Monday, January 13, 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,

Confucius believed that only the wisest and stupidest of persons never *change*. Today, the use of crypto-currencies is a major development, but is it a wise one too?

According to Napoleon Bonaparte, people are moved by two levers only: *fear* and self-interest. Leonardo da Vinci believed that just as courage imperils life, *fear* protects it. Regulatory bodies have to deal with the *fear,* and to make tough decisions.

According to the Basel Committee, while certain types of crypto-assets are at times referred to as "crypto-currencies", such assets do not reliably provide the standard functions of money and can be unsafe to rely on as a medium of exchange or store of value.

In considering how to specify a prudential treatment for crypto-assets, the Basel Committee has been guided by the following general principles:

1. *Same risk, same activity, same treatment:* A crypto-asset and a 'traditional' asset that are otherwise equivalent in their economic functions and the risks they pose should not be treated differently for prudential purposes.

The prudential framework should not be designed in a way to explicitly advocate or dissuade specific technologies related to crypto-assets, but it should account for any additional risks resulting from the unique features and other factors of cryptoassets relative to traditional assets.

2. *Simplicity:* As noted above, crypto-assets are currently a relatively small asset class globally and are not widely used, but there is the potential for

certain types of crypto-assets to become systemically important. The design of the prudential treatment of crypto-assets should therefore be simple and flexible in nature.

For example, complex internally-modelled approaches should not be used to calculate regulatory requirements. And, where appropriate, the prudential treatment should build on the existing framework, especially for crypto-assets with equivalent economic functions and risks as other asset classes.

In addition, there may be merit in starting with specifying the prudential treatment for the types of crypto-assets that could be considered as 'high-risk' due to their characteristics, some of which have been in existence for several years, while continuing to assess the risk profile and appropriate treatment for other types of cryptoassets based on ongoing developments.

3. *Minimum standards:* Any specified prudential treatment of crypto-assets by the Committee would constitute a minimum standard. Jurisdictions would be free to apply *additional* and/or more conservative measures if warranted. As such, jurisdictions that currently prohibit their banks from having any exposures to crypto-assets would be deemed compliant with any potential global prudential standard.

I remember what Alan Greenspan believed: "I do not understand where the backing of Bitcoin is coming from. There is no fundamental issue of capabilities of repaying it in anything which is universally acceptable, which is either intrinsic value of the currency or the credit or trust of the individual who is issuing the money, whether it's a government or an individual."

Read more at number 1 and 2 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com

Number 1 (Page 6)

Designing a prudential treatment for crypto-assets

BIS

The past few years have seen rapid growth in crypto-assets. The estimated market capitalisation of cryptoassets reached a historical peak exceeding $800 billion in January 2018.

While the crypto-asset market remains small relative to the size of the global financial system, and banks' exposures to crypto-assets are currently limited, its absolute size is meaningful and there continues to be rapid developments, with increased attention from a broad range of stakeholders.

Number 2 (Page 8)

US regulations and approaches to cryptocurrencies

Michael Held, Executive Vice President of the Legal Group of the Federal Reserve Bank of New York, at the BIS Central Bank Legal Experts' Meeting, Basel.

"Policy makers and regulators in the United States, to date, have not developed an overarching framework for regulating private digital currencies."

Number 3 (Page 10)

Critical Audit Matters Spotlight

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.

To support the implementation of the new requirement, the Public Company Accounting Oversight Board (PCAOB) has conducted extensive outreach to audit firms and other stakeholders as well as issued guidance and other resource tools.

Number 4 (Page 11)

EIOPA consults on guidelines on Information and Communication Technology security and governance

The European Insurance and Occupational Pension Authority (EIOPA) has launched a consultation on guidelines on Information and Communication Technology (ICT) security and governance.

Number 5 (Page 13)

European Commission publishes EU Cybersecurity Taxonomy

On 12 September 2018, the Commission has proposed a Regulation setting up a European Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres (COM/2018/630). The overall mission of the Competence Centre and the Network (CCCN) is to help the Union retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market.

Number 6 (Page 15)

Helping to Protect the 2020 US Census

Kevin Martin, VP of US Public Policy, and Samidh Chakrabarti, Director of Product Management, Civic Engagement

Next year, all US households will be able to complete the US census online for the first time. As the format of the census evolves, so do the ways that people share information about the census. This means we have to be more vigilant about protecting against census interference across posts and ads on Facebook and Instagram and help promote an accurate count of every person in the country.

Number 7 (Page 19)

Warnings about compromised passwords

Google Security Blog

Google first introduced password breach warnings as a Password Checkup extension early this year. It compares passwords and usernames against over 4 billion credentials that Google knows to have been compromised.

Number 8 (Page 22)

EIOPA publishes annual report on the use of capital add-ons under Solvency II

eiopa
European Insurance and Occupational Pensions Authority

The European Insurance and Occupational Pensions Authority (EIOPA) published today its annual report on the use of capital add-ons by national competent authorities (NCAs) under Solvency II.

Number 9 (Page 24)

Fake 'free giveaway' websites

National Cyber Security Centre

Cyber security researchers have uncovered a fake 'free giveaway' website that tricks users into revealing their login credentials.

Cyber criminals posted links to a phishing website in the comments section of the legitimate Steam website, encouraging users to visit a convincing – but fake – page that contained free downloadable content for the platform.

Number 10 (Page 25)

NIST Releases Data to Help Measure Accuracy of Biometric Identification

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

New biometric research data — ranging from fingerprints to facial photographs and iris scans — is now available from the National Institute of Standards and Technology (NIST).

Number 1

Designing a prudential treatment for crypto-assets

BIS

The past few years have seen rapid growth in crypto-assets. The estimated market capitalisation of cryptoassets reached a historical peak exceeding $800 billion in January 2018.

While the crypto-asset market remains small relative to the size of the global financial system, and banks' exposures to crypto-assets are currently limited, its absolute size is meaningful and there continues to be rapid developments, with increased attention from a broad range of stakeholders.

As previously indicated, the Committee is of the view that the growth of crypto-assets and related services has the potential to raise financial stability concerns and increase risks faced by banks.

Cryptoassets are an immature asset class given the lack of standardisation and constant evolution. Certain cryptoassets have exhibited a high degree of volatility, and present risks for banks, including liquidity risk; credit risk; market risk; operational risk (including fraud and cyber risks); money laundering and terrorist financing risk; and legal and reputation risks.

While certain types of crypto-assets are at times referred to as "crypto-currencies", the Committee is of the view that such assets do not reliably provide the standard functions of money and can be unsafe to rely on as a medium of exchange or store of value.

These types of crypto-assets are not legal tender, and are not backed by any government or public authority. Therefore, if banks are authorised, and decide, to acquire crypto-assets or provide related services, the Committee is of the view that banks should apply a conservative prudential treatment to such exposures, especially for high-risk crypto-assets.

To that end, the Committee is publishing this discussion paper to seek the views of stakeholders on a range of issues related to the prudential regulatory treatment of crypto-assets, including:

(i) the features and risk characteristics of crypto-assets that should inform the design of a prudential treatment for banks' crypto-asset exposures; and

(ii) general principles and considerations to guide the design of a prudential treatment of banks' exposures to crypto-assets, including an illustrative

example of potential capital and liquidity requirements for exposures to high-risk crypto-assets.

There have been recent initiatives related to some types of crypto-assets. For example, some initiatives seek to reduce the volatility exhibited to date by anchoring crypto-assets to a reference asset.

Other initiatives include redemption or repurchase assurances by a legal entity. These crypto-assets are sometimes referred to as 'stablecoins', although the stability of such assets has yet to be tested completely.

The scope of stablecoin initiatives vary, with some focusing on intragroup or interbank payment systems, while others seek to target a broader audience, including consumers globally.

While many of these types of crypto-assets have yet to become operational in practice, some may have the potential to become systemically important.

The Committee is of the view that these types of crypto-assets warrant further assessment and elaboration before specifying a prudential treatment.

A separate initiative relates to central bank digital currencies, where many central banks are continuing to look at the implications of this potential type of central bank money.

Such forms of digital currencies are outside the scope of this discussion paper. The responses to this paper will inform the Committee's development of a prudential treatment for crypto-assets at large, including for crypto-assets that are issued by regulated financial institutions, or that make use of stabilisation tools.

The Committee is continuing to assess the appropriate prudential treatment for such types of crypto-assets, and will consult on any specific measures.

To read more: https://www.bis.org/bcbs/publl/d490.pdf

Number 2

US regulations and approaches to cryptocurrencies

Michael Held, Executive Vice President of the Legal Group of the Federal Reserve Bank of New York, at the BIS Central Bank Legal Experts' Meeting, Basel.

Thank you, Diego, for "volunteering" me to speak about digital currencies — a field in which I count myself as very much a trainee, not an expert. Today I will focus on the U.S. regulatory landscape for digital currencies, in particular on digital currencies issued by private organizations that are intended to be used like money.

As always, the views I express are my own, not necessarily those of the Federal Reserve Bank of New York or the Federal Reserve System.

Policy makers and regulators in the United States, to date, have not developed an overarching framework for regulating private digital currencies.

The field has been seen as too new for a comprehensive regulatory response. To be sure, the digital nature of new private currencies will raise challenges to which policy makers must respond.

In my view, however, we spend so much time wrestling with the novelty of digital currencies that we forget that private currency is nothing new.

The theme of my talk today is accordingly best encapsulated by a quote that is attributed—perhaps wrongly—to Mark Twain: "History may not repeat itself, but it does rhyme."

The Past Is Not Dead. It Isn't Even Past

So, let's take a little walk through the history of privately-issued currency. We begin in Michigan in 1837, when the state legislature passed the first "free" banking law in the United States.

Upon commencing business, free banks could issue banknotes—that is, private currencies—that were redeemable in specie—gold or silver.

These banknotes were transferable debt backed by the general creditworthiness of the bank that issued them, plus assets like bonds and mortgages on real estate, and for a brief time, personal guarantees.

The statute permitted bank organizers to establish a bank by filing an application with the local county treasurer and county clerk. They did not need approval from the state banking commissioner. (At the time, the United States had no federal banking supervisor. Indeed, the "free banking" era generally begins with Congress's failure to recommission the Second Bank of the United States before its charter expired in 1836, and ends with the passage of the National Bank Act in 1863).

The result, predictably, was chaotic. The state banking commissioner was unsure of how many banks had even been established.

Some banks in Michigan were established with the intent to issue banknotes but without the intent to ever redeem them.

By 1839 almost the entire system had collapsed. After closing down one bank in Michigan, the commissioner found shards of window glass, lead, and nails where he should have found gold and silver coin.

Some of these free banks became known as "wildcat" banks. They set up offices in remote areas—where only the wildcats roamed—making it difficult to redeem notes for specie.

To read more: https://www.bis.org/review/r191212d.pdf

Number 3

Critical Audit Matters Spotlight

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.

To support the implementation of the new requirement, the Public Company Accounting Oversight Board (PCAOB) has conducted extensive outreach to audit firms and other stakeholders as well as issued guidance and other resource tools.

In 2019, we selected 12 audits of large accelerated filers with fiscal years ending on or after June 30, 2019, to specifically review how auditors of these filers implemented the CAM requirements.

This Spotlight focuses on observations from our inspections of these new requirements and from our outreach and data analysis activities.

To read more: https://pcaobus.org/Documents/CAMs-Spotlight.pdf

PCAOB
Public Company Accounting Oversight Board

Critical Audit Matters
SPOTLIGHT

Number 4

EIOPA consults on guidelines on Information and Communication Technology security and governance

The European Insurance and Occupational Pension Authority (EIOPA) has launched a consultation on guidelines on Information and Communication Technology (ICT) security and governance.

These guidelines shall provide guidance to national supervisory authorities and market participants on how regulation regarding operational risks set forth in Directive 2009/138/EC and in the Commission's Delegated Regulation 2015/35 and EIOPA Guidance set out in EIOPA's Guidelines on System of Governance is applied in the case of ICT security and governance. The consultation is open until Friday, 13 March 2020.

In line with its Joint ESA's Advice and in reply to the European Commission's FinTech Action Plan, EIOPA developed these guidelines addressed to national supervisory authorities with the following objectives:

- To create a common baseline for information security throughout the EU Member States

- To enhance convergence of supervisory practices in this area

In developing the Joint Advice, the ESAs' objective was that every relevant entity should be subject to clear and general requirements on governance of ICT, including cybersecurity, to ensure the safe provision of regulated services.

As these requirements are not in general 'sector-specific for the (re)insurance market, EIOPA also considered the most recent guidelines published by the European Banking Authority

EIOPA's Guidelines cover the following areas:

- Governance and risk management
- ICT operations security
- ICT operations management

For responding to this consultation you may visit:
https://ec.europa.eu/eusurvey/runner/ICT_GLs

The deadline for submission of feedback is Friday, 13 March 2020 at 23.59 hrs CET.

Unless requested otherwise, all contributions received will be published after the deadline for submission.

To read more:
https://eiopa.europa.eu/Publications/Consultations/guidelines_ICT_security_and_governance_12122019_for_consultation.pdf

Number 5

European Commission publishes EU Cybersecurity Taxonomy

On 12 September 2018, the Commission has proposed a Regulation setting up a European Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres (COM/2018/630).

The overall mission of the Competence Centre and the Network (CCCN) is to help the Union retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market.

This goes hand-in-hand with the key objective to increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other European industries.

One of the first steps during the Impact Assessment of the Proposed Regulation was to provide a clear definition of the cybersecurity context, its domains of application, research and knowledge.

In this context, the first version of the proposed taxonomy was published with the goal of aligning the cybersecurity terminologies, definitions and domains.

The taxonomy was then used for the categorisation and mapping of existing EU cybersecurity centres (e.g. research organisations, laboratories, associations, academic institutions, groups, operational centres, etc.) according to their cybersecurity expertise in specific domains.

Based on this first analysis, a survey was also conducted where more than 600 institutions participated and registered their cybersecurity expertise.

In order to assess essential aspects of the CCCN regulation proposal, the Commission launched a pilot phase under Horizon 2020. In particular, the proposals CONCORDIA, ECHO, SPARTA and CyberSec Europe were selected as the four pilot projects to assist the EU in the establishment of a European Cybersecurity Competence Network of cybersecurity centres of

excellence. The pilots bring together more than 160 partners, including big companies, SMEs, universities and cybersecurity research institutes, from 26 EU Member States.

The four pilot projects were asked to review the proposed taxonomy and provided feedback, which was used to improve the first version of the taxonomy in order to publish this second enhanced version.

For the purpose of this document, cybersecurity is considered an interdisciplinary domain. This starting point finds support in the Cybersecurity Report issued by the High Level Advisory Group of the EC Scientific Advice Mechanism in March 2017, where it is stated clearly that:

"cybersecurity is not a clearly demarcated field of academic study that lends itself readily to scientific investigation. Rather, cybersecurity combines a multiplicity of disciplines from the technical to behavioural and cultural. Scientific study is further complicated by the rapidly evolving nature of threats, the difficulty to undertake controlled experiments and the pace of technical change and innovation. In short, cybersecurity is much more than a science".

To read more:
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

Number 6

Helping to Protect the 2020 US Census

Kevin Martin, VP of US Public Policy, and Samidh Chakrabarti, Director of Product Management, Civic Engagement

Next year, all US households will be able to complete the US census online for the first time. As the format of the census evolves, so do the ways that people share information about the census.

This means we have to be more vigilant about protecting against census interference across posts and ads on Facebook and Instagram and help promote an accurate count of every person in the country.

Today, we are announcing a new census interference policy that bans misleading information about when and how to participate in the census and the consequences of participating.

We are also introducing a new advertising policy that prohibits ads that portray census participation as useless or meaningless or advise people not to participate in the census.

These policies are due in large part to the work being done with the civil rights community through our civil rights audit and represent the culmination of a months-long process between Facebook, the US Census Bureau and experts with diverse backgrounds to develop thoughtful rules around prohibiting census interference on our platforms and making sure people can use their voice to be counted.

Updating Our Community Standards to Ban Census Interference

Our census interference policy will prohibit:

- Misrepresentation of the dates, locations, times and methods for census participation;

- Misrepresentation of who can participate in the census and what information and/or materials must be provided in order to participate;

- Content stating that census participation may or will result in law enforcement consequences;

- Misrepresentation of government involvement in the census, including that an individual's census information will be shared with another government agency; and

- Calls for coordinated interference that would affect an individual's ability to participate in the census, enforcement of which often requires additional information and context.

We will begin enforcement next month and use a combination of technology and people to proactively identify content that may violate this policy.

All content surfaced will be assessed by a team of reviewers who will benefit from the training and guidance of a consultant with census expertise.

And as with voter interference, content that violates our census interference policy will not be allowed to remain on our platforms as newsworthy even if posted by a politician.

Content that does not violate this policy, but may still be inaccurate, will be eligible for fact-checking by our third-party partners and, if rated false, will have more prominent labels and will be ranked lower in News Feed.

We will also fight against potential misinformation by sharing accurate, non-partisan information about how to participate in the census in consultation with the US Census Bureau.

It's important to note that our census interference policy is one of several policies that protect against abusive behavior that may be related to the census.

Our violence and incitement policies, for example, prohibit threats of and incitement to violence.

We don't allow attempts to gather sensitive personal information by deceptive or invasive methods as laid out under our cybersecurity policies.

We also have policies to protect against privacy violations if we were to learn about the posting or sharing of hacked census data or phishing attempts to gain access to personally identifiable information.

Similarly, our bullying and harassment policies aim to protect against potential harassment or intimidation.

Banning Ads that Aim to Limit Census Participation

While all ads must adhere to our Community Standards and therefore cannot include things like harassment or threats of violence, we are also introducing a new advertising policy that prohibits ads that portray census participation as useless or meaningless or advise people not to participate in the census.

In addition, ads about the census will be subject to the increased transparency requirements for issue ads.

This means any advertiser who wants to run an ad about the census will have to complete our strengthened authorization process for ads about social issues, elections or politics and include a disclaimer on such ads so people know who paid for them.

These ads will be saved in our Ad Library for at least seven years.

Partnering with the US Census Bureau and Other Experts

Our work to help protect the census from interference is strengthened thanks to input from Members of Congress, the Census Bureau and other experts. We support the bipartisan resolution introduced by Senators Schatz and Murkowski to ensure the census is fair and accurate, and to encourage everyone in the US to be counted.

We have also met with Census officials multiple times to brief them on our plans and coordinate with them to disrupt census interference, and we're working with the Census Bureau to identify trusted partners who will be able to flag potentially suppressive census content on Facebook and Instagram.

We've set up a multi-disciplinary team across product, engineering, policy, operations and legal to work on protecting and promoting the census. We are also using our operations center for real-time monitoring of potential census interference so that we can quickly address any abuse.

We are also working with local officials and Census Bureau partners by giving them access to CrowdTangle displays, a Facebook tool used to track how content spreads online.

CrowdTangle has already helped fact-checkers and local governments ahead of elections by monitoring for potential misinformation and suppressive content, so we plan to use the same tools and preparedness

mechanisms to monitor census-related content on Facebook and Instagram.

We have also joined Get Out The Count efforts in partnership with the Census Bureau and will continue to train organizations identified by the Bureau on how to encourage census participation.

We must do our part to ensure an accurate census count, which is critical for the distribution of federal funds, the apportioning of electoral representatives and the functioning of a democracy.

We believe that the partnerships, policies and products we've developed this year have put us on strong footing heading into next year's census.

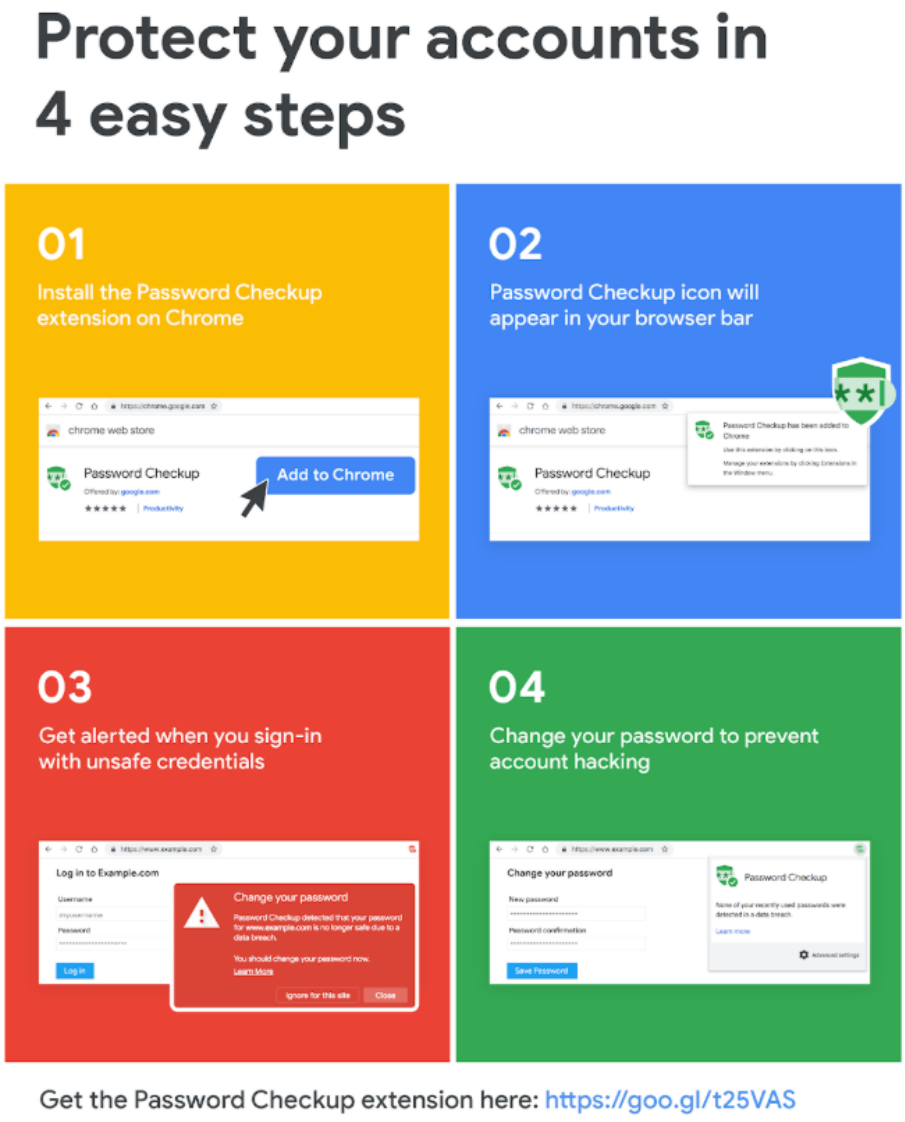
Number 7

Warnings about compromised passwords

Google Security Blog

Google first introduced password breach warnings as a Password Checkup extension early this year. (You may visit: https://chrome.google.com/webstore/detail/password-checkup-extensio/pncabnpcffmalkkjpajodfhijclecjno?hl=en)

It compares passwords and usernames against over 4 billion credentials that Google knows to have been compromised. You can read more about it at: https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html



In October, Google built the Password Checkup feature into the Google Account, making it available from passwords.google.com.

Chrome's integration is a natural next step to ensure we protect even more users as they browse the web.

Here is how it works:

- Whenever Google discovers a username and password exposed by another company's data breach, we store a hashed and encrypted copy of the data on our servers with a secret key known only to Google.

- When you sign into a website, Chrome will send a hashed copy of your username and password to Google encrypted with a secret key only known to Chrome.

  No one, including Google, is able to derive your username or password from this encrypted copy.

- In order to determine if your username and password appears in any breach, we use a technique called private set intersection with blinding that involves multiple layers of encryption.

  This allows us to compare your encrypted username and password with all of the encrypted breached usernames and passwords, without revealing your username and password, or revealing any information about any other users' usernames and passwords.

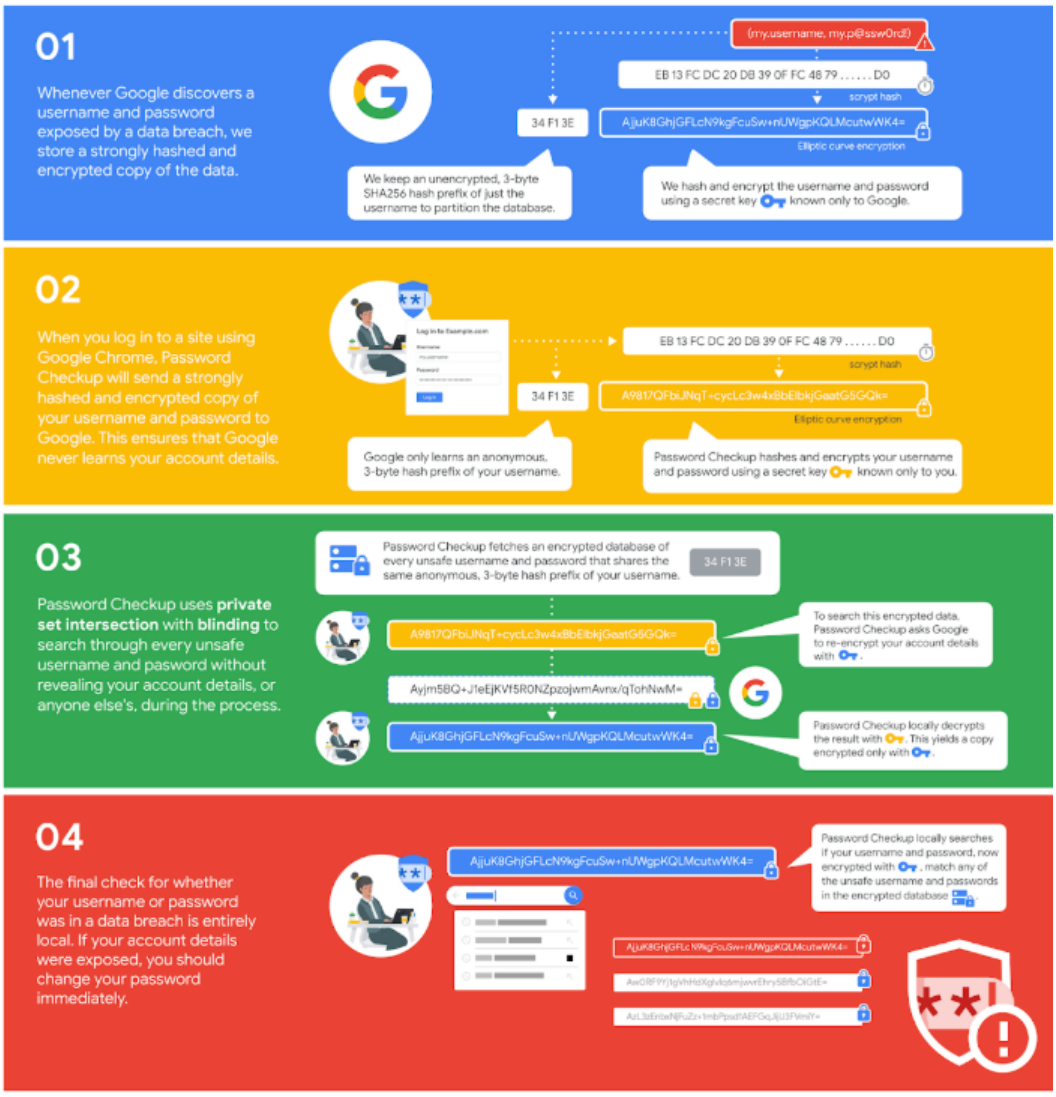
  In order to make this computation more efficient, Chrome sends a 3-byte SHA256 hash prefix of your username to reduce the scale of the data joined from 4 billion records down to 250 records, while still ensuring your username remains anonymous.

- Only you discover if your username and password have been compromised.

  If they have been compromised, Chrome will tell you, and we strongly encourage you to change your password.

Under the hood:

How Password Checkup for Google Chrome helps keep your accounts safe



Number 8

EIOPA publishes annual report on the use of capital add-ons under Solvency II

The European Insurance and Occupational Pensions Authority (EIOPA) published today its annual report on the use of capital add-ons by national competent authorities (NCAs) under Solvency II.

The objective of the capital add-on measure is ensuring that the regulatory capital requirements reflect the risk profile of the undertaking or of the group.

Therefore, it is important that it is used by NCAs when needed and it is also important to ensure a high degree of supervisory convergence within the 31 European Economic Area (EEA) countries, including the EU Member States, regarding its use.

This analysis is based on 2018 year-end Solvency II data collected under Directive 2009/138/EC as reported by the undertakings and insurance groups complemented by a survey that entailed both qualitative and quantitative questions.

During 2018, eight NCAs set capital add-ons to 21 solo undertakings, out of 2819 (re)insurance undertakings under the Solvency II Directive in the EEA. These include 10 non-life undertakings, eight life undertakings, two reinsurers and one composite undertaking.

In 2017, six NCAs had set capital add-ons for a total of 23 solo undertakings. Hence, although the number of capital add-ons is extremely low and decreased slightly from 2017 to 2018, two more NCAs made use of this tool in 2018.

The amount of capital add-ons imposed on undertakings using the standard formula remains very low overall in 2018 accounting for 1% of the total Solvency Capital Requirement (SCR). However, the amount of capital add-on is not insignificant when considering the amount at individual level.

In sum, as of year-end 2018, the weight of the capital add-on increased to 32% (30% in 2017) when looking at the amount of capital add-ons as a

percentage of the total SCR for those undertakings using the standard formula with capital add-ons.

The distribution of the capital add-ons as a percentage of the total SCR in 2018 for undertakings that imposed capital add-ons varies substantially once more.

In 2018, the largest percentage was 80% (83% in 2017), whereas the smallest percentage rounded close to 0% (1% in 2017). It should be noted that in all but five cases, if applied, the capital add-on increased the SCR by more than 10%.

The report:
https://eiopa.europa.eu/Publications/Reports/EIOPA_2018_Capital_add_ons_report_Final.pdf

Number 9

Fake ‘free giveaway’ websites

Cyber security researchers have uncovered a fake ‘free giveaway’ website that tricks users into revealing their login credentials.

Cyber criminals posted links to a phishing website in the comments section of the legitimate Steam website, encouraging users to visit a convincing – but fake – page that contained free downloadable content for the platform.

In order to download the content, users were instructed to log in to the fake site using their Steam credentials. While the screen looks like a legitimate Steam login page, any usernames and passwords that users entered were sent to the attackers instead.

Phishing scams such as this are a particularly devious method used by cyber criminals to steal sensitive information, and it can be a worrying time for victims. The NCSC has produced guidance for spotting and dealing with phishing emails. You may visit:
https://www.ncsc.gov.uk/guidance/suspicious-email-actions

Number 10

NIST Releases Data to Help Measure Accuracy of Biometric Identification

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

New biometric research data — ranging from fingerprints to facial photographs and iris scans — is now available from the National Institute of Standards and Technology (NIST).

Stripped of identifying information and created expressly for research purposes, the data is designed primarily for testing systems that verify a person's identity before granting access — be it to another room or another country.

Few available resources exist to help developers evaluate the performance of the software algorithms that form the heart of these systems, and the NIST data will help fill that gap.

"This all gets back to reproducible research," said NIST computer scientist Greg Fiumara. "The data will help anyone who is interested in testing the error rates of biometric identification systems."

The files, which are available on the NIST website, are organized into three Special Databases (SDs).

Numbered SD 300, SD 301 and SD 302, they represent the first in what is intended to be an expanding collection of biometric resources. You may visit:
https://www.nist.gov/itl/iad/image-group/resources/biometric-special-databases-and-software

While the three databases contain varied types of data collected at different times, two of them contain information gathered during the Nail to Nail Fingerprint Challenge, an IARPA-funded competition that NIST helped to design and carry out.

One of the new resources, SD 301, is significant for being the first "multimodal" dataset NIST has ever released.

Multimodal means that an individual's different biometric markers — in this case face, fingerprints and iris scan — are all linked so that they can be used together for identification by systems that use a combination of

identification approaches, such as a photograph from the individual's face in addition to their fingerprints.

"This opens up possibilities for types of multimodal research that haven't been done before," Fiumara said. "We want to get more secure and more accurate identification, as multimodal systems are harder to spoof."

SD 302 contains fingerprint data from a few hundred people gathered by a mixture of eight commercially available and prototype devices.

Data collected during both portions of the Nail to Nail challenge includes prints taken with contactless fingerprint devices, a technology that could simplify and speed up print gathering as it improves.

"It also includes latent fingerprint data, in which prints are left while handling everyday objects," Fiumara said. "Realistically and expertly collected latent data is difficult to come by."

All of the individuals represented in the two sets have formally consented to the inclusion of their biometric and demographic data and its distribution for use in advancing research, Fiumara said. The data has been scrubbed of identifying information such as their names and places of residence.

Rounding out the datasets is SD 300, a collection of fingerprints taken from 900 old ink cards. All of the record cards have been stripped of identifying data and are from individuals who are now deceased.

According to Fiumara, a benefit of the data is helping manufacturers evaluate how well their modern systems can produce results that will be interoperable with hard-copy ink records, which will remain important to the criminal justice system for some time.

As a whole, the group of three SDs contain data retained with archival-grade lossless compression — a step forward, Fiumara said, because the research data sets in the past often did not retain this level of fidelity to the original image.

Each dataset in the series has an accompanying user's guide offering background about collection methods and other details useful to researchers.

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.

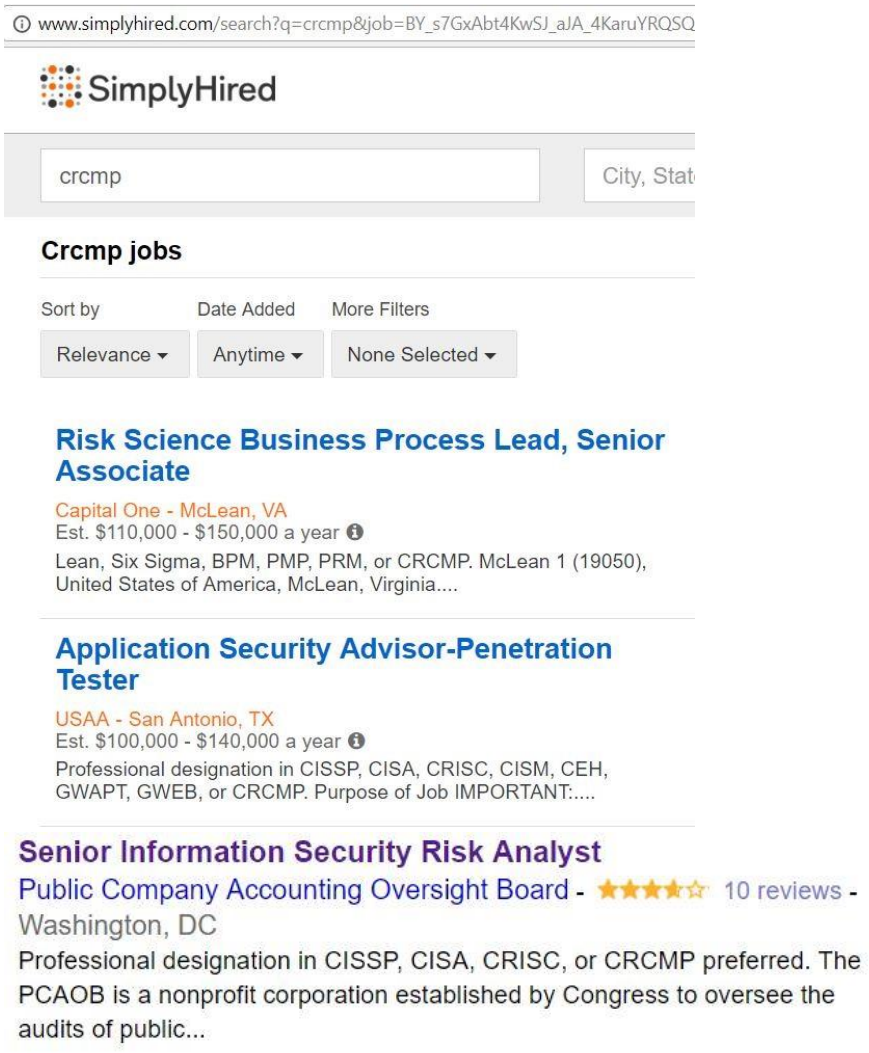
International Association of Risk and Compliance Professionals

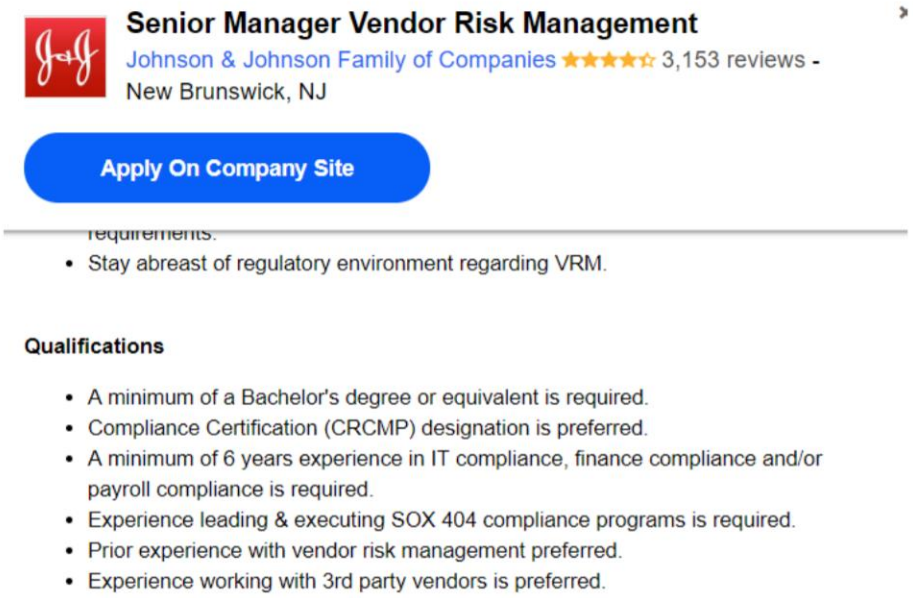
You can explore what we offer to our members:

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