA regulated fraudsters from the financial system.

We will publish findings from our data reviews and provide feedback to industry on common issues, so firms can improve their controls.

Finally, we prosecute money laundering and fraud within our remit, pursuing both firms we regulate and firms who are not properly authorised.

We will continue to work closely with our partners – in the UK and internationally – to drive a whole-system response to stopping and preventing financial crime.

As the financial conduct regulator, and supervisor of the professional body supervisors through OPBAS, we have an important role in the implementation of UK-wide economic crime plans.

Over the next two years, we will focus additional efforts on two types of fraud where we can have the greatest impact and see the greatest potential for life-changing harm.

Through our Consumer Investments Strategy, we have committed to enhancing our focus on investment fraud.

We will also enhance our focus on authorised push payment. These efforts go over and above our existing work to stop and prevent fraud.

Ultimately, we want consumers and market participants to have confidence that the financial services industry is safe.

One of the ways we measure success is through reported investment and authorised push payment fraud.

To read more:
https://www.fca.org.uk/publication/corporate/our-strategy-2022-25.pdf

Contents

Number 4

EBA proposes to simplify and improve the macroprudential framework

The European Banking Authority (EBA) published its response to the European Commission's Call for Advice on the review of the macroprudential framework, proposing a set of recommendations to simplify the procedures around some of the existing macroprudential tools and to increase harmonisation for others.

The EU banking system proved resilient during the COVID pandemic and banks continued to provide credit to the real economy. This was partly due to the extraordinary fiscal, monetary and prudential measures, that were put in place and that included a release of macroprudential buffers.

The lessons learnt since the inception of the macroprudential framework, including those gained during the COVID pandemic highlighted the need for some targeted changes to make the macroprudential framework more effective and to improve the functioning of the Single Market.

The EBA's advice includes the following recommendations:

- to rebuild regulatory capital buffers to sufficient levels so that they can be released when needed again in the future;

- to undertake a comprehensive evaluation of the interaction of macroprudential measures with other capital requirements, such as leverage ratio, own funds and eligible liabilities (MREL) requirements;

- to maintain clear roles and responsibilities of the different authorities involved in microprudential and macroprudential policy as well as close coordination between them;

- to include a legal mandate in the Capital Requirements Directive (CRD) to develop methodologies covering both the identification of other systemically important institutions (O-SIIs) and the setting of buffer rates;

- to simplify the text of the CRD and the Capital Requirements Regulation (CRR) around governance procedures for some macroprudential measures;

- to perform further assessments on the ability of current macroprudential tools to address environmental, crypto assets and cyber security risks;

- to establish an oversight and monitoring system for non-bank lenders and enlarge the scope of the macroprudential framework to cover non-bank lenders.

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Other%20publications/2022/1031866/EBA%20advice%20on%20the%20review%20of%20the%20macroprudential%20framework.pdf

Number 5

Joint Committee, Annual Report 2021

In 2021, the Joint Committee under the chairmanship of the ESMA, continued to have a central role for the coordination and exchange of information between the European Supervisory Authorities (ESAs), the European Commission (EC) and the European Systemic Risk Board (ESRB).

The main areas of cross-sectoral focus continued to be joint risk assessment, enhancement of consumer protection, development of the regulatory and supervisory frameworks for sustainable finance and securitisation as well as monitoring and contributing to the development in digital finance, supporting scale up of FinTech through innovation hubs and sandboxes and cyber security.

Joint risk assessment

The Joint Committee issued two Joint Risk Assessment Reports on Risks and Vulnerabilities in the EU Financial System.

The 2021 Spring Joint Risk Report highlighted how the COVID-19 pandemic continued to weigh heavily on short-term recovery prospects, focused on a number of vulnerabilities in the financial markets, and warned of possible further market corrections.

The ESAs also warned of a possible deterioration of asset quality and recommended policy actions for supervisors and regulated institutions, including for banks to ensure sound lending practices and adequate pricing of risks, and to adjust provisioning models to adequately address the impact of the economic shock of the pandemic.

The ESAs also called on competent authorities, financial institutions, and market participants to continue to develop further actions to accommodate a “low-for-long” interest rate environment and its risks.

The 2021 Autumn Joint Risk Report highlighted increasing vulnerabilities in the financial sector, not least because of side effects of the COVID-19 crisis measures, such as increasing debt levels and upward pressure on asset prices.

The Report noted that expectations of inflation and yield growth, as well as increased investor risk-taking, might put additional pressure on the financial system.

Against this context, the ESAs warned of the continued risk of possible asset quality deterioration, potential disorderly increases in yields and sudden reversals of risk premia.

In addition to these economic vulnerabilities, the Joint Risk Report highlighted the increased exposure of the financial sector to cyber risk and information and communication technology (ICT) related vulnerabilities.

The ESAs highlighted the need that appropriate technologies and adequate control frameworks are in place to address threats to information security and business continuity in the financial sector.

Consumer protection and financial education In 2021, consumer protection continued to be a key element in the work of the Joint Committee.

Following the submission of the draft RTS with the proposed amendments to the PRIIPs Delegated Regulation to the European Commission in January 2021 and as part of a wider initiative of the European Commission to develop a new retail investment strategy for the EU, the Joint Committee received in July 2021 from the Commission a Call for Advice on the review of the PRIIPs Regulation.

The scope of the mandate from the European Commission follows the areas referred to in Article 33 of the PRIIPs Regulation, as well as additionally including issues related to the use of digital media.

In order to gather evidence, the Joint Committee published a Call for evidence for a public consultation until 16 December 2021 and is working to deliver its Joint Advice by the end of April 2022.

During 2021, in total 13 administrative sanctions or measures under the PRIIPs Regulation were reported to the ESAs by the competent authorities in 3 Member states (Croatia, Czech Republic and Hungary).

These measures were fines and orders to the PRIIP manufacturer or person advising on, or selling, the PRIIP to remedy specified breaches of the PRIIPs Regulation or the PRIIPs Delegated Regulation.

Furthermore, the Joint Committee finalised its review of the application of the Joint ESAs' Guidelines on complaints-handling that the three ESAs had issued in 2014.

The review concluded that the Joint Guidelines have contributed to a consistent approach to complaints-handling across the banking, insurance and securities sectors and have resulted in better outcomes for consumers.

This review examined how the ESAs Guidelines on complaints-handling have been applied since they came into force.

In particular, the Final Report of the review describes the extent to which the objectives of the Guidelines have been achieved, the supervisory actions that NCAs have undertaken as a result of their national implementation, including the steps taken to identify good/poor practices by firms, as well as the remaining challenges faced.

Finally, the Joint Committee started a new work stream on Financial Education with the aim to fulfil the ESAs' mandate to review and coordinate national financial education initiatives.

The main focus of the Joint Committee work in this area in 2021 was the preparation of a joint high-level conference on financial education and the development of a Joint ESAs repository of national education initiatives focused on fraud, scams and cybersecurity, both of which are scheduled for February 2022.

Sustainability-related disclosures

A very significant part of the work of the Joint Committee in 2021 focused on development of the regulatory and supervisory framework for sustainability-related disclosures.

The Sustainable Finance Disclosure Regulation (SFDR), which has been amended by Article 25 of the Taxonomy Regulation mandated the ESAs to develop through the Joint Committee a number of

Regulatory Technical Standards (RTS). In 2021, the Joint Committee have developed two sets of draft RTS, containing a total of 13 RTS.

Firstly, the ESAs published on 4 February 2021 draft RTS on the content, methodologies and presentation of disclosures under SFDR that aim to strengthen protection for end-investors by providing sustainability disclosures on the principal adverse impacts of investment decisions and on the sustainability features of a wide range of financial products.

This will help to respond to investor demands for sustainable products and reduce the risk of greenwashing.

In addition, the draft RTS contain proposals under Taxonomy Regulation on the do not significantly harm (DNSH) principle.

Secondly, the ESAs have also published on 22 October 2021 draft RTS regarding disclosures under SFDR that relate to financial products investing in economic activities that contribute to environmental objectives.

The draft RTS provide disclosures to end-investors regarding the investments of financial products in environmentally sustainable activities, providing them with comparable information to make informed investment choices and enable a single rulebook for sustainability disclosures under the SFDR and the Taxonomy Regulation.

The draft RTS include pre-contractual and periodic disclosures for products referred to in Articles 5 and 6 of the Taxonomy Regulation that identify the environmental objectives to which the product contributes and show how and to what extent the product's investments are aligned with the EU Taxonomy.

The ESAs have also addressed emerging implementation and supervisory issues. In a letter to the European Commission on 7 January 2021 the ESAs highlighted the priority issues relating to the draft RTS under SFDR.

The European Commission responded in July 2021 and provided interpretative guidance to a number of the questions highlighted in the letter in its response.

In addition, the Joint Committee published on 25 February 2021 a Joint ESAs Supervisory Statement to mitigate the risk of divergent application of SFDR within the period from 10 March 2021 (SFDR application date) to the application date of the SFDR RTS.

The overall objective of the joint supervisory statement is to achieve an effective and consistent application and national supervision of the SFDR, promoting a level playing field and the protection of investors.

The Commission informed the European Parliament and Council in November 2021 that due to the technical complexity of the RTS and the timing of the submission, the bundled February and October RTS would become applicable by 1 January 2023.

Apart from the SFDR related work, through the Joint Committee, the ESAs coordinated their approach with regards to the membership and

governance of the new Sustainability Reporting Pillar of European Financial Reporting Advisory Group (EFRAG).

In the letter in July 2021 the ESAs reiterated their strong commitment to contribute to the development of high-quality sustainability reporting standards, and expressed their preference to remain active observers in the EFRAG governance framework.

The ESAs considered that such an observer status is in line with the proposal for a Corporate Sustainability Reporting Directive (CSRD) to require ESMA, and invite the other ESAs, to provide an opinion on EFRAG's draft sustainability reporting standards.

Securitisation

With a view to support the development of the EU securitisation market, the Joint Committee continued its work to address obstacles in the implementation of the Securitisation Framework and to suggest improvements to the regulatory and supervisory regime to the National Competent Authorities (NCAs) and the European Commission.

In particular, the Joint Committee considered the difficulties to ascertain the jurisdictional scope of application of certain provisions in the Securitisation Regulation in case one or more of the securitisation parties are located in a third country.

In the Joint Opinion issued in March 2021, the ESAs examined the EU securitisation requirements which may be applicable to third-country parties, as well as related compliance aspects of a transaction under the Securitisation Regulation.

The ESAs also set out their common view on the practical difficulties faced by market participants and recommended that these difficulties should be addressed through interpretative guidance from the European Commission.

Furthermore, in the report prepared according to Article 44 of the Securitisation Regulation, the ESAs assessed the implementation and the functioning of the Securitisation Regulation, and provided recommendations on how to address initial inconsistencies and challenges which may affect the overall efficiency of the current securitisation regime.

In particular, the report highlighted specific issues related to transparency and due diligence requirements, criteria for simple, transparent and standardised (STS) securitisation and requirements related to supervision

of securitisation. The report was meant to provide guidance to the European Commission in the context of its review of the functioning of the Securitisation Regulation.

It also includes an analysis of the efficiency of the STS securitisation framework, considering in particular the role that securitisation could play in the economic recovery post the Covid-19 pandemic.

In addition, the Joint Committee provided further guidance on the application of the Securitisation Regulation through Q&As.

These Q&As clarify in particular:

(i) the content and the format of the information of a securitisation transaction that should be disclosed by the originator, sponsor and securitisation special purpose entity (SSPE);

(ii) the transaction documentation of a STS securitisation that should be made publicly available to facilitate investors' compliance with its due diligence requirements; and

(iii) the type of STS certification services that can be provided by Third-party Verifiers to the securitisation parties.

These Q&As were subsequently updated to clarify whether a "vendor financing" structure can be considered a synthetic securitisation.

Finally, the Joint Committee has initiated work to address the Call for Advice from the European Commission in October 2021.

This Call for Advice seeks the Joint Committee's assistance to assess the recent performance of the rules on capital requirements (for banks, and insurance and reinsurance undertakings) and liquidity requirements (for banks) relative to the framework's original objective of contributing to the sound revival of the EU securitisation market on a prudent basis.

The Joint Committee report is scheduled for submission to the European Commission by 1 September 2022.

Digital finance

In 2021 the Joint Committee stepped up its digital finance-related work, including in the context of the European Commission's Digital Finance Strategy, with extensive technical discussions on topics such as crypto-assets and digital operational resilience.

Moreover, the ESAs prepared a comprehensive response to the Call for advice from the European Commission's February 2021 Call for Advice on Digital Finance on value chains, platformisation and new mixed activity groups.

The ESAs have been actively involved in the discussions on the legislative proposals for a regulation on markets in crypto-assets (MiCA) and the regulation on digital operational resilience for the financial sector (DORA).

In particular, apart from considering technical and resource elements relating to operational preparations for the proposed supervision and oversight tasks, the Chairs of the ESAs sent a letter to colegislators, where the ESAs set out their views on how to take forward most efficiently important aspects of the governance and operational processes of the oversight framework for critical third-party service providers and the application of the proportionality principle in the proposed DORA.

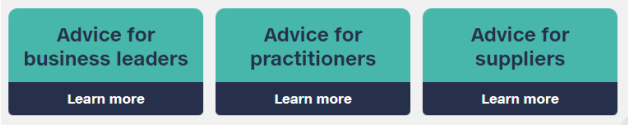
Among other things the ESAs stated that the proposal raised challenges on the practical functioning of the oversight framework, especially the complexity of the governance and decision-making process between the Joint Committee of the ESAs, the Boards of Supervisors of the ESAs and the Oversight Forum.

The report:
https://www.eiopa.europa.eu/document-library/annual-report/joint-committee-annual-report-2021_en

Number 6

Supply Chain Guidance

CPNI
Centre for the Protection of National Infrastructure



Overview

Your supply chain exposes you to damaging security threats. Certain states could target you via your supply chain for their economic, political, or military gain because:

1. Your suppliers have weaker security measures in place so are easier to attack; or

2. One of your suppliers serves various organisations of interest, so targeting that supplier gives them access to several targets via a single attack

Supply chain attacks can result in the compromise of entire organisations and pose a potentially terminal risk to businesses. Hostile actors are looking for vulnerabilities in organisations of every size across a broad range of sectors.

Supply chains are not just compromised by cyber-attacks.

An insider can provide damaging access and insight, or organisations could be unwittingly handing over parts of their business to a state-controlled organisation through offshoring or foreign direct investment in their suppliers.

By giving suppliers access to information without setting expectations about how it should be protected, you are exposing your business to a range of security threats.

Act now to develop your supply chain security, avoid business disruption, and protect your business.

Governance

Implement strong and clear governance that cascades from the top downwards and ensures you are protecting your organisation as much as possible.

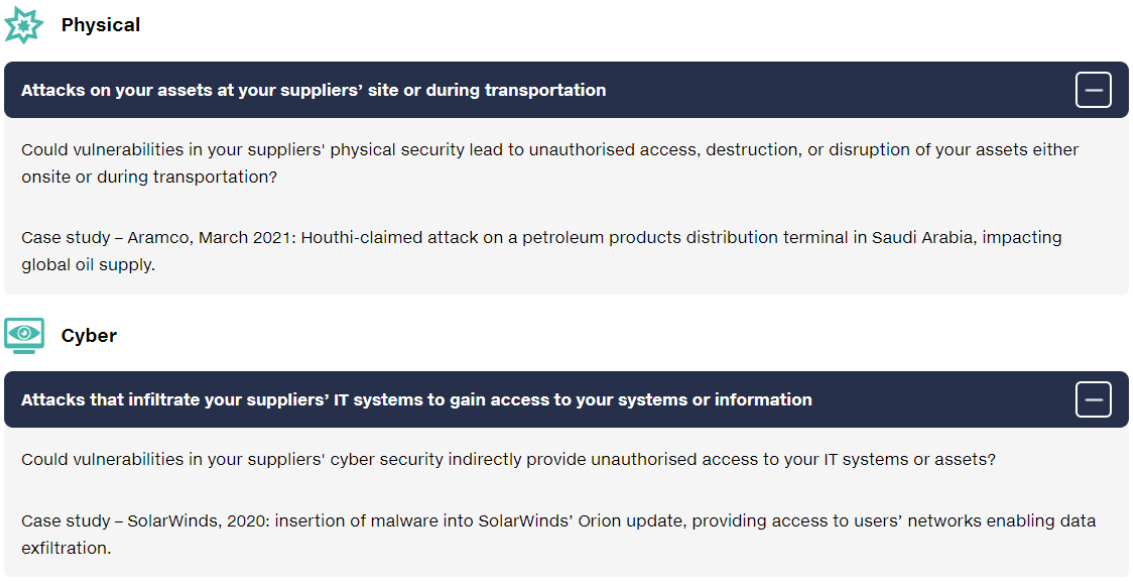
- Appoint a senior lead to take responsibility for supply chain security. Integrate procurement teams into the security management process, alongside those responsible for physical, personnel and information security. Representation from teams with the tools to defend your business from both direct and indirect attacks will ensure you have holistic protection from malicious threats. Ensure supply chain risks are captured on your organisation's risk register

- Ensure senior-level visibility of the security of your procurement processes and supply chain. This should include visibility of high-risk suppliers, and those with access to sensitive information or systems

- Create a clear policy to help staff identify and highlight high-risk suppliers and procurement activities to senior leaders. Regularly review all security policies and procedures with a clearly identified lead to take responsibility for them. Develop a strong security culture across your organisation

Threats

Attacks on your supply chain security can come from a range of sources. Ensure you are aware of the variety of potential attacks.



Insider

Attacks by your suppliers' employees or sub-contractors to gain access to your assets or systems

What access do your suppliers' employees have to your assets, and what level of personnel security checks are in place to detect and disrupt insider threats?

Scenario: Company A holds sensitive commercial data regarding a technology with military and civilian applications. A subcontractor of Company A downloads the data and sells it to competitors in the defence sector of another state.

Geographical

Foreign state access to your information due to the location of your suppliers' business or operations

Do you understand the laws by which suppliers' outside the UK might be bound regarding access and storage of your assets?

Scenario: Company A holds sensitive data in a data centre owned by Company B. Company B decides to relocate the data to a data centre in Country X, which is then able to access that data.

International suppliers' must comply with their home country's laws. Ensure your processes and oversight consider the local legal frameworks in which international organisations operate. This could include laws and regulations that require organisations to share information and data with their state. Take this into account when considering offshoring.

Hostile ownership

Foreign ownership, control, or influence over part of your supply chain

Could suppliers' owned, controlled or influenced by a foreign state lead to unintended exposure of your assets?

Scenario: Law Firm A holds sensitive data as part of due diligence for early stage investment by VC Company B. Law Firm A is purchased by an entity in Country X, offering potential access to that data by Country X.

Technology

Dependencies on technologies with inherent vulnerabilities

Could you be exposing your critical assets by relying on technology with inherent vulnerabilities that could be exploited by hostile actors?

Scenario: a range of sensitive sites procure CCTV equipment with a cloud-based recording capability run from servers in Country X, which requires any company within its jurisdiction to provide access to all data and communications.

Exposure

If a future supplier is compromised, how much damage would they be able to inflict?

- Will they have access to commercially sensitive information that could undermine your commercial success?

- Will they have access to your organisation's IT systems and sensitive information?

- How easily would you be able to detect a compromise of the supplier?

- Would a compromise be easily detected and acted upon, or if unnoticed could it be exploited over a significant period?

Consider how to reduce unnecessary or high-risk sharing of sensitive data or access to sensitive systems.

- Eliminate - If a specific activity you planned to outsource provides suppliers with an unacceptable level of access to business-critical assets, deliver the activity in-house

- Mitigate - If a specific activity you planned to outsource exposes more of your business-critical assets than you are comfortable with, reduce the assets shared to minimise your exposure

- Accept - In some circumstances, businesses may find it difficult to set security expectations for suppliers that dominate the market. You should still embed as much security as possible across your procurement processes

To read more:
https://www.cpni.gov.uk/protected-procurement-business-leaders

Number 7

Government of Jersey publishes first National Risk Assessment of Non-Profit Organisations

Jersey Financial Services Commission

The Government of Jersey has published its first National Risk Assessment (NRA) of Non-Profit Organisations (NPOs). You may visit: https://www.gov.je/SiteCollectionDocuments/Industry%20and%20finance/R%20National%20Risk%20Assessment%20of%20NPOs.pdf

Factors considered in determining an NPOs risk level

Factor 1. Abuse of environmental and jurisdictional aspects
Factor 2. Higher risk rating based on specific activities
Factor 3. Payment remittance methods - Bank accounts
Factor 4. Payment remittance methods – Funds managed outside a bank account
Factor 5. Payment remittance methods - Cash
Factor 6. Use of foreign currency
Factor 7. Transfer risk
Factor 8. Lack of adequate and robust systems and controls
Factor 9. Other key information

This follows the NRA of money laundering published in September 2020 and the NRA of Terrorist Financing published in April 2021.

This latest report concludes that, overall, the non-profit sector in Jersey presents a medium to low risk. However, there is a subsector of around 11% of Jersey's NPOs that present heightened risk and greater vulnerability to terrorist financing abuse and misuse.

These NPOs, being both Registered NPOs and Regulated NPOs, tend to:

- Operate in higher risk jurisdictions, such as conflict zones, failed states and disaster areas where support such as humanitarian aid and disaster relief is desperately needed, and which, equally, are areas where terrorists also tend to undertake activities

- Use partners with the aim to seek to reduce risk, however this practice may also bring additional transfer risk, requiring careful management

- Use different money remittance methods which may render the tracing of funds to legitimate beneficiaries more challenging.

Information provided in the NRA suggests that the sub-section of vulnerable NPOs, in the main, have a high-risk tolerance and a low systems and control environment, rendering them more vulnerable to terrorist financing misuse and abuse.

Since the risk of Proliferation Financing (PF) also benefits from robust systems, controls and displays, as well as similarities in terms of vulnerabilities to those of financing of terrorism misuse and abuse, it is also anticipated that some of the non-profit sector equally presents a higher risk to PF misuse and abuse.

National Risk Assessment (NRA) of Non-Profit Organisations (NPOs), Foreword

Globally, it is recognised that Non-Profit Organisations (“NPOs”), including registered charities, may be exploited to raise and move funds to support terrorist activity.

Jersey is proud to have a thriving and diverse NPO sector and must endeavour to protect it from terrorist exploitation, both as a critical component of the global fight against terrorism as well as to preserve the integrity of the sector and the trust of our donor community.

Some NPOs may be at inherently high risk of being used to facilitate terrorist financing because of where they operate or the nature of the work they carry out.

Others, in fact the vast majority, may represent very little risk.

The Financial Action Task Force recommends that jurisdictions undertake a domestic review of their non-profit sector to identify which are at greater risk. That will allow us to take steps to ensure those organisations are protected from such abuse.

I am therefore pleased to publish Jersey's first National Risk Assessment Report of NPOs.

The assessment shows that the non-profit sector in Jersey presents a medium to low risk and identified that around 11% of non-profit organisations present a heightened risk of being vulnerable to terrorist financing abuse.

To reduce the overall exposure to risk, further work will be completed during 2022 to ensure additional and appropriate safeguards are put in place.

As with all National Risk Assessments, this report is the result of a collaborative effort by multiple agencies.

I am particularly grateful to the Jersey Financial Services Commission and the non-profit sector itself.

It was encouraging to see that responses were received from over 85% of those organisations known to have received the initial questionnaire. This engagement is testament to the commitment and connection of the sector to our Island community.

Senator Ian Gorst
Minister for External Relations & Financial Services

Executive Summary

1 The Terrorist Financing National Risk Assessment (TF NRA) published in April 2021 found that the risk for financial services and NPOs being abused for TF purposes was assessed as Medium-Low.

2 The updated NRA shows that this remains correct when considering the NPO sector holistically, with circa 90% of the assessed sector falling within the Low or Standard risk categories.

3 Of the 170 Regulated NPOs (those NPOs provided with a specified service by a regulated trust company business (TCSP)) 19% fell within the higher risk bracket.

Regulated NPOs are more likely to disburse substantial funds (£1M+) to jurisdictions, territories, or areas at a higher risk of being vulnerable to TF.

They often fund their charitable giving privately by underlying investments. They tend to have broad powers to adjust their Beneficiary base and are not usually registered as charities.

4 Ten Regulated NPOs disbursed between £500,000 and £999,999 outside the Island, whilst 21 Regulated NPOs disbursed in excess of £1M outside Jersey.

5 There are 713 Registered NPOs (those not administered by a TCSP) of which 9% fell within the higher risk bracket. When building in the contingency figures, the number in the higher risk bracket increases to circa 13%.

6 For Registered NPOs the majority of funds collected and disbursed outside Jersey fell within the range of £0 to £19,999, whilst funds raised and disbursed within Jersey ranged from £0 to £499,999. Ten Registered NPOs raised and disbursed funds above this amount with each disbursing in excess of £1M outside the Island.

7 Jersey NPOs that become involved in disaster relief and humanitarian aid work are more likely to be Registered NPOs, working closely with foreign Partners.

Currently, there is no designated TF supervisor for the non-profit sector in Jersey and oversight by third parties is limited.

Registered NPOs are more likely to use alternative money remittance methods, such as Hawala, MoneyGram, mobile money and preloaded cards, as well as cash.

You can read the full report on gov.je:
https://www.gov.je/industry/finance/pages/nationalriskassessmentnpos.aspx

To read more:
https://www.jerseyfsc.org/news-and-events/government-of-jersey-publishes-first-national-risk-assessment-of-non-profit-organisations/

Number 8

FINMA Annual Report

finma

Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Marlene Amstad takes up her duties as Chair of FINMA's Board of Directors. **p. 78**

Regulations implementing FinSA and FinIA come into force. **p. 30, p. 47 ff., p. 83 ff.**

FINMA welcomes small banks to the annual symposium, held in an entirely digital format for the first time. **p. 73**

For the first time, all of the domestic systemically important banks now have credible resolution strategies. **p. 58**

FINMA opens enforcement proceedings against Credit Suisse in connection with the "Archegos" and "Greensill" cases. **p. 39**

JANUARY | **FEBRUARY** | **MARCH** | **APRIL**

Banks around the world suffer large losses as a result of dealings with financial firm Greensill and hedge fund Archegos.

FINMA CEO Mark Branson is appointed President of the Federal Financial Supervisory Authority BaFin in Germany.

FINMA's Takeover and State Liability Committee rejects the appeal against the Swiss Takeover Board's ruling 750/02 regarding Swiss Steel Holding AG. **p. 56**

Established supervisory practice on supplementary health insurance regarding the protection of insured persons from abuse is integrated into a circular. **p. 64**

FINMA enables the scanning of chips embedded in biometric identity documents for the purposes of digital client onboarding. **p. 18**

Specific transparency obligations for climate risks come into force. **p. 28 ff.**

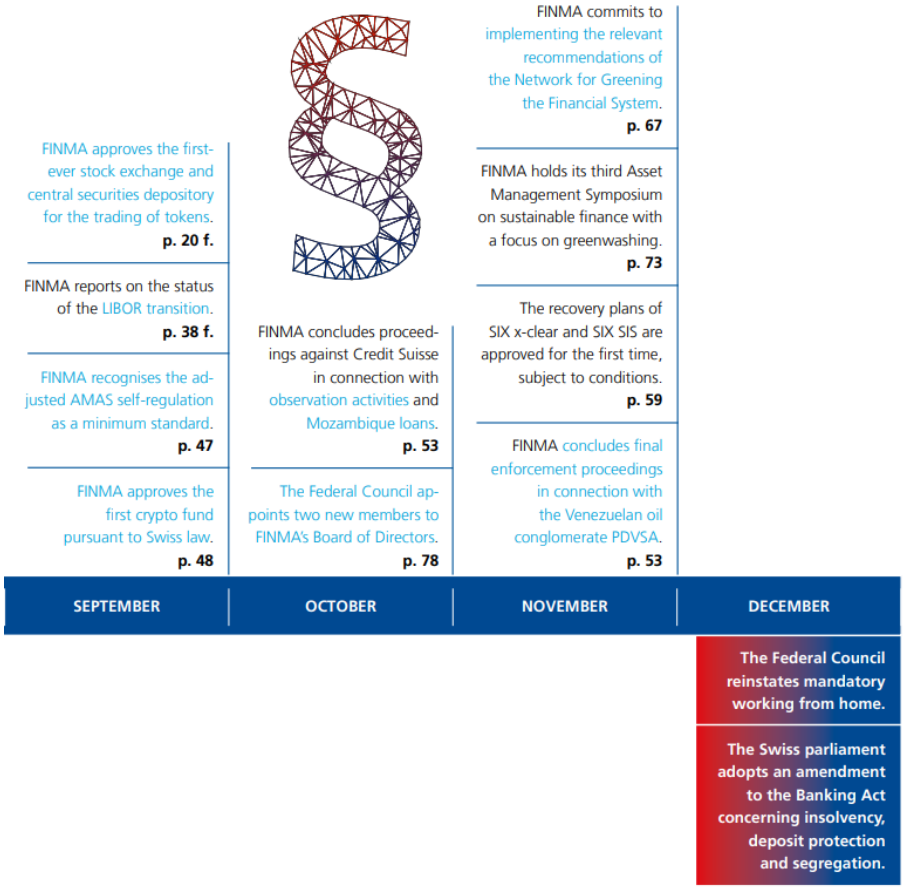
The Federal Council approves the appointment of Urban Angehrn as FINMA's new CEO with effect from 1 November 2021. **p. 80**

MAY | **JUNE** | **JULY** | **AUGUST**

Diem Networks GmbH withdraws its application for authorisation as a payment system in Switzerland, which was at an advanced stage. p. 19

Negotiations commence regarding an agreement on cross-border market access for financial services between the United Kingdom and Switzerland.

The Distributed Ledger Technology Act comes into force.



Market developments and innovation

Regulation

FINMA regulates only when necessary to meet its supervisory goals. It is committed to principles-based and proportional regulation on the basis of a robust regulatory process.

To read more:
https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20220405-finma_jahresbericht_2021.pdf?sc_lang=en&hash=39D0EED3823CAE735B128E31DE0FDAD1

Number 9

The HKMA launches the Regtech Knowledge Hub

HONG KONG MONETARY AUTHORITY
香港金融管理局

The Hong Kong Monetary Authority (HKMA) launched the "Regtech Knowledge Hub" (Hub) to encourage greater sharing of Regtech adoption experience and expertise within the Regtech ecosystem in Hong Kong.

The establishment of the Hub forms part of the HKMA's two-year Regtech promotion roadmap announced in November 2020 to promote Regtech adoption.

The Hub provides an online platform for the Regtech community, including banks and Regtech providers, to share success stories and implementation experience. The Hub's launch is accompanied by three innovative Regtech use cases, featuring:

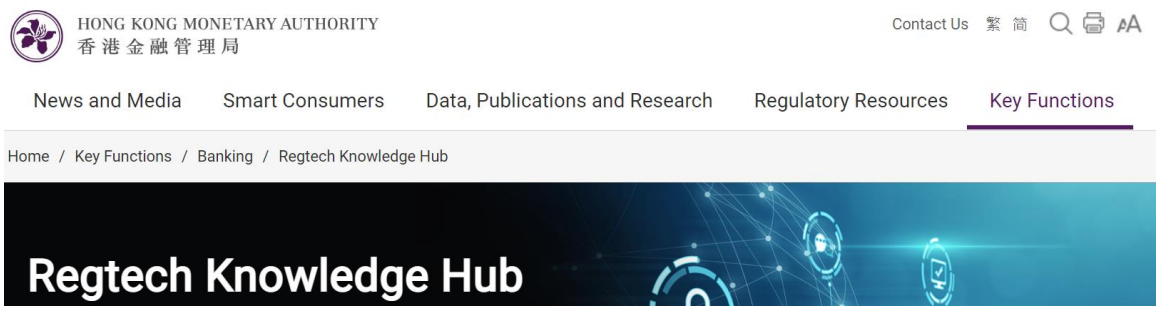
- A Digital Ledger Technology-based foreign exchange (FX) settlement solution that helps to reduce FX settlement risk

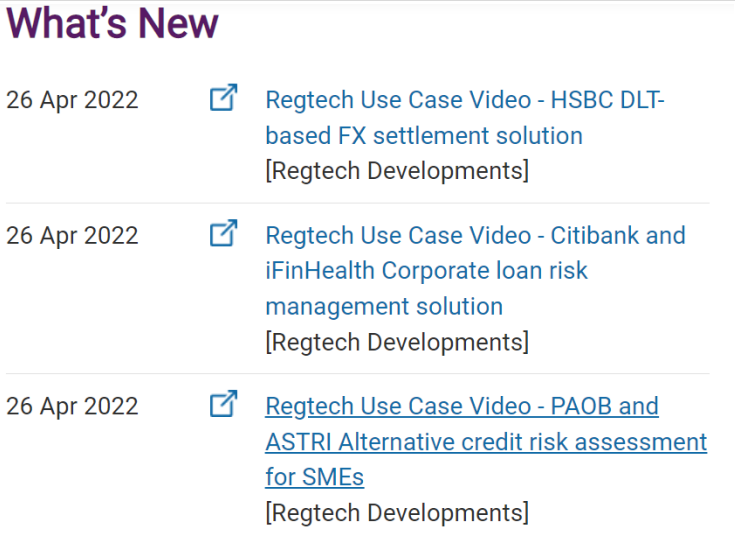
- Alternative credit risk assessment solutions for small and medium-sized enterprises enabled by Application Programming Interface and Federated Learning

- Artificial Intelligence solutions for corporate loan credit risk assessment

Apart from sharing industry use cases, the Hub also acts as a central repository of the HKMA's Regtech-related information, including past circulars, guidance papers, and research reports.

For details, you may visit the Hub at:
https://www.hkma.gov.hk/eng/key-functions/banking/regtech-knowledge-hub/





The Hong Kong Monetary Authority (HKMA) has developed a two-year roadmap to promote Regtech adoption in the Hong Kong banking sector, as laid out in a White Paper entitled "Transforming Risk Management and Compliance: Harnessing the Power of Regtech".

Banks' evolving business models, regulatory initiatives in response, and a challenging external environment continue to drive banks to explore the use of technology to enhance risk management and compliance.

Against this backdrop, the HKMA commissioned an external consultant to explore the current state of Regtech in Hong Kong, examine common practices and barriers to adoption, and outline a roadmap to accelerate adoption in the banking sector.

The HKMA's Regtech roadmap is developed with reference to the recommendations in the white paper. The 16 recommendations span five core areas: -

- boosting awareness by issuing practical guidance and organising targeted events;

- promoting innovation among the local and global Regtech community and facilitating access to infrastructure;

- enhancing regulatory engagement with the Regtech ecosystem through ongoing dialogue and collaboration;

- developing the talent pool by formalising a Regtech training and skills framework; and

- sustaining adoption via continued industry engagement and effective tracking of progress.

To implement the recommendations, the HKMA will roll out a series of events and initiatives in the coming two years, including: -

- hosting a large-scale event to raise the banking sector's awareness of the potential of Regtech;

- launching a Regtech Adoption Index;

- organising a Global Regtech Challenge to stimulate innovation;

- publishing a "Regtech Adoption Practice Guides" series;

- creating a centralised "Regtech Knowledge Hub" to encourage information sharing; and

- establishing a Regtech skills framework to develop talents.

Mr Arthur Yuen, Deputy Chief Executive of the HKMA, said, "The HKMA has been promoting fintech adoption since the announcement of our seven Smart Banking initiatives in 2017. The resulting development in fintech has been phenomenal. We are now putting the same emphasis on Regtech considering its pivotal role in revolutionising risk management and compliance. The banking industry should seize the opportunity to capitalise on the benefits of Regtech. The HKMA's two-year roadmap will help to build a thriving ecosystem, transforming Hong Kong into a Regtech hub."

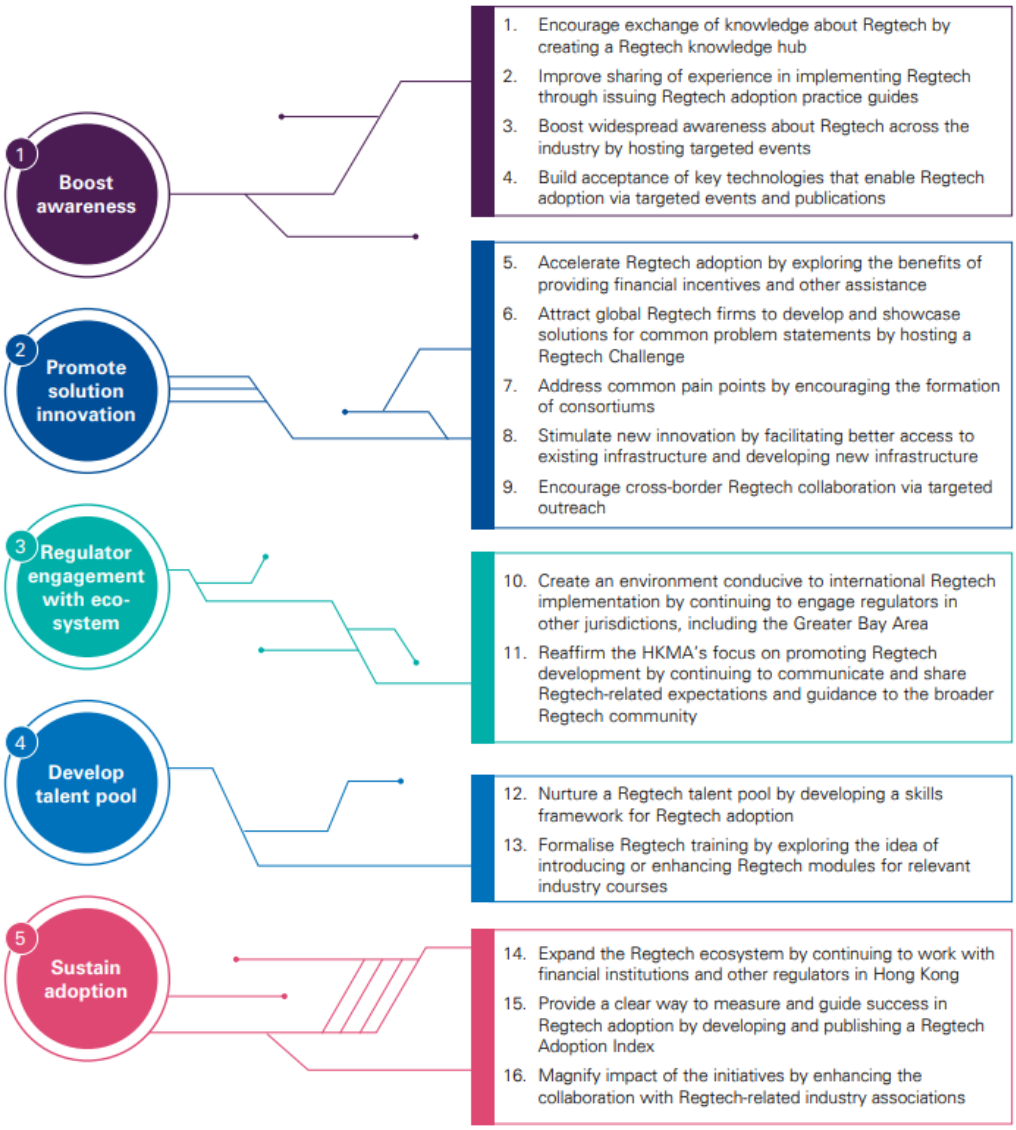
Implementation of the 16 recommendations will reinforce the HKMA's earlier work in promoting Regtech development such as opening up the Fintech Supervisory Sandbox and Chatroom to Regtech projects and ideas in 2018, the "Regtech Watch" newsletter series and the "AML/CFT RegTech Forum" in 2019.

Transforming Risk Management and Compliance: Harnessing the Power of Regtech

HONG KONG MONETARY AUTHORITY
香港金融管理局

KPMG

Figure 1: Overview of recommendations



The paper:
https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2020/20201102e3a1.pdf

To read more:
https://www.hkma.gov.hk/eng/news-and-media/press-releases/2020/11/20201103-3/

Number 10

Final Report - Emission allowances and associated derivatives

esma European Securities and Markets Authority

Executive Summary

Reasons for publication

The European Emission Trading System (ETS) is a key tool of the EU policy against climate change. It puts a price on the CO2 that entities subject to compliance obligations can release to the atmosphere, with the overall objective of reducing net greenhouse gas emissions.

In its Communication on Energy Prices "Tackling rising energy prices: a toolbox for action and support", published on 13 October 2021, the European Commission highlights those questions have emerged around the functioning of the European carbon market.

In order to examine more closely patterns of trading behaviours and the potential need for targeted actions, the Commission asked ESMA for a first preliminary assessment of European carbon markets by 15 November and tasked it to analyse, by early 2022, the trading of emission allowances.

Following the publication of its Preliminary Report on Emission Allowances and derivatives thereof, ESMA is publishing in this report its analysis of the trading of emission allowances.

Content

Following the introduction (Section 2) where ESMA provides a high-level overview of the functioning of primary and secondary emission allowance markets, including the process from the creation of emission allowances until they are surrendered every year by entities subject to compliance obligations under the EU ETS, the report is structured as follows:

Section 3 describes the different mechanisms foreseen in the Market Abuse Regulation (MAR) which aim at identifying and preventing abusive market behaviours.

A description of the follow-up carried out by National Competent Authorities (NCAs) upon identification of alerts for potential market abuse or upon reception of a STOR is also provided.

Section 4 presents ESMA's analysis of the data regarding emission allowances gathered from different sources, including EMIR reporting, MiFIR transaction reporting, MiFID II daily and weekly position reports, auction data and data obtained from the EU Registry.

The analysis focuses in particular on the evolution of carbon prices and its volatility. The data analysis performed by ESMA evidences the specificities and unique characteristics of the EU carbon market, as well as the challenges of having a comprehensive view of this market and an in-depth understanding of its developments.

Overall, ESMA considers that the data analysis has not unearthed any major abnormality or fundamental issue in the functioning of the EU carbon market from a financial supervisory perspective.

The observed evolution of carbon prices and volatility seem to have followed market fundamentals.

In this context, the emergence of new participants (and instruments) with buy-and-hold strategies warrants future monitoring to the extent that they may lead to a reduction in the supply of physical emission allowances available for trading, even though the available evidence suggests that their impact is only limited so far.

When looking at trading on emission allowances and counterparties in this market, the various segments of the EU carbon market appear to broadly function as expected.

The report:
https://www.esma.europa.eu/sites/default/files/library/esma70-445-38_final_report_on_emission_allowances_and_associated_derivatives.pdf

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,

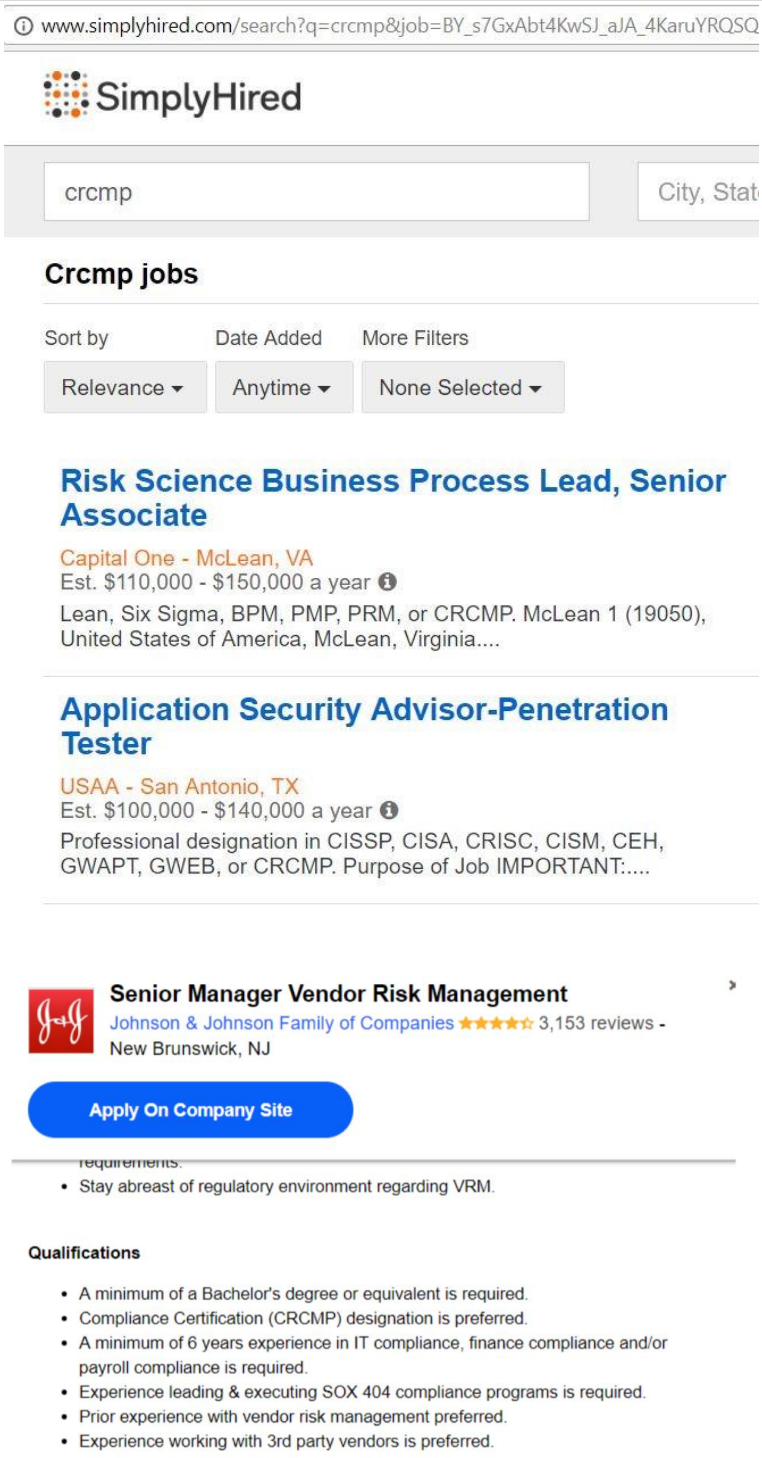
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.