Monday, November 16, 2020

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 have just read an interesting presentation from Fabio Panetta, Member of the Executive Board of the European Central Bank, with title "*The two sides of the (stable)coin"*.

We read: "New providers have progressively shifted their business models from fee-based to data-driven, where payment services are provided free of charge in exchange for personal data that offer deep insights into users' preferences".

I remember whet the Economist magazine has proclaimed a couple of years ago: "The world's most valuable resource is no longer oil, but data." I also remember the paper *"Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes"* (US Senate, Committee on commerce, science and transportation) where we learned:

"(1) *Data brokers collect a huge volume of detailed information on hundreds of millions of consumers*. Information data brokers collect includes consumers' personal characteristics and preferences as well as health and financial information.

Beyond publicly available information such as home addresses and phone numbers, data brokers maintain data as specific as whether consumers view a high volume of YouTube videos, the type of car they drive, ailments they may have such as depression or diabetes, whether they are a hunter, what types of pets they have; or whether they have purchased a particular shampoo product in the last six months;

(2) *Data brokers sell products that identify financially vulnerable consumers*. Some of the respondent companies compile and sell consumer

profiles that define consumers in categories or "score" them, without consumer permission or knowledge of the underlying data.

A number of these products focus on consumers' financial vulnerability, carrying titles such as "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Retiring on Empty: Singles," "Tough Start: Young Single Parents," and "Credit Crunched: City Families."

One company reviewed sells a marketing tool that helps to "identify and more effectively market to under-banked consumers" that the company describes as individuals including "widows" and "consumers with transitory lifestyles, such as military personnel" who annually spend millions on payday loans and other "non-traditional" financial products.

The names, descriptions and characterizations in such products likely appeal to companies that sell high-cost loans and other financially risky products to populations more likely to need quick cash, and the sale and use of these consumer profiles merits close review;

(3) *Data broker products provide information about consumer offline behavior to tailor online outreach by marketers*. While historically, marketers used consumer data to locate consumers to send catalogs and other marketing promotions through the mail, or contact via telephone, increasingly the information data brokers sell marketers about consumers is provided digitally.

Data brokers provide customers digital products that target online outreach to a consumer based on the dossier of offline data collected about the consumer;

(4) *Data brokers operate behind a veil of secrecy*. Data brokers typically amass data without direct interaction with consumers, and a number of the queried brokers perpetuate this secrecy by contractually limiting customers from disclosing their data sources.

Three of the largest companies – Acxiom, Experian, and Epsilon – to date have been similarly secretive with the Committee with respect to their practices, refusing to identify the specific sources of their data or the customers who purchase it.

Further, the respondent companies' voluntary policies vary widely regarding consumer access and correction rights regarding their own data – from virtually no rights to the more fulsome policy reflected in the new access and correction database developed by Acxiom."

Fabio Panetta continued:

"The global technology firms – the so-called big techs – are using this model to leverage their large customer base and expand in global markets.

Thanks to their global footprint, they are uniquely positioned to offer services in the area of global cross-border transactions, where current solutions are low quality and expensive.

This is the backdrop against which stablecoins have emerged. They could be used by the big techs to offer innovative payment solutions that work both within and across national borders.

While stablecoin initiatives are still in their infancy, they should be carefully analysed as they could radically transform the payments landscape."

Montesquieu believed that *in the infancy of societies, the chiefs of state shape its institutions; later the institutions shape the chiefs of state.* If stablecoin initiatives are still in their *infancy*, what is going to happen in the future?

Read more at number 8 below. Welcome to the top 10 list.

Best regards,

George Lekatis

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

Number 1 (Page 6)

Task Force on Climate-related Financial Disclosures, 2020 Status Report

Number 2 (Page 9)

NIST Offers 'Quick-Start' Guide for Its Security and Privacy Safeguards Catalog

Companion to recently updated controls catalog provides useful starting points for risk management.

Number 3 (Page 11)

Implementation of Basel standards - A report to G20 Leaders on implementation of the Basel III regulatory reforms

A report to G20 Leaders on implementation of the Basel III regulatory reforms, November 2020

Number 4 (Page 16)

Post-Implementation Review of AS 3101, The Auditor's Report on an Audit of Financial Statements When the Auditor Expresses an Unqualified Opinion

Number 5 (Page 19)

New Auditor's Report (Updated October 29, 2020)

Number 6 (Page 21)

EU Agency for Cybersecurity launches ISAC in a BOX Toolkit

Number 7 (Page 24)

Payments go (even more) digital

Number 8 (Page 28)

The two sides of the (stable)coin

Fabio Panetta, Member of the Executive Board of the European Central Bank, at Il Salone dei Pagamenti 2020, Frankfurt am Main.

Number 9 (Page 33)

Alert (AA20-302A) - Ransomware Activity Targeting the Healthcare and Public Health Sector

Number 10 (Page 35)

Electromagnetic Spectrum Superiority Strategy Released

Number 1

Task Force on Climate-related Financial Disclosures, 2020 Status Report

In June 2017, the Financial Stability Board's Task Force on Climate-related Financial Disclosures (Task Force or TCFD) released its final recommendations (2017 report), which provide a framework for companies and other organizations to develop more effective climate related financial disclosures through their existing reporting processes.

In its 2017 report, the Task Force emphasized the importance of transparency in pricing risk — including risk related to climate change — to support informed, efficient capital-allocation decisions.

Since the release of its 2017 report and at the request of the Financial Stability Board (FSB), the Task Force has issued two status reports — with this being its third — describing the alignment of companies' reporting with the TCFD recommendations.

In the months between this status report and the 2019 status report, the Task Force has seen significant momentum around adoption of and support for its recommendations. This report describes the progress made to date and highlights the challenges of more consistent and robust implementation.

It is important to view these challenges in the context of the substantial progress made in "mainstreaming" the Task Force's recommendations in the financial markets through investor demand for TCFD disclosures, policy and regulatory actions, and good business practices.

Over the past 15 months, the number of organizations expressing support for the TCFD has grown more than 85%, reaching over 1,500 organizations globally, including over 1,340 companies with a market capitalization of $12.6 trillion and financial institutions responsible for assets of $150 trillion.

Many of these companies have begun to implement the TCFD recommendations or continue to refine and improve their climate-related financial disclosures.

Through the efforts of the World Business Council for Sustainable Development, the Institute for International Finance, the United Nations

Environment Programme Finance Initiative, and other organizations, peer companies implementing the TCFD recommendations have come together to discuss effective climate-related financial disclosure practices and undertake work needed to enhance the effectiveness of such disclosures.

Similar to the growth in the number of organizations supporting the TCFD, investor demand for companies to report information in line with the TCFD recommendations has also grown dramatically.

For example, as part of Climate Action 100+, more than 500 investors with over $47 trillion in assets under management are engaging the world's largest corporate greenhouse gas emitters to strengthen their climate-related disclosures by implementing the TCFD recommendations.

In addition, many large asset managers and asset owners have asked or encouraged investee companies broadly to report in line with the TCFD recommendations and reflected this in their investment practices or policies.

Over 110 regulators and governmental entities from around the world support the TCFD, including the governments of Belgium, Canada, Chile, France, Japan, New Zealand, Sweden, and the United Kingdom.

In addition, central banks and supervisors from across the globe — through the Network for Greening the Financial System — have encouraged companies issuing public debt or equity to disclose in line with the TCFD recommendations.

The Task Force is also seeing governments embed the recommendations in policy and guidance and move toward requiring TCFD disclosures through legislation and regulation.

Table A1

TCFD Recommendations and Supporting Recommended Disclosures

Governance	Strategy	Risk Management	Metrics and Targets
Disclose the company's governance around climate-related risks and opportunities.	Disclose the actual and potential impacts of climate-related risks and opportunities on the company's businesses, strategy, and financial planning where such information is material.	Disclose how the company identifies, assesses, and manages climate-related risks.	Disclose the metrics and targets used to assess and manage relevant climate-related risks and opportunities where such information is material.

Figure A2

TCFD-Aligned Disclosures by Year

Recommendation	Recommended Disclosure	Pt. Change 2017–2019	Percent of Companies That Disclose Information Aligned with TCFD Recommended Disclosures
Governance	a) Board Oversight	8	2017 16% 2018 21% 2019 24%
	b) Management's Role	8	2017 20% 2018 24% 2019 28%
Strategy	a) Risks and Opportunities	1	2017 40% 2018 42% 2019 41%
	b) Impact on Organization	6	2017 29% 2018 32% 2019 35%
	c) Resilience of Strategy	3	2017 4% 2018 5% 2019 7%
Risk Management	a) Risk ID and Assessment Processes	11	2017 14% 2018 19% 2019 25%
	b) Risk Management Processes	9	2017 15% 2018 21% 2019 25%
	c) Integration into Overall Risk Management	9	2017 8% 2018 11% 2019 17%

To read more: https://www.fsb.org/wp-content/uploads/P291020-1.pdf

Number 2

NIST Offers 'Quick-Start' Guide for Its Security and Privacy Safeguards Catalog

Companion to recently updated controls catalog provides useful starting points for risk management.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

If you've ever tried to set up a home entertainment system by poring over a thick manual, you might appreciate the manufacturer also providing you with a quick-start guide so you can get your party going in short order.

Information security experts at the National Institute of Standards and Technology (NIST) have created what is essentially a quick-start guide to their flagship risk management tool, to help organizations reduce their security and privacy risks more easily.

Their creation, whose full title is Control Baselines for Information Systems and Organizations (NIST Special Publication (SP) 800-53B – you may visit: https://csrc.nist.gov/publications/detail/sp/800-53b/final), is a companion publication to SP 800-53 Revision 5 (you may visit: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final), which NIST updated last month after a multiyear effort.

SP 800-53 offers a comprehensive set of security and privacy safeguards — referred to as controls — that address specific weaknesses in an organization or information system. It is used by organizations of all sizes, across public and private sectors. The new companion guide can help them with selecting the baseline, or group of safeguards, that is appropriate for the risk level and threats the organization faces.

"Choosing security and privacy controls is a bit like building a car from parts that fit the driving conditions you expect," said Ron Ross, a NIST Fellow and one of the guide's authors. "If you're building an SUV for trips around town, you might choose different parts than you'd use for a race car. Whether you're managing risk for a routine business system or one whose breach would compromise our nation's critical infrastructure, we've got a baseline for you."

The federal government needs wildly varying levels of cybersecurity as it performs a diverse set of functions for the country, ranging from operating the air traffic control system to conducting financial transactions in the banking system to providing veterans' health care. The 800-53B guide offers low-, moderate- and high-impact security control baselines, and it

also offers a privacy control baseline to protect individual privacy in the processing of personally identifiable information.

“Every system is important in its own right, but some systems support functions that are more critical to the national and economic security interests of the United States, making them more attractive targets for our adversaries,” Ross said. “These systems need higher levels of protection, and NIST provides appropriate safeguarding recommendations for them.”

Ross described the control baselines as starting points for security and privacy. Because every organization will have its own specific goals, the guide also provides tailoring guidance for specific communities of interest, technologies and environments of operation.

“Using the guidance we provide, an organization can choose the right security and privacy baseline and then customize it effectively,” Ross said. “That way they can ensure that they have the capability to protect their critical operations and assets.”

While NIST guidelines are nonregulatory, the Federal Information Security Modernization Act (FISMA) and OMB Circular A-130 require implementation of a minimum set of controls selected from SP 800-53 to protect federal information and information systems. Because many organizations interact with the federal government, Ross said the security and privacy control baselines will have far-reaching effects.

“Many external programs and organizations depend on the NIST recommendations to help protect cloud, health care, financial, transportation, manufacturing, defense and industrial control systems,” he said. “It’s our goal to get all of them the right kind of protection.”

The new control baselines and the security and privacy controls from NIST SP 800-53 Revision 5 can also be used with NIST’s Risk Management Framework, Cybersecurity Framework and Privacy Framework, which together provide a comprehensive toolkit to help manage security and privacy risk. You may visit: https://www.nist.gov/news-events/news/2020/10/nist-offers-quick-start-guide-its-security-and-privacy-safeguards-catalog

Number 3

Implementation of Basel standards - A report to G20 Leaders on implementation of the Basel III regulatory reforms

A report to G20 Leaders on implementation of the Basel III regulatory reforms, November 2020

BIS

This report updates G20 Leaders on progress by the member jurisdictions of the Basel Committee on Banking Supervision (BCBS) in implementing the Basel III regulatory reforms.

It is the 10th such report, and summarises the outcomes of the Committee's Regulatory Consistency Assessment Programme (RCAP).

You can find all the reports at:
https://www.bis.org/bcbs/implementation/impl_moni_g20.htm

The RCAP:

(i) monitors members' progress in adopting the Basel III standards;

(ii) assesses the consistency of domestic (national or regional) banking regulations with the Basel III standards; and

(iii) analyses the prudential outcomes of those regulations.

Overall, further progress has been made since last year in implementing the Basel III standards in a full, timely and consistent manner.

In addition, banks have continued to build capital and liquidity buffers while reducing their leverage.

Prior to the impact of Covid-19, large internationally active banks made further progress towards meeting fully phased-in final Basel III capital requirements, and their liquidity ratios remained stable compared with end-2018.

More recent data, which incorporate the impact of Covid-19, suggest that banks' capital and liquidity ratios have generally remained stable.

The Basel III standards for capital, liquidity and global systemically important banks (G-SIBs) have generally been transposed into domestic regulations within the time frame set by the Basel Committee.

The key components, including the risk-based capital standards and the Liquidity Coverage Ratio (LCR), are now enforced by all member jurisdictions.

Further, most of the member jurisdictions have final rules in place for other Basel III standards, including those relating to the Net Stable Funding Ratio (NSFR), the leverage ratio, the standardised approach for measuring counterparty credit risk (SA-CCR) and the supervisory framework for measuring and controlling large exposures (LEX).

However, final rules for some standards have not yet come into force in some jurisdictions, and many jurisdictions have faced delays in implementing some standards based on the agreed timelines.

In December 2017, the Basel Committee's oversight body, the Group of Governors and Heads of Supervision (GHOS), finalised the Basel III reforms and members reaffirmed their expectation of full, timely and consistent implementation of all elements of the package that includes the following elements:

• a revised standardised approach for credit risk;

• revisions to the internal ratings-based (IRB) approach for credit risk;

• revisions to the credit valuation adjustment (CVA) framework;

• a revised standardised approach for operational risk;

• revisions to the measurement of the leverage ratio and a leverage ratio buffer for G-SIBs; and

• an aggregate output floor, which will ensure that banks' risk-weighted assets (RWA) generated by internal models are no lower than 72.5% of RWA as calculated by the Basel III Framework's standardised approaches.

Banks will also be required to disclose their RWA based on these standardised approaches.

The revised standards were to take effect from 1 January 2022, with the output floor to be phased in over five years.

However, in March 2020 the GHOS endorsed a set of measures to provide additional operational capacity for banks and supervisors to respond to the immediate financial stability priorities resulting from the impact of Covid-19 on the global banking system.

The measures endorsed by the GHOS comprise the following changes to the implementation timeline of the outstanding Basel III standards:

• The implementation date of the Basel III standards finalised in December 2017 has been deferred by one year to 1 January 2023. The accompanying transitional arrangements for the output floor have also been extended by one year to 1 January 2028.

• The implementation date of the revised market risk framework finalised in January 2019 has been deferred by one year to 1 January 2023.

• The implementation date of the revised Pillar 3 disclosure requirements finalised in December 2018 has been deferred by one year to 1 January 2023.

The capital strength of the global banking system will be maintained under the revised timeline and GHOS members unanimously reaffirmed their expectation of full, timely and consistent implementation of all Basel III standards based on this revised timeline.

In order to maximise the benefits of its regulatory post-crisis reforms, the Basel Committee will continue to closely monitor the implementation and evaluate the impact of its standards and regularly report to the G20 on progress.

Regarding the consistency of regulatory implementation, the Committee has published its assessment reports on all 27 members regarding their implementation of the initial risk-based capital standards and LCR.

Further, assessments of implementation of the G-SIB framework were published in June 2016, covering the five jurisdictions that were home to G-SIBs at that time.

These reviews have shown that the domestic regulations are generally consistent with Basel III standards, while further consistency may be achieved in some jurisdictions.

Importantly, most member jurisdictions have actively rectified observed deviations by amending their domestic regulations in the course of the assessment.

In 2018, the Committee started assessing the consistency of implementation of the NSFR and the LEX framework. To date, 10 jurisdictions have been assessed and found to be “compliant” with both standards.

The Committee initially planned to complete its review of the implementation of the NSFR and the LEX framework for all member jurisdictions in 2021.

However, in March 2020 the Committee agreed to postpone all outstanding jurisdictional assessments planned in 2020 under its RCAP in order to commit all the resources that are required to assess and address the banking and supervisory implications of Covid-19.

The Committee has been gradually mapping out a return to resuming its jurisdictional assessments, with a view to completing the outstanding implementation assessments of the NSFR and LEX framework by end-2022 and preparing the implementation assessments of the final Basel III reforms.

Regarding the analysis of regulatory outcomes, the Committee has published five reports on the regulatory consistency of risk-weighted assets (RWAs) in the banking book and in the trading book.

Further, the Basel III monitoring exercises show that, over the past few years, the international banking system has made substantial progress in building capital and liquidity buffers.

As of end-2019, all internationally active banks continue to meet the fully phased-in risk-based minimum capital requirement and the target Common Equity Tier 1 (CET1) capital requirements.

In addition, the Committee is taking forward the evaluation of its Basel III reforms that have been implemented to date.

The evaluation will examine the extent to which Basel III standards have achieved their intended objectives and will incorporate lessons learned from the Covid-19 crisis.

The Committee has also been monitoring the regulatory and supervisory measures taken by its members in response to Covid-19 and related to the Basel Framework, including the use of flexibility and consistency of these measures with Basel III standards.

Overall, most measures taken by members have been capital- or liquidity-related, with the primary objective to support banks' ability to continue lending and providing liquidity to the real economy.

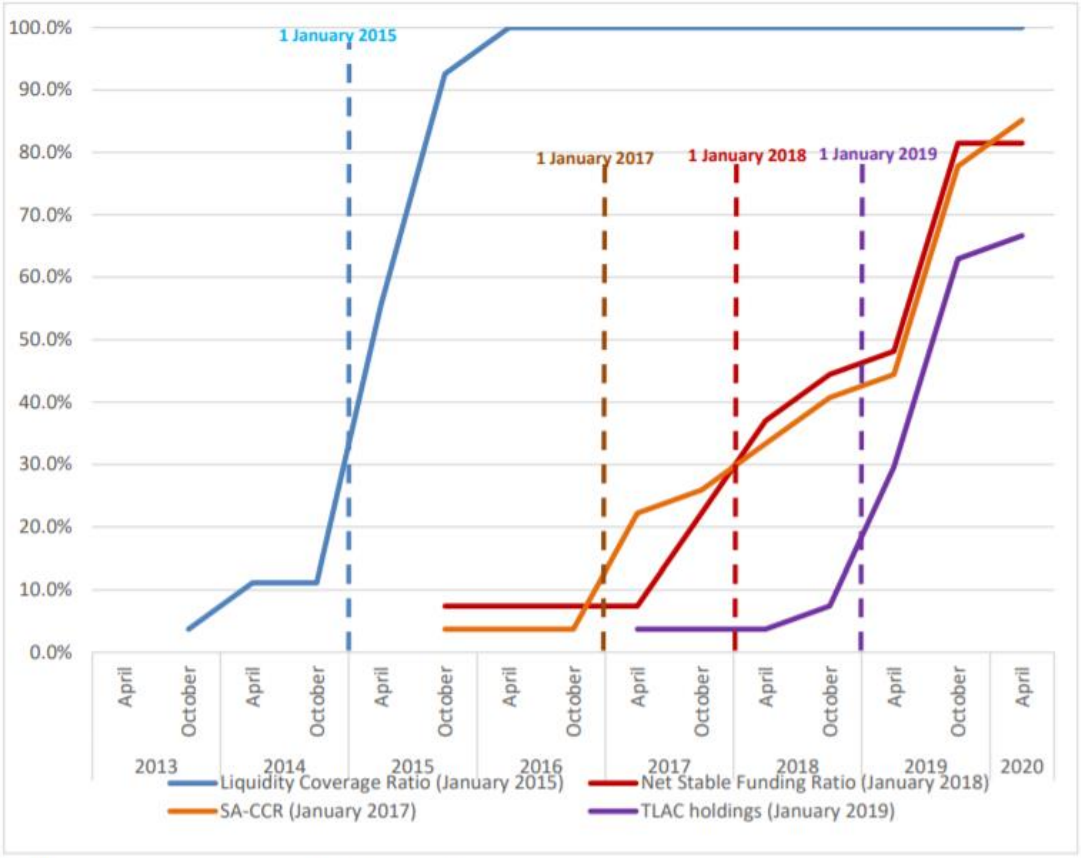
Most measures make use of the flexibility embedded in the Basel Framework, or are otherwise temporary in nature.

The measures are summarised in Section 5 of the present report, which served as an input to the Financial Stability Board (FSB)'s Covid-19 reports to the G20.

Progress in implementing Basel standards

Percentage of Basel Committee member jurisdictions in which the final rules for the standard are in force

Graph 1



The Basel Committee's agreed implementation dates in brackets.

Source: Basel Committee monitoring reports on the adoption of Basel standards, www.bis.org/bcbs/implementation/bprl1.htm; BCBS Secretariat's calculation.

To read more: https://www.bis.org/bcbs/publ/d510.pdf

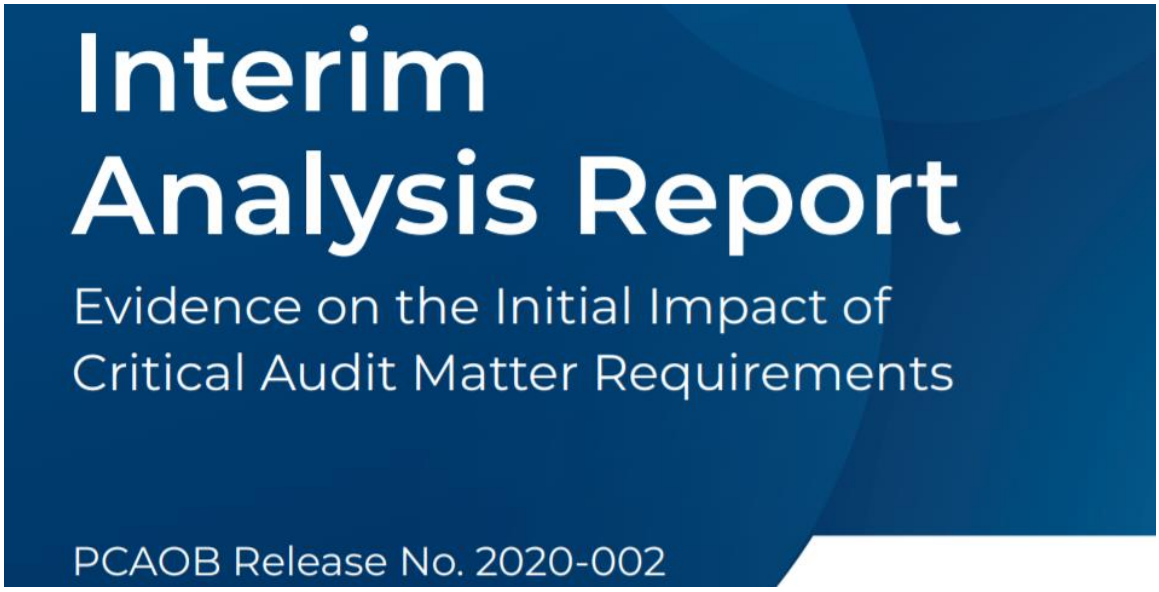
Number 4

Post-Implementation Review of AS 3101, The Auditor's Report on an Audit of Financial Statements When the Auditor Expresses an Unqualified Opinion

PCAOB
Public Company Accounting Oversight Board

The new requirement for auditors to report critical audit matters (CAMs) is the most significant change to the auditor's report in more than 70 years.

The PCAOB is committed to fully understanding the impact of CAM requirements on audit firms, preparers, audit committees, investors, and other financial statement users.



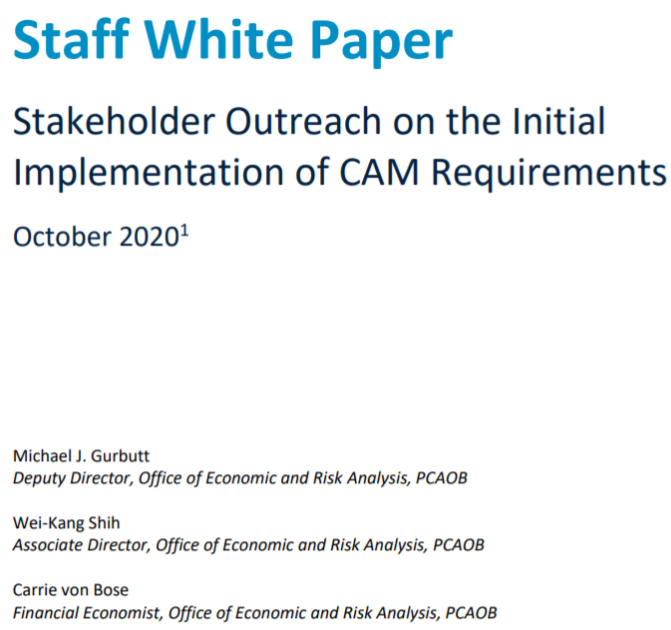
Interim Analysis of Critical Audit Matter Requirements

The PCAOB has released an interim analysis report and two accompanying white papers analyzing the initial impact of the CAM requirements. You may visit:
https://pcaobus.org/EconomicAndRiskAnalysis/pir/Documents/ARM-Interim-Analysis-Report.pdf

The PCAOB has also made available the CAMs dataset used in its analysis.

The interim analysis report and white papers are part of an ongoing evaluation of the overall effect of the CAM requirements on key stakeholders in the audit process.

Staff of the PCAOB's Office of Economic and Risk Analysis conducted extensive stakeholder outreach and performed large-sample statistical analysis. You may visit:
https://pcaobus.org/EconomicAndRiskAnalysis/pir/Documents/Stakeholder-Outreach-Initial-Implementation-CAM-Requirements.pdf



Staff White Paper

Stakeholder Outreach on the Initial Implementation of CAM Requirements

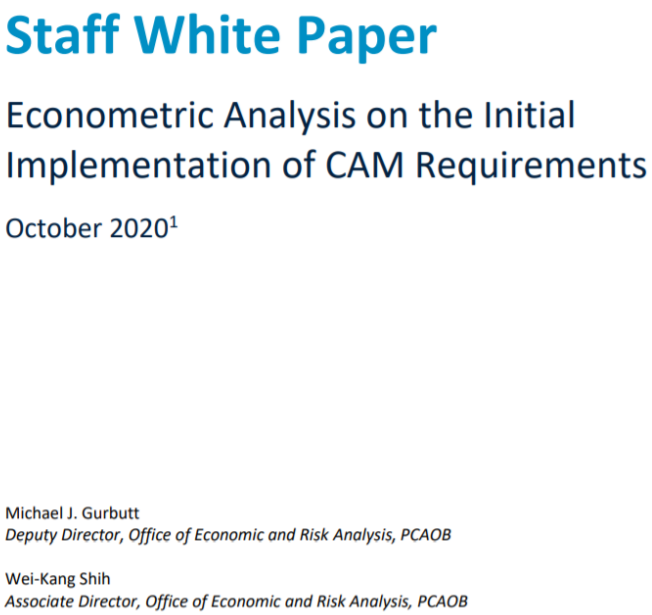
October 2020[1]

Michael J. Gurbutt
Deputy Director, Office of Economic and Risk Analysis, PCAOB

Wei-Kang Shih
Associate Director, Office of Economic and Risk Analysis, PCAOB

Carrie von Bose
Financial Economist, Office of Economic and Risk Analysis, PCAOB

Also:
https://pcaobus.org/EconomicAndRiskAnalysis/pir/Documents/Econometric-Analysis-Initial-Implementation-CAM-Requirements.pdf



Staff White Paper

Econometric Analysis on the Initial Implementation of CAM Requirements

October 2020[1]

Michael J. Gurbutt
Deputy Director, Office of Economic and Risk Analysis, PCAOB

Wei-Kang Shih
Associate Director, Office of Economic and Risk Analysis, PCAOB

Staff of the PCAOB's Office of Economic and Risk Analysis conducted extensive stakeholder outreach and performed large-sample statistical analysis to provide an initial understanding of:

- Audit firm and audit engagement team responses to the CAM requirements.

- Investor use of CAM communications.

- Audit committee and preparer experiences related to CAM implementation.

Key findings from the staff's analyses include the following:

- Audit firms made significant investments to support initial implementation of the CAM requirements.

- Investor awareness of CAMs communicated in the auditor's report is still developing, but some investors are reading CAMs and find the information beneficial.

- The staff has not found evidence of significant unintended consequences from auditors' implementation of the CAM requirements for audits of large accelerated filers in the initial year.

Further information on implementation of the CAM requirements is available in the Standards section of this website. You may visit: https://pcaobus.org/Standards/Implementation-PCAOB-Standards-rules/Pages/new-auditors-report.aspx

Number 5

New Auditor's Report (Updated October 29, 2020)

PCAOB
Public Company Accounting Oversight Board

The new auditing standard retained the pass/fail opinion of the existing auditor's report, but made significant changes to the auditor's report, including:

Communication of critical audit matters—matters communicated or required to be communicated to the audit committee and that:

(1) relate to accounts or disclosures that are material to the financial statements; and

(2) involved especially challenging, subjective, or complex auditor judgment.

Disclosure of auditor tenure—the year in which the auditor began serving consecutively as the company's auditor.

Other improvements to the auditor's report—a statement that the auditor is required to be independent, changes to certain standardized language in the auditor's report, and changes to the standardized form of the auditor's report.

The PCAOB adopted the standard to make the auditor's report more relevant to investors and other financial statement users by requiring more information about the auditor and the audit.

The communication of critical audit matters arising from the audit is intended to inform investors and other financial statement users about matters that required especially challenging, subjective, or complex auditor judgment, and the response that the auditor had to those matters.

Disclosure of auditor tenure in the auditor's report will make this information readily accessible in a timely way for investors who find it useful.

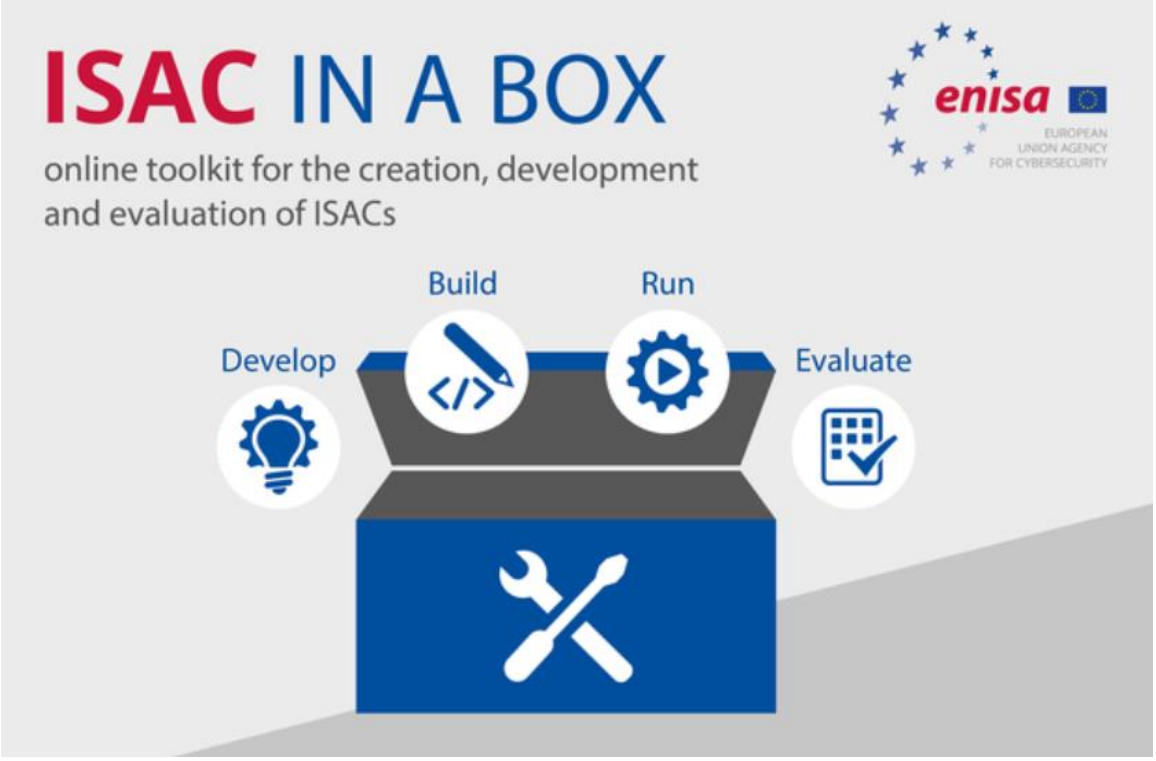
The other improvements to the auditor's report are intended to enhance the user's understanding of the auditor's role and responsibilities related to the audit of the financial statements, make the auditor's report easier to read, and provide a consistent format.

To read more:
https://pcaobus.org/Standards/Implementation-PCAOB-Standards-rules/Pages/new-auditors-report.aspx

Number 6

EU Agency for Cybersecurity launches ISAC in a BOX Toolkit

The EU Agency for Cybersecurity has launched ISAC in a BOX, a comprehensive online toolkit to support the establishment, development and evaluation of Information Sharing and Analysis Centres (ISACs).



European legislation, such as the Cybersecurity Act and the NIS Directive (NISD), promotes the creation of European and National Information Sharing and Analysis Centres (ISACs).

ISACs are private public partnerships (PPPs) between stakeholders exposed to similar cybersecurity vulnerabilities and threats and they are usually formed by private sector initiative, in particular operators of essential services of the critical sectors.

ISACs collect, analyse and disseminate actionable threat information to their members and provide them with tools to mitigate risks and enhance resilience.

ENISA's task is to support the creation and development of ISACs and advise them to strengthen their cooperation, build trust and exchange information using tools and mechanisms that are beneficial for all parties.

ENISA participates and offers advice and expertise in several European initiatives regarding the development of ISACs through:

- Connecting Europe Facilities (CEF) call for ISACs as a technical advisor;
- Inter-EU ISAC platform as a facilitator;
- European Energy (EE) ISAC as a member;
- European Financial (FI) ISAC as secretariat;
- European Maritime (EM) ISAC as a member;
- European Rail (ER) ISAC as a member.

Objective and description of the toolkit

ENISA developed this comprehensive toolkit, following studies on the ISAC concept, to address the need to facilitate community building and collaboration across ISACs.

The toolkit aims at providing practical guidance and the means to empower industry to create new ISACs and to further develop already existing ones.

The main success factors for ISACs are Trust and Sharing. If there is trust, information will be shared and added value will be created - ISAC in a BOX follows the same approach.

It is divided in four phases and contains all activities, documents and tools needed to start, develop and evaluate an ISAC. Each phase includes the basic elements that need to be fulfilled to go to the next phase.

1. Build phase: It's all about setting the goals, participants and purpose for the ISAC; agreeing on the budget and the right cooperation mechanisms.

2. Run phase: Governance is key to share information through meetings and develop trust and building capacities among the ISAC participants.

3. Evaluation phase: Evaluation is an essential part of the ISAC lifecycle which helps to keep it on track, measure its impact and assess its momentum in order to bring it to the next phase.

4. Develop phase: Time for action! This phase focuses on enhancing ISAC's sophistication, its further development and outreach strategies.

To learn more:
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/view

Number 7

Payments go (even more) digital

BIS

- Cash is still in demand, but payments are increasingly shifting to digital instruments.

- Consumers are embracing faster, more efficient and more convenient forms of payment.

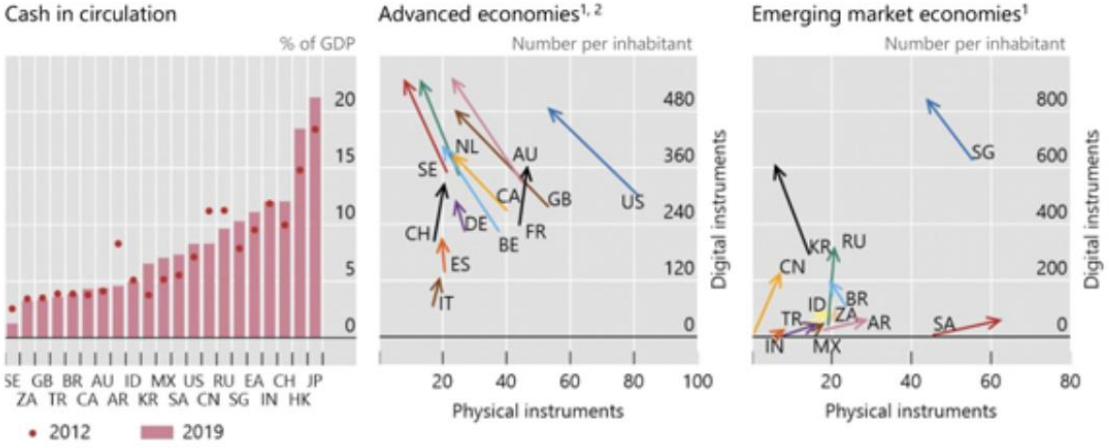
- The number of bank branches and ATMs is decreasing in advanced economies.

The digital revolution is reshaping payments. Consumers are increasingly shifting from physical to digital instruments. The shift is promoting efficient, faster and more convenient payments.

To investigate these trends, this commentary looks at the payments landscape through the lens of the Committee on Payments and Market Infrastructures (CPMI) Red Book statistics.

While digital payments are growing rapidly, cash and, in some jurisdictions, other paper-based payments such as cheques remain important payment instruments.

Cash is still in demand, but payments are shifting to digital instruments — Graph 1



[1] The start (end) of an arrow represents 2012 (2019). Digital instruments include credit transfers, direct debits, card and e-money payments, and other cashless instruments. Physical instruments include paper-based payment instruments (cheques) and cash withdrawals at ATMs (used as a proxy for cash payments). Data not available for HK and JP. [2] For CA, latest data for cash withdrawals at ATMs is for 2017. For ES, the start of the arrow represents 2014. For CH and GB, physical instruments include cheques and total cash withdrawals.

Source: CPMI Red Book.

In more than half of the CPMI jurisdictions, "cash is still king" and its circulation continues to grow (Graph 1, left-hand panel). The largest ratio to GDP is in Japan and Hong Kong SAR (21% and 18% of GDP, respectively).

In contrast, cash has declined by 3 percentage points of GDP in China since 2012. Sweden continues to be the model of a "cash-lite" society, with a cash-to-GDP ratio of 1%. From 2012 to 2019, the period under review, the value of banknotes in circulation relative to GDP increased by 14% while the ratio of coins to GDP fell by roughly 5% across CPMI countries.

In the same time frame, more than half of the CPMI countries have experienced a decline in the use of physical payment instruments and a rise in the use of digital payments (Graph 1, centre and right-hand panels).

The former include both cash (with cash withdrawals at automated teller machines (ATMs) used as a proxy) and cheques, while digital payment instruments include direct debits, credit transfers, and card and e-money payments.

The average number of digital payments in CPMI jurisdictions increased from 176 per inhabitant in 2012 to 303 per inhabitant in 2019.

For advanced economies the use of physical payments declined on average by about 30% in the period under review, while for emerging market economies it continued to grow.

In 2019, the most frequently used digital instruments were card payments, with people in CPMI countries making debit and credit card purchases worth USD 15 trillion a year.

The shift to digital goes beyond debit and credit card payments. Digital technologies allow consumers to use efficient, faster and more convenient payment instruments (Graph 2, left-hand panel).

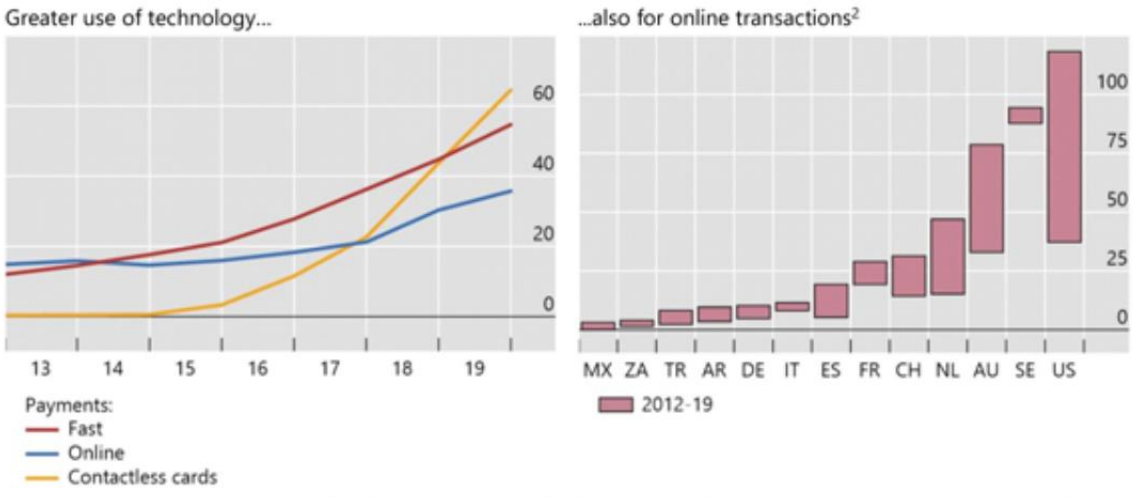
The number of fast payment2 transactions per person continues to increase, as fast payment systems are rolled out in more and more CPMI jurisdictions.

In period under review, payments with contactless cards, and remote (eg card-not-present) payments became more popular.

On average, residents in CPMI jurisdictions made 65 contactless card transactions per person in 2019, which is about three times more than in 2017.

Use of fast, efficient and more convenient forms of payments is increasing[1]

Number per inhabitant Graph 2



[1] CPMI average. Data are not available for all CPMI countries and for all years. [2] Card-not-present transactions. The lower part of the bar represents 2012 value while the upper part of the bar represents 2019 value.

Source: CPMI Red Book.

When it comes to online payments, the divergence in the growth rate is noticeable (right-hand panel).

In countries such as the United States, Sweden and Australia, where e-commerce revenue is more than 1.5% of GDP, residents make more than 75 online payments per person annually.

At the low end are residents in South Africa and Mexico, with fewer than five online payments per year.

New technologies are also shaping the access points to payments.

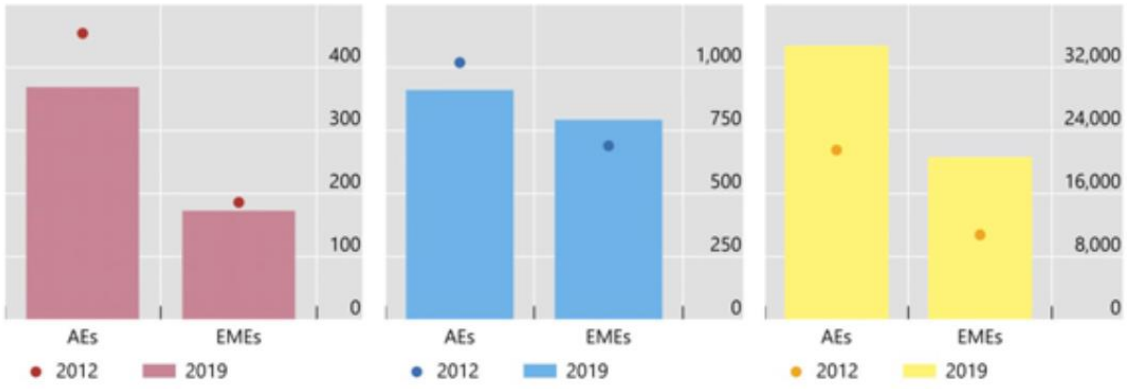
As digital and mobile payments take off, the network of traditional access points becomes less dense, while store tills are substituting for bank branches and ATMs to some extent by allowing customers to deposit/withdraw cash from their bank accounts (as debit card transactions).

Across CPMI jurisdictions, bank branches per million people declined by about 13% in 2012-19 (Graph 3, left-hand panel). A similar decline is seen in the total number of ATMs per million people in CPMI advanced economies (centre panel).

In the same period, the density of point of sale (POS) terminals almost doubled, with 34 POS terminals per thousand people in advanced economies and 20 in emerging market economies (right-hand panel).

Moving away from traditional access points

Number per million inhabitants[1] Graph 3



[1] Average of the respective groups; data are not available for all CPMI countries for all indicators and for all years.

Source: CPMI Red Book.

While the 2020 Red Book data will not be available for some time, the Covid-19 pandemic is likely to accelerate the current trends towards digital payments outlined in this 2019 Red Book data summary.

Several studies have already looked, or are looking, at the impact of the pandemic on payments.

Social distancing, public concerns about the viral transmission from cash, and the surge in e-commerce activity are accelerating the use of digital payments, and may have a structural impact going forward.

Number 8

The two sides of the (stable)coin

Fabio Panetta, Member of the Executive Board of the European Central Bank, at Il Salone dei Pagamenti 2020, Frankfurt am Main.

The payments industry is undergoing a digital transformation, and this transformation is accelerating. We can now pay with cards that are stored in our mobile wallets, ready for a transaction to be initiated at the touch of a button.

Mobile payment apps allow us to easily pay or send money to friends. New services based on application programming interfaces, such as payment initiation services, are expanding consumers' choice of e-commerce payments.

Fintechs have sparked the latest wave of innovation. In a recent survey by the European System of Central Banks, over 200 new payment solutions were reported, of which more than one-third were provided by start-ups.

New providers have progressively shifted their business models from fee-based to data-driven, where payment services are provided free of charge in exchange for personal data that offer deep insights into users' preferences.

The global technology firms – the so-called big techs – are using this model to leverage their large customer base and expand in global markets.

Thanks to their global footprint, they are uniquely positioned to offer services in the area of global cross-border transactions, where current solutions are low quality and expensive.

This is the backdrop against which stablecoins have emerged. They could be used by the big techs to offer innovative payment solutions that work both within and across national borders.

While stablecoin initiatives are still in their infancy, they should be carefully analysed as they could radically transform the payments landscape.

Today, I will discuss the potential advantages and risks of stablecoins, and their implications for the payments market, the financial sector and the overall economy. I will then turn to the forward-looking policies that are needed to steer innovation towards welfare-enhancing outcomes.

Two sides of the same (stable)coin

Stablecoins are digital units of value designed to minimise fluctuations in their price against a reference currency or basket of currencies.

To this end, some stablecoin initiatives pledge to hold a reserve of State-issued currencies or other assets against which stablecoin holdings can be redeemed or exchanged.

Stablecoins became the subject of heated debate last year, after the technology giant Facebook and its partners announced their own global stablecoin, Libra.

Global stablecoins are initiatives which aim to achieve a global footprint, without necessarily relying on existing payment schemes and clearing and settlement arrangements.

For example, Libra is an integrated construct that simultaneously encompasses a new settlement asset, a new payment rail and new end-user solutions.

Global stablecoins could drive further innovation in payments, responding to the need for cross-border payments and remittances that are more efficient and cheaper.

Indeed, the Financial Stability Board has proposed a roadmap to enhance cross-border payments that recognises a role for sound global stablecoin arrangements.

The flip side of stablecoins is the host of risks they can pose to our social and economic life.

For example, data-driven models could pose a risk of misuse of personal information for commercial or other purposes, which could jeopardise privacy and competition and harm vulnerable groups.

Another concern is that wide acceptance of stablecoins offered by foreign companies would make European payments dependent on technologies designed and governed elsewhere.

This could raise potential issues of traceability in the fight against money laundering, terrorist financing and tax evasion.

It could also make the European payment system unfit to support our Single Market and single currency and vulnerable to external disruption, such as cyberattacks.

Risks to financial stability and monetary sovereignty

Other risks involve the monetary and financial system. In fact stablecoins, if widely adopted, could threaten financial stability and monetary sovereignty.

As I mentioned earlier, stablecoin issuers often promise that their stablecoins can be converted into fiat currencies. But this promise generally differs significantly from the convertibility mechanism for bank deposits or e-money.

In the case of bank deposits, one-to-one convertibility to the fiat currency is safeguarded by deposit insurance schemes and prudential regulation and supervision. The value and safety of e-money holdings are protected by the fact that e-money issuers must hold customer funds in custody by third parties.

These safeguards may not apply to stablecoins, which are therefore vulnerable to runs. If the issuer does not guarantee a fixed value, the price of the stablecoin will vary with the value of the reserve assets, and a run could occur whenever users – who bear all the risks – expect a decrease in the redemption price of the stablecoin.

But a run could also occur if issuers do guarantee a fixed value of the stablecoin, if they are perceived as being incapable of absorbing losses. Moreover, the need to cover redemptions could force the stablecoin issuer to liquidate assets, generating contagion effects throughout the entire financial system.

In the case of a global stablecoin, this would affect multiple markets at once.

The payment network of a systemic stablecoin arrangement could also be a source of instability. Stablecoin arrangements are payment systems, insofar as they permit the transfer of value between stablecoin holders.

Moreover, stablecoin arrangements can qualify as a payment scheme.

Just like any other payment system or scheme, if liquidity, settlement, operational and cyber risks are not properly managed, they may threaten the functioning of stablecoin arrangements and lead to systemic instability.

Large investments in safe assets by stablecoin issuers could have implications for monetary policy. By affecting the availability of safe assets, these issuers could influence the level and volatility of real interest rates, with potentially undesirable consequences for financial conditions from a monetary policy perspective.

Market functioning could also be negatively affected. Furthermore, to the extent that stablecoins are used as a store of value, a large shift of bank deposits to stablecoins may influence banks' operations and the transmission of monetary policy.

Extreme scenarios are probably not around the corner. Under current conditions, the reserve assets of the stablecoin issuers would be remunerated negatively, so non-interest-bearing stablecoins would hardly be viable unless they were subsidised by the issuer.

We must nonetheless remain alert to possible developments that may affect how a central bank exercises its core mandate.

Risks would seemingly be mitigated by allowing stablecoin issuers to deposit funds in accounts at the central bank. This would eliminate custody and investment risks for stablecoins and underpin their issuers' commitment to redemption at par value into fiat currencies.

But other fundamental problems would then emerge. In fact, the perceived safety of a private settlement asset – the stablecoin – would come at the risk of relegating other settlement assets, especially public assets, to a minor role.

A large take-up of stablecoins could replace sovereign money – a public good offered for centuries by the State to its citizens – with a "club good", whereby payment services are offered to a select group of people in exchange for platform membership and personal data.

This would not be acceptable. The function of sovereign money reflects citizens' need for safety and their trust in the State.

Central banks offer sovereign money to all citizens, and manage it in the public interest.

Citizens should not have to choose between the convenience of their favourite apps and devices and safety, of which central bank money remains the highest expression. And we should safeguard the sovereignty of public money.

To read more: https://www.bis.org/review/r201104b.pdf

Number 9

Alert (AA20-302A) - Ransomware Activity Targeting the Healthcare and Public Health Sector

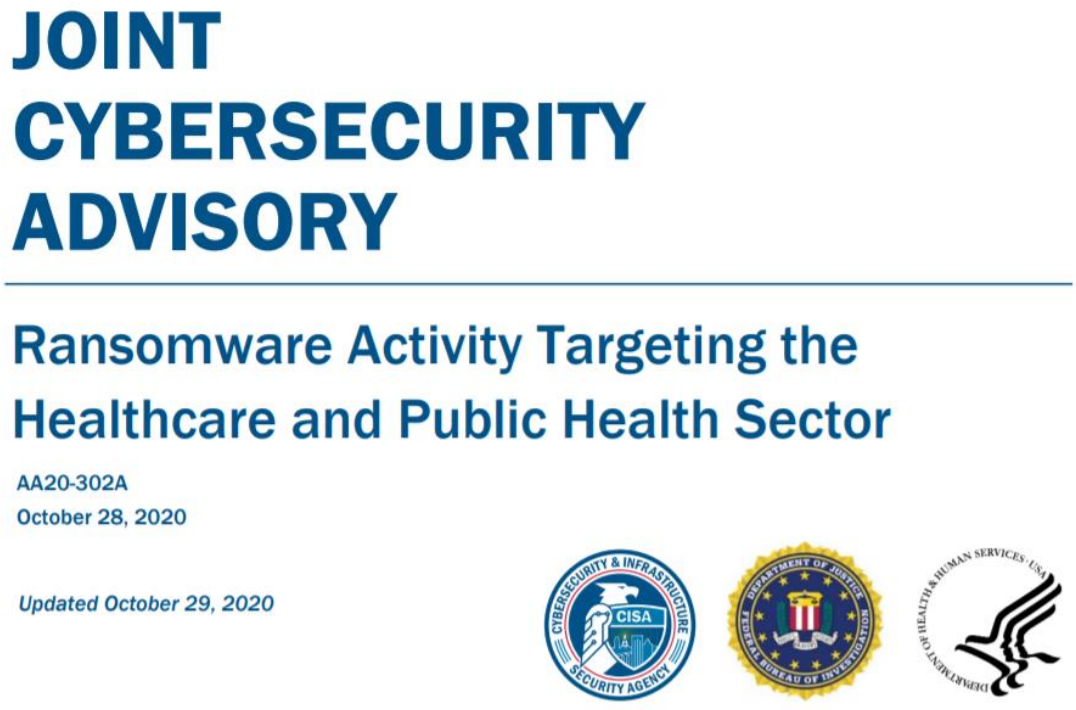
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS).

This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health (HPH) Sector to infect systems with ransomware, notably Ryuk and Conti, for financial gain.

CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.

CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.



To read more: https://us-cert.cisa.gov/ncas/alerts/aa20-302a

https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf

Network Best Practices

- Patch operating systems, software, and firmware as soon as manufacturers release updates.
- Check configurations for every operating system version for HPH organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled.
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Audit logs to ensure new accounts are legitimate.
- Scan for open or listening ports and mediate those that are not needed.
- Identify critical assets such as patient database servers, medical records, and teleheatlh and telework infrastructure; create backups of these systems and house the backups offline from the network.
- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

Number 10

Electromagnetic Spectrum Superiority Strategy Released

The Department is challenged to assure and maintain access, use, fires, and maneuver within the Electromagnetic Spectrum (EMS) at home and abroad.

This jeopardizes the U.S. military's ability to sense, command, control, communicate, test, train, protect, and project force effectively.

Without the capabilities to assert EMS superiority, the nation's economic and national security will be exposed to undue and significant risk.

Adversary actions, commercial development, and regulatory constraints impede U.S. forces' freedom of action in the EMS.

Ensuring such freedom of action will require new ways of thinking about access, sharing, and maneuver in the EMS.

Our adversaries have recognized DoD's reliance on EMS-dependent capabilities and are seeking to exploit this vulnerability.

They seek to restrict U.S. spectrum access through international forums while they organize, train, and equip their forces for EMS advantage.

The Department must also account for the EMS requirements of coalition and commercial partners.

These competing spectrum needs result in an increasingly congested, contested, and constrained electromagnetic operational environment (EMOE).

Combined, these factors require DoD to reexamine how it gains and maintains control of the EMS.

The Department seeks to maintain military overmatch against its adversaries, while sharing the spectrum with commercial partners.

Increased adversary competition and commercial congestion drives the need to develop new capabilities, new techniques, and better integration within DoD and with its partners to enhance spectrum efficiency, maximize spectrum compatibility, and ensure EMS superiority.

The shift in these activities to a sharing and maneuver focus must tightly align with efforts across the EMS enterprise to achieve U.S. military readiness, integration across warfighting domains, and increased lethality of U.S. forces.

Glossary

The terms defined herein are for the purpose of clarity in this document only. Where a more authoritative source definition is used, that source is indicated.

Competition Continuum – Describes a world of enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict.

This is the environment in which the United States applies the instruments of national power (diplomatic, informational, military, economic) to achieve objectives. (JDN 1-19)

Electromagnetic Attack – Division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. [previously Electronic Attack] (JP 3-85)

Electromagnetic Battle Management – The dynamic monitoring, assessing, planning, and directing of operations in the electromagnetic spectrum in support of the commander's concept of operation. Also called EMBM. (JP 3-85)

Electromagnetic Protection – Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. Also called EP. [previously Electronic Protection] (JP 3-85)

Electromagnetic Spectrum (EMS) – The range of all types of electromagnetic radiation. (National Aeronautics and Space Administration (NASA)).

Electromagnetic Spectrum Access – The ability of spectrum-dependent systems to enter the electromagnetic spectrum and occupy a frequency, or band of frequencies, in space and time for the purpose of transmission and/or reception of electromagnetic energy.

Electromagnetic Spectrum-Dependent Systems – All electronic systems, subsystems, devices, and equipment that depend on the use of the spectrum to properly accomplish their functions. (DoDD 3610.01)

Electromagnetic Spectrum Enterprise – The organizing construct consisting of DoD EMS assets, processes, activities and resources required to enable EMS superiority through the conduct of DoD EMSO.

This includes policy, governance, organization, equipment, procedures, doctrine, information, facilities, training, and material responsibilities to ensure that DoD maintains access and control of EMS across the full spectrum of operations. (DoDD 3610.01) 2020 Department of Defense Electromagnetic Spectrum Superiority Strategy 20

Electromagnetic Spectrum Management – The operational, engineering, and administrative procedures to plan, and coordinate operations within the electromagnetic operational environment. [previously Spectrum Management] (JP 3-85)

Electromagnetic Spectrum Maneuver – The movement in three-dimensional positioning, time, and EMS operating parameters (e.g., frequency, power, modulation) to gain an advantage over the enemy. (JP 3-85)

Electromagnetic Spectrum Operations – Coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment. Also called EMSO. (JP 3-85)

Electromagnetic Spectrum Professional – A member of the EMS Workforce who has achieved and maintained a demonstrated standard of expertise in EMS-related core skills.

Electromagnetic Spectrum Sharing – The simultaneous usage of a specific frequency band in a specific geographical area and time by a number of independent entities where harmful electromagnetic interference is mitigated through agreement (i.e., policy, protocol, process.)

Electromagnetic Spectrum Superiority – That degree of control in the electromagnetic spectrum that permits the conduct of operations at a given time and place without prohibitive interference, while affecting the threat's ability to do the same. (JP 3-85)

Electromagnetic Spectrum Workforce – The totality of personnel required to staff the EMS Enterprise.

Electromagnetic Support – Division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. Also called ES. [previously Electronic Warfare Support] (JP 3-85)

Electromagnetic Warfare – Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. [previously Electronic Warfare] (JP 3-85)

To read more:
https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.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.

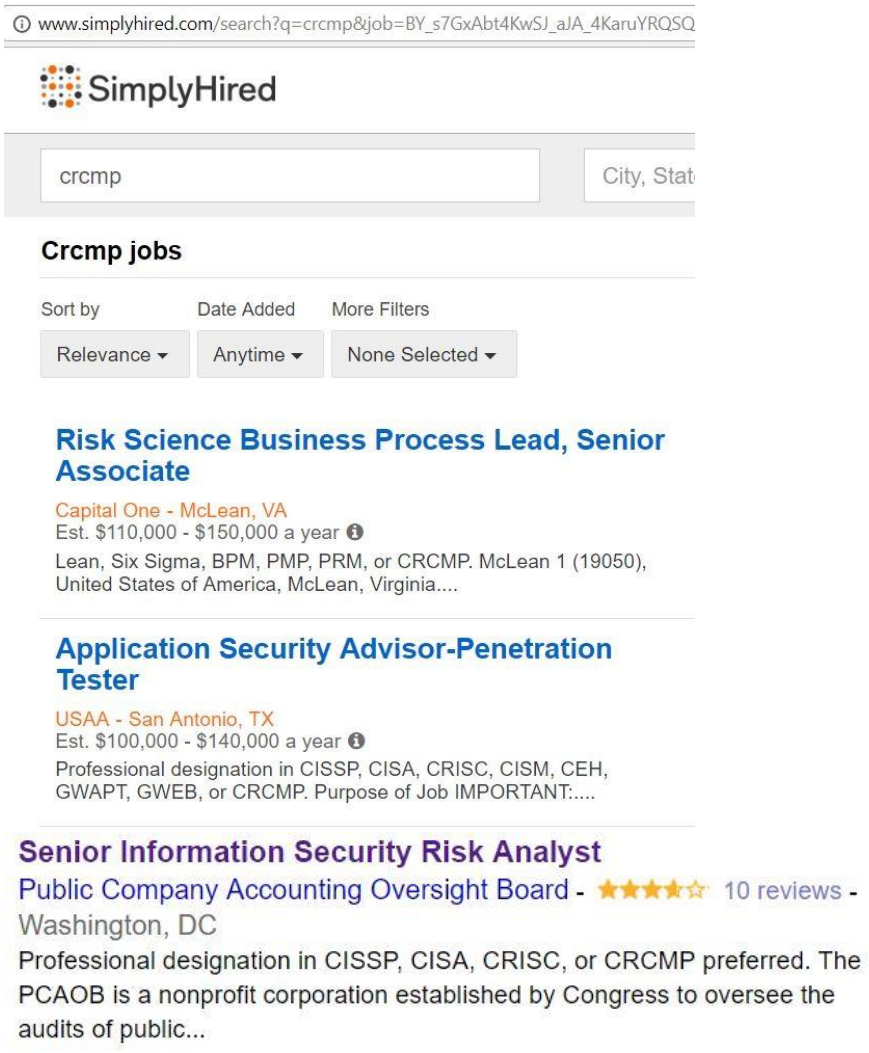
International Association of Risk and Compliance Professionals

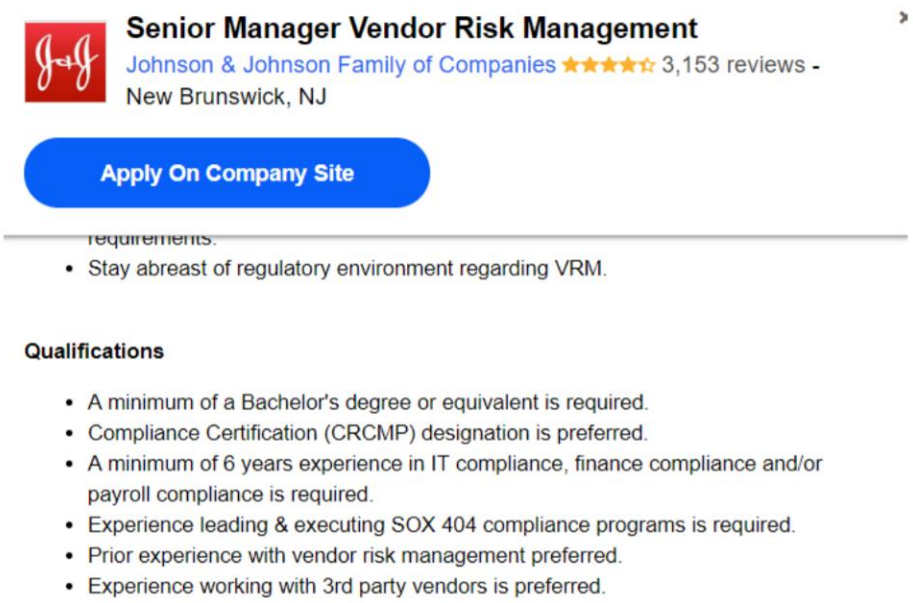
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

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

3. *Training and Certification* – Become a Certified Risk and Compliance Management Professional (CRCMP), a Certified Information Systems Risk and Compliance Professional (CISRCP), a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, and / or a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I.





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

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

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

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

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

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

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

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

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
https://www.risk-compliance-association.com/IARCP_ACT.html

5. *Approved Training and Certification Centers (IARCP-ATCCs)* - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor led training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
https://www.risk-compliance-association.com/Approved_Centers.html