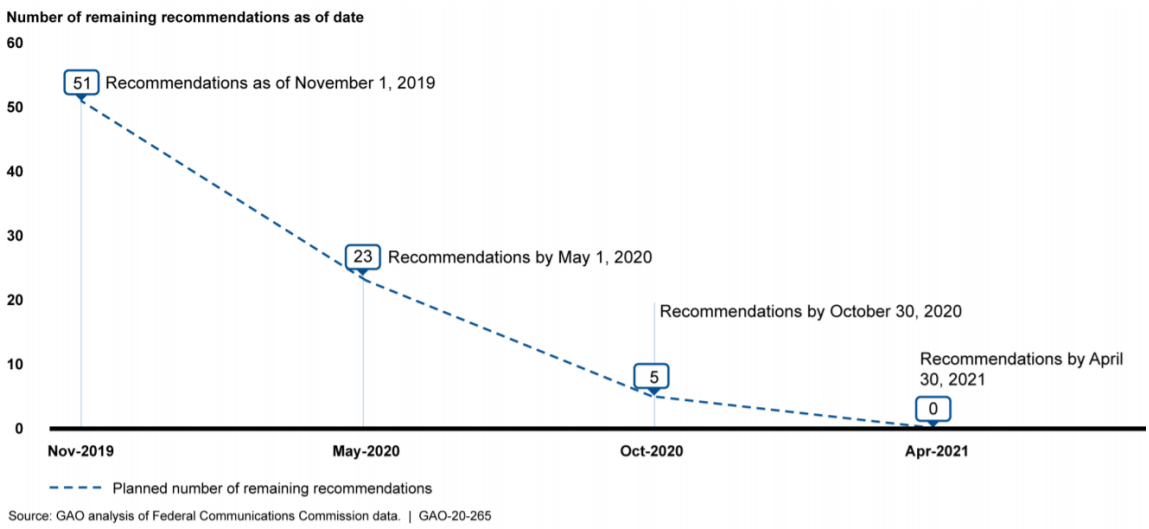
Monday, May 11, 2020

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,

The *Reports to Congressional Requesters* from the United States Government Accountability Office (GAO) are always interesting. When one of these reports covers *remaining control deficiencies*, I change my schedule and I simply cannot wait to read it.

I like the way the GAO ensures all recommendations will be implemented:



According to the paper, the Commission *had not effectively implemented controls intended to detect cybersecurity events or deficiencies.*

The *detect* core security function is intended to allow for the timely discovery of cybersecurity events and deficiencies. Controls associated with this function include logging and monitoring system activities, and

assessing security controls in place. NIST SP 800-53 states that agencies should enable system logging features and retain sufficient audit logs to support the investigations of security incidents and monitoring of select activities for significant security-related events.

Additionally, NIST SP 800-53 and industry leading practices state that organizations should increase their situational awareness through enhanced monitoring capabilities to analyze network traffic data over an extended period of time at external boundaries and inside their internal network to identify anomalous, inappropriate, or unusual malicious activities.

Lastly, FISMA requires each agency to periodically test and evaluate the effectiveness of its information security controls in place applicable to policies, procedures, and practices.

In September 2019, the Government Accountability Office (GAO) reported that the Commission had implemented security monitoring controls, such as performing regular vulnerability scanning and deploying a system information and event management tool, to detect the presence of potential malicious threats.

However, six technical control deficiencies in these capabilities diminished the effectiveness of the controls to detect cybersecurity events in the systems we reviewed.

For example, the Commission did not fully capture system log data on certain devices and had limited network monitoring visibility into portions of its data center environment.

According to Information Technology Center officials, the Commission had deficiencies in logging, retention, and monitoring because the Commission had not fully configured its security information and event monitoring tool to capture and monitor sufficient system log and network traffic data to adequately detect cybersecurity events.

As a result, the Commission may not be able to detect or investigate anomalous activities inside its network.

In addition, although the commission established a process for assessing the effectiveness of the security controls for its systems, its control tests and evaluations were not sufficiently robust.

For example, the Commission's evaluations did not identify many of the security control deficiencies the GAO identified. Consequently, the

Commission had limited assurance that the security controls were in place and operating as intended. As of November 2019, the Commission had acted to address several technical control deficiencies, and associated recommendations, such as capturing network traffic data and providing for real-time network monitoring; however, other technical control deficiencies remain.

Also, the Commission *did not consistently encrypt sensitive data*.

NIST SP 800-53 recommends that organizations employ cryptographic mechanisms to prevent the unauthorized disclosure of information during transmission and establish a trusted communications path between users and security functions of information systems.

However, in seven instances, the Commission did not consistently deploy strong encryption capabilities to protect sensitive data or establish a secure communications path between users and information systems.

Read more at number 1 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)

The Federal Communications Commission (FCC) made significant progress, but needs to address remaining control deficiencies and improve its program

United States Government Accountability Office

GAO

Report to Congressional Requesters

Number 2 (Page 9)

BIS global liquidity indicators at end-December 2019

BIS

Number 3 (Page 11)

The legal implications of malicious exploitation of social media

Published by the NATO Strategic Communications Centre of Excellence

Number 4 (Page 13)

CONSUMER GUIDE: Understand your insurance coverage during Coronavirus/COVID-19 Outbreak

eiopa

European Insurance and Occupational Pensions Authority

Number 5 (Page 14)

EBA provides additional clarity on measures to mitigate the impact of COVID-19 on the EU banking sector

EBA European Banking Authority

Number 6 (Page 15)

Selecting and Safely Using Collaboration Services for Telework

Number 7 (Page 17)

IFC Report - Computing platforms for big data analytics and artificial intelligence

Number 8 (Page 19)

Red carpet for silver surfers

BaFin President Felix Hufeld wants to ensure that senior citizens continue having unobstructed access to financial services, also in a digitalised world.

Number 9 (Page 23)

Millions of fitness app users exposed after data breach

Number 10 (Page 24)

In Glowing Colors: Seeing the Spread of Drug Particles in a Forensic Lab

Black-light videos from NIST will help crime labs manage an invisible risk.

Number 1

The Federal Communications Commission (FCC) made significant progress, but needs to address remaining control deficiencies and improve its program

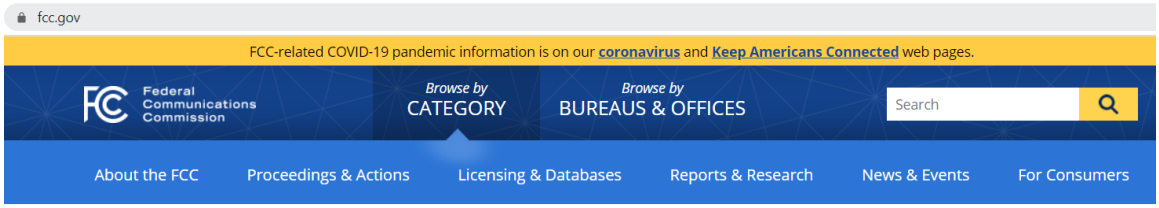
United States Government Accountability Office

GAO

Report to Congressional Requesters

Established by the Communications Act of 1934, FCC regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and U.S. territories.

FCC is responsible for, among other things, making available nationwide worldwide wire and radio communication service.



More recently, it has been responsible for promoting competition and reducing regulation of the telecommunications industry in order to secure lower prices and higher quality services for consumers.

FCC's functions include:

• issuing licenses for broadcast television and radio;

• overseeing licensing, enforcement, and regulatory functions of carriers of cellular phones and other personal communication services;

• regulating the use of radio spectrum and conducting auctions of licenses for spectrum;

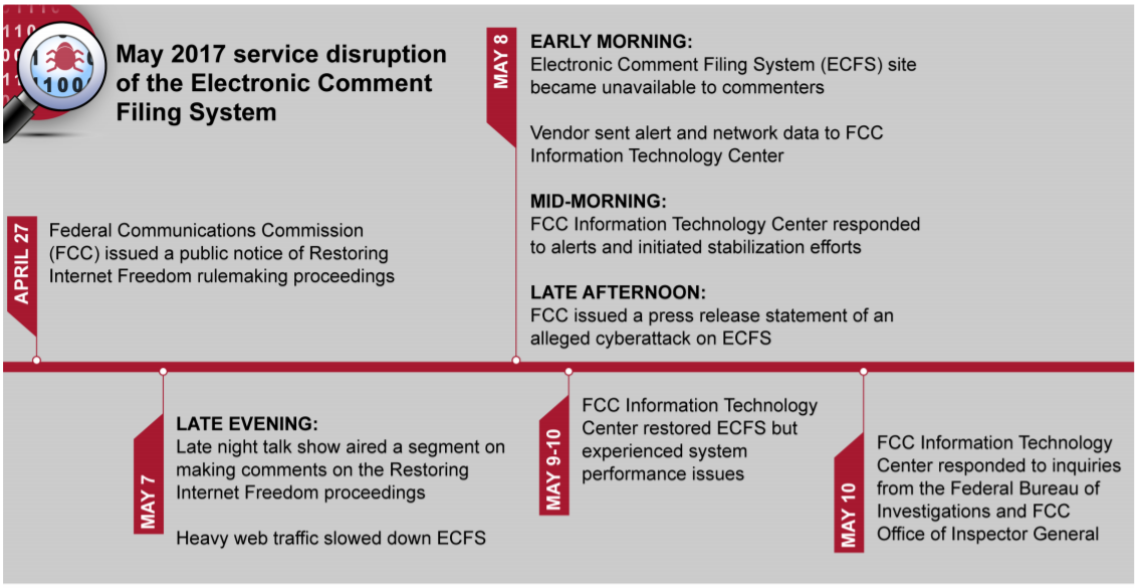
• investigating complaints and taking enforcement actions if it finds that there have been violations of the various communications laws and commission rules that are designed to protect consumers;

• addressing issues related to public safety, homeland security, emergency management, and preparedness;

• educating and informing consumers about communications goods and services; and

• reviewing mergers of companies holding FCC-issued licenses.

Figure 1: The Federal Communications Commission's Electronic Comment Filing System May 2017 Service Disruption and Subsequent Related Events Timeline



June 21, 2017	FCC Office of Inspector General opened an investigation of an alleged cyberattack of ECFS.
January 4, 2018	FCC Office of Inspector General referred the ECFS investigation to the Department of Justice.
August 7, 2018	FCC Office of Inspector General published an investigative report on the ECFS event.
August 16, 2018	FCC Chairman testified at a Senate oversight hearing on the investigative report on the ECFS event.

Source: GAO analysis of Federal Communications Commission information. | GAO-20-265

Figure 2: FCC Improvements to the Electronic Comment Filing System (ECFS) in Response to the May 2017 Service Disruption (as of November 2018)

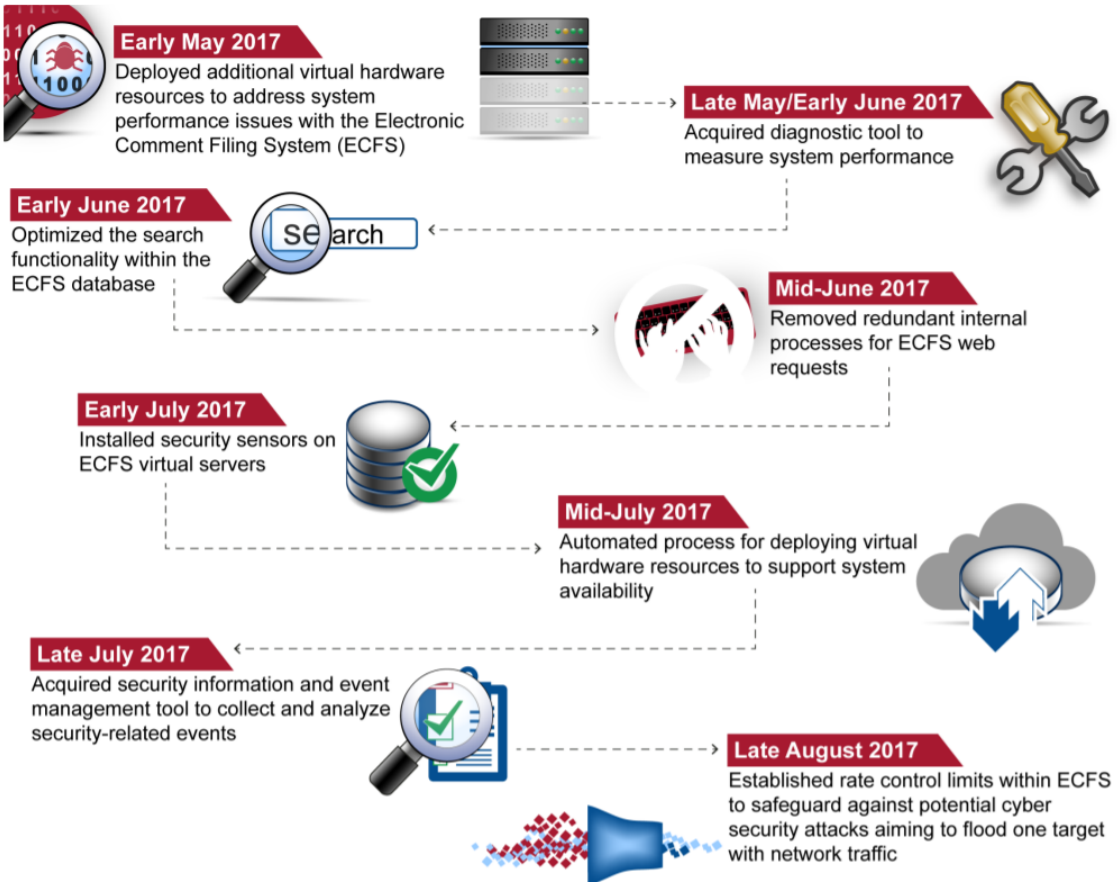


Table 1: Number of GAO-Identified Information Security Program and Technical Control Deficiencies at FCC and Associated Recommendations by Core Security Function, as of September 2019

Core security function	Number of information security program deficiencies	Number of information security program recommendations	Number of technical control deficiencies	Number of technical control deficiency recommendations
Identify	3	4	0	0
Protect	1	1	37	108
Detect	0	0	6	17
Respond	2	2	1	2
Recover	2	2	0	0
Total	**8**	**9**	**44**	**127**

Source: GAO analysis of Federal Communications Commission information security program and technical controls. | GAO-20-265.

Note: The five core security functions are part of the NIST cybersecurity framework, as updated in National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Apr. 16, 2018). As discussed later in this report, FCC has taken action to address many of these deficiencies and associated recommendations.

The report:
https://www.gao.gov/assets/710/705514.pdf

Number 2

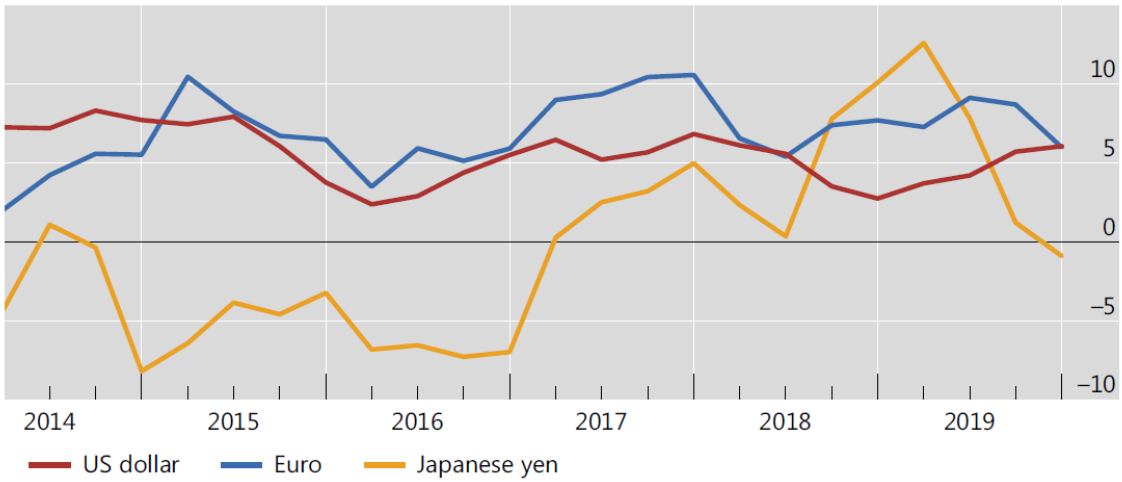
BIS global liquidity indicators at end-December 2019

• US dollar credit to non-bank borrowers outside the United States grew by 6% in 2019, to reach $12.2 trillion at end-2019.

• The annual growth rate of euro-denominated credit outside the euro area slowed to 6%, while that of yen-denominated credit outside Japan turned negative (–1%).

• In 2019, euro-denominated credit overtook US dollar-denominated credit as the largest stock of foreign currency credit to emerging Europe.

• The debt securities share in US dollar credit outside the United States has risen considerably over the past decade across a number of major borrowing regions.



Graph 1: Annual percentage change of US dollar-, euro- and yen-denominated credit to non-resident non-banks (interactive graph).

Source: BIS global liquidity indicators (Tables E2.1, E2.2 and E2.3).

US dollar-denominated credit to non-banks outside the United States grew by 6% during 2019 (Graph 1, red line).

This brought the outstanding amount of USD denominated credit outside the United States to $12.2 trillion as of end-2019.

Growth in euro-denominated credit to non-banks outside the euro area (blue line) slowed to 6% year on year (yoy), reaching €3.4 trillion (equivalent to $3.8 trillion).

Credit denominated in Japanese yen to non-banks outside Japan contracted at 1% yoy (yellow line).

Bank loans were the main driver of the deceleration observed for both currencies. US dollar-denominated credit to non-banks in emerging market and developing economies (EMDEs) grew by 5% during 2019. Euro-denominated credit to those borrowers expanded at an even faster clip (10% yoy).

It has consistently expanded more rapidly than USD credit for more than five years. Nevertheless, the outstanding stock of euro-denominated credit to EMDEs (€763 billion, equivalent to $857 billion) was still considerably smaller than its US dollar counterpart ($3.9 trillion).

US dollar-denominated credit expanded in all but one EMDE region during 2019. Credit to Africa and the Middle East, which has been growing at double-digit rates since mid-2015, rose by 14% in 2019.

Credit to emerging Asia-Pacific and Latin America also expanded, by 4% and 3%, respectively, during 2019.

To read more:
https://www.bis.org/statistics/gli2004.pdf

Number 3

The legal implications of malicious exploitation of social media

Published by the NATO Strategic Communications Centre of Excellence

The growing use of digital media is a well-observed phenomenon, with 90% of adults regularly accessing the Internet, and youth use averaging at least six hours a day.

Together with the increasing digitalization of private and public sector models, digital space is creating a parallel space of social activity.

This activity functions in a decentralized structure and across a variety of Websites and platforms, each under its own legal regimes and stakeholders.

Information flows are filtered through a few 'points of control,' directly impacting interaction between individuals, sovereigns, and other entities.

Through popular use, social media and video platforms are becoming especially important gatekeepers. Such platforms have morphed into concentrated arenas for public discourse and attention.

While this brings many benefits, it also presents a gamut of new digital manipulation threats which necessitate governance.

For example, the difficulty of authentication has given rise to the use of troll and cyborg entities capable of increasingly authentic proliferation of disinformation narratives.

Traditional hacking tools resulting in impersonation capacity are further benefiting from advances in image and sound manipulation software capable of 'deepfaking' individuals.

These tools are being amalgamated by states and non-states to engage in massive social media manipulation and social engineering campaigns.

Concurrently, new over- and underground markets have sprawled to collect and broker internet user data, expediting access to information that can be used for the purpose of manipulation.

The initial difficulty with managing the transnational digital domain is only reinforced by the proprietary nature of social media entities.

This has made regulating against the malicious use of digital space a complex matter, interweaving several types of stakeholders.

While from a legal standpoint, activity on the Internet is generally not differentiated from activity offline, its digital character necessitates a different approach.

The aim of this report is to outline the types of legal frameworks that have been set up by sovereigns to maneuver through and against the malicious use of social media networks, comment on the challenges faced, and identify policy trajectories.

Focus is placed on the German Network Enforcement law (NetzDG) as the prototypical archetype for a comprehensive and binding regime for social media intermediaries.

Through a transatlantic comparison with other jurisdictions and courts, the legal tendencies of the malicious use of digital space are outlined, and recommendations are provided for the path forward.

To read more:
https://www.stratcomcoe.org/legal-implications-malicious-exploitation-social-media

Number 4

CONSUMER GUIDE: Understand your insurance coverage during Coronavirus/COVID-19 Outbreak

Number 5

EBA provides additional clarity on measures to mitigate the impact of COVID-19 on the EU banking sector

Following its call for flexibility in the prudential framework and supervisory approaches to support lending into the real economy, the European Banking Authority (EBA) clarified today its expectations in relation to dividend and remuneration policies, provided additional guidance on how to use flexibility in supervisory reporting and recalled the necessary measures to prevent money laundering and terrorist financing (ML/TF).

The EBA supports all the measures taken so far to ensure banks maintain a sound capital base and provide the needed support to the economy.

In this respect, the EBA reiterates and expands its call to institutions to refrain from the distribution of dividends or share buybacks for the purpose of remunerating shareholders and assess their remuneration policies in line with the risks stemming from the economic situation.

In addition, the EBA provides details on its call for competent authorities to offer leeway on reporting dates, urging one-month flexibility for reports with remittance dates between March and the end of May 2020.

The EBA also called for flexibility in assessing deadlines of institutions' Pillar 3 disclosures. This flexibility would not put at risk the access to crucial information on banks' capital, risks and liquidity, which is needed to monitor closely their financial and prudential situation.

Furthermore, the EBA decided, in coordination with the Basel Committee on Banking Supervision (BCBS), to cancel the Quantitative Impact Study based on June 2020 data.

Finally, as measures to prevent money laundering and terrorist financing (ML/TF) remain crucial in this challenging time, the EBA calls on competent authorities to support financial institutions' ongoing efforts by sharing information on emerging ML/TF risks, setting clear regulatory expectations and using supervisory tools flexibly.

Number 6

Selecting and Safely Using Collaboration Services for Telework

During a global pandemic or other crisis contingency scenarios, many United States Government (USG) personnel must operate from home while continuing to perform critical national functions and support continuity of government services.

With limited access to government furnished equipment (GFE) such as laptops and secure smartphones, the use of (not typically approved) commercial collaboration services on personal devices for limited government official use becomes necessary and unavoidable.

We define collaboration services as those capabilities that allow the workforce to communicate via internet-enabled text, voice, and video, and can include the sharing of files and other mission content.

Collaboration can occur between two people or widened to include a large group to support mission needs.

This document provides a snapshot of best practices and criteria based on capabilities available at the time of publication and was coordinated with the Department of Homeland Security (DHS), which is releasing a similar guide: “Cybersecurity Recommendations for Federal Agencies When Using Video Conferencing Solutions.”

This NSA publication is designed to provide simple, actionable, considerations for individual government users.

The intent of this document is not meant to be exhaustive or based on formal testing, but rather be responsive to a growing demand amongst the federal government to allow its workforce to operate remotely using personal devices when deemed to be in the best interests of the health and welfare of its workforce and the nation.

Recommendations in this document are likely to change as collaboration services evolve and also address known vulnerabilities and threats.

Users should be aware that even the most secure collaboration service cannot defend against a compromised user device.

Service	Basic Functionality	1 – E2E Encryption	2 – Testable Encryption	3 – MFA	4 – Invitation Controls	5 – Minimal 3rd Party Sharing	6 – Secure Deletion	7 – Public Source Code Shared	8 – Certified Service (FedRAMP / NIAP)
Cisco Webex®[9]	a, b, c, d, e	Y[1]	Y	Y[12]	Y[1]	Y	Client – Y Server – N[3]	N	FedRAMP
Dust	a	Y	N[3]	N	Y	N	Client – Y Server – Y	N	None
Google G Suite™[10]	a, b, c, d	N	Y	Y[1]	Y[1]	Y	Client – Y Server – Y[2]	N	FedRAMP
GoToMeeting®[11]	a, b, c	Y[1]	Y	N	Y[1]	Y	Client – Y Server – N[3]	N	None
Mattermost™[12]	a, b, c, e	Y	Y	Y[2]	Y	N	Client – Y Server – N	Y	FedRAMP
Microsoft Teams®[13]	a, c, d, e	N	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Signal®[14]	a, b, d	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Skype for Business™[15]	a, c, d, e	Y[4]	Y[4]	Y	Y	N	Client – Y Server – N[3]	N	None
Slack®[16]	a, c, d, e	N	Y	Y	Y	N[3]	Client – N Server – N	N	FedRAMP
SMS Text	a, d	N	N	N	N	N	Client – Y Server – N	N	None
WhatsApp®[17]	a, c, d	Y	Y	Y	Y	Y	Client – Y Server – Y	N	None
Wickr®[18]	a, c, d, e	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Zoom®[19]	a, b, c, e	Y[14]	Y	N	Y	Y	Client – Y Server – N[3]	N	FedRAMP

Table of Assessments against Criteria

To read more:
https://media.defense.gov/2020/Apr/24/2002288652/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-FINAL.PDF

Number 7

IFC Report - Computing platforms for big data analytics and artificial intelligence

Public authorities, and central banks in particular, are increasingly realising the potential of big data sets and analytics – with the development of artificial intelligence (AI) and machine learning (ML) techniques – to provide new, complementary statistical information (Hammer et al (2017)).

Yet the question remains: how should institutions organise themselves to benefit the most from these opportunities?

Two areas appear particularly important for central banks.

The first is how to organise their statistical information in relation to their IT infrastructure.

The second is to think strategically as to how to use appropriate techniques to further process and analyse the new information collected.

Like many national statistical offices (NSOs) and international organisations, central banks have already launched numerous initiatives to explore these issues and exchange on their experience, in particular through the cooperative activities organised by the Irving Fisher Committee on Central Bank Statistics (IFC) of the Bank for International Settlements (BIS).

The BIS itself has developed its new medium-term strategy, Innovation BIS 2025, which relies on important investment in next generation technology to build a resilient and future-ready digital workplace for the organisation (BIS (2019)).

A key feature of these various initiatives is that many central banks are currently setting up, or envisaging implementing, big data platforms to facilitate the storage and processing of very large data sets.

They are also developing high-performance computing (HPC) infrastructure that enables faster processing, in-depth statistical analysis and complex data simulations.

However, these initiatives face important organisational challenges, as central banks trade off factors such as technology trends, system complexity, cost, performance, reliability, operating model and security.

In view of this experience, it is essential to carefully assess the options available before selecting a technology and architecture to set up big data / HPC platforms.

Among the various issues to be considered, attention should primarily focus on the hardware selection, the choice between proprietary and open source technology, the decision to develop the solution in-house or in the cloud, and the type of information to be handled.

Once the main options are selected, the actual implementation of the related technologies is often a long and multiform journey.

From a project development perspective, success will depend on the approach for conducting the project, the types of workload to be supported, the data architecture envisaged and the use of software development best practices.

Having a broader, institution-level perspective is also key, so as to adequately take into account the full range of business requirements as well as resources and security constraints.

It may therefore be recommended to develop a comprehensive information strategy for the institution, with a high-level roadmap for the adoption of continuously changing technologies to manage data and respond to users' needs.

Last but not least, knowledge-sharing can be instrumental, and can be facilitated by the cooperative activities promoted by the BIS and the IFC.

To read more:
https://www.bis.org/ifc/publ/ifc_report_computing_2004.pdf

Number 8

Red carpet for silver surfers

BaFin President Felix Hufeld wants to ensure that senior citizens continue having unobstructed access to financial services, also in a digitalised world.

BaFin Federal Financial Supervisory Authority

Anyone able to remember Paul McCartney crooning to "When I'm 64" is also likely to be well into their sixties by now.

As the character in the Beatles' hit contemplates what the future may hold, the average person in Germany can expect to live many years past the age of 64.

This is because the remaining life expectancy of 65-year olds in Germany is currently 18 years for men and 21 for women. Mathematically, this means that people entering retirement in Germany can expect to enjoy another two decades of adult life.

In BaFin's guide to investing for people in retirement ("Geld anlegen im Ruhestand"), BaFin Chief Executive Director Elisabeth Roegele noted that, for most of us, entering retirement also marks a financial turning point.

Whether someone needs money for their dream holiday or to cover unexpected health costs – both the upsides and downsides of life are influenced by our financial situation.

In addition, the world of finance is increasingly advancing into the world of digitalisation.

This is why being able to access banking or insurance services is one of the biggest financial challenges facing older people alongside issues such as the amount of household income available per person and protection against fraud.

"Senior citizens must be given unobstructed access to financial services, also in times of rapid digitalisation", said BaFin President Felix Hufeld.

Analogue versus digital

While it is still possible for consumers to manage their current accounts and insurance policies without using digital technology, it can be a huge challenge for older people if a bank branch closes in their neighbourhood.

Alternative solutions, such as withdrawing cash at the supermarket checkout, can only compensate for this to a limited extent. “It is important that older people continue to have access to the market – whether by analogue or digital means“, said Hufeld.

In order to guarantee the financial inclusion of senior citizens or, conversely, prevent their digital exclusion, it is necessary to ensure that consumers are well-informed and to have both the right regulatory framework and vigilant supervision.

Regulatory response

“We, here in Europe, need to invest more time and energy in our efforts to find an appropriate regulatory response to the issues we will inevitably face“, said Hufeld during an event in Berlin at the end of October 2019 in his review of the G20 symposium in Tokyo.

The demographic challenges facing Japan as a result of its low birth rate and high life expectancy was a key topic at the meeting bringing together the representatives of the world’s 20 leading industrialised and emerging economies.

Recent EU legislation does not account for age as a criterion based on which a distinction between consumers may need to be made.

Neither the Markets in Financial Instruments Directive II (MiFID II) nor the Insurance Distribution Directive (IDD) stipulate that those selling a financial instrument or insurance are required to gear their advice to the customer’s needs based on their age.

Even so, both MiFID II and the IDD are aimed at ensuring that consideration is given to the individual needs of customers when an appointment to discuss investment options takes place and when subsequent investment recommendations are made.

This naturally excludes a 30-year horizon as possible recommendation for an 80-year-old, for example.

Consumer information provided by BaFin

Ideally, customers will know which investments are suitable for their needs because they will have already obtained information, for example directly from BaFin. Among the brochures that have been published, BaFin’s investment primer written in simple language (“Das kleine ABC der

Geldanlage in Leichter Sprache") has become a bestseller that is popular with all age groups and educational levels.

This shows that there is a high demand for information about financial matters in clear and simple language. Hufeld also believes that "financial markets need to remain understandable."

BaFin has published a brochure that is aimed specifically at older readers. The BaFin guide to investing for people in retirement ("Geld anlegen im Ruhestand") discusses a range of financial instruments and their suitability – from current accounts ("not the best financial product for saving money") and overnight accounts ("also suitable as an emergency reserve") to securities ("higher investment risk, better earnings prospects"). Like insurance, all these products are also available online.

Secure access to the internet is the main theme of meet-ups run by Digital-Kompass, a project supported by various senior citizen and consumer protection organisations.

BaFin's experts have also taken part in such a meet-up where they provided information on the digital transformation of the financial industry.

Virtual currencies, robots that make investment recommendations (known as "robo-advisers"), motor insurance based on a person's style of driving or crowdfunding platforms have been a reality for a while now.

As the starting point for activities and transactions on the internet, online banking continues to play a major role.

With 79 per cent of 60- to 69-year-olds and 45 per cent of those over 70 now online, it is becoming increasingly important to ensure that they are able to take advantage of various services such as real-time transfers and that risks such as data theft are reduced as far as possible.

BaFin's role

For this reason, BaFin issues regular warnings about dubious activities, for example, when companies are conducting banking business or providing financial services without the required authorisation.

In early December 2018, BaFin and the police had already warned against fraudulent international online trading platforms that attempt to woo customers with the prospect of high returns by persuading them to invest in speculative financial instruments such as contracts for difference (CFDs).

The information on the costs for using such platforms is unclear, leaving customers unable to make profits. Fraudulent trading platforms care little about the age of their victims.

What makes the activities of these online criminals particularly insidious is the way in which they make it particularly easy for consumers to gain access to these dubious platforms.

“In serious cases, we can, as a last resort, restrict or even prohibit the sale of products or certain sales practices – in the case of CFDs, we recently decided to impose stronger restrictions”, said Elisabeth Roegele after the BaFin Consumer Protection Forum with reference to BaFin’s general administrative act on CFD.

Right to a basic payment account

Basic payment accounts are not restricted to a specific group of people. In fact, the German Payment Accounts Act (Zahlungskontengesetz – ZKG) grants all consumers legally residing in the European Union the right to hold a payment account with basic features, thereby enabling them to deposit or withdraw money and carry out direct debits, transfers and payment card transactions.

People who were unsuccessful in concluding a basic payment account agreement with a bank can file an application to BaFin in order to request the initiation of administrative proceedings or make use of the online complaints form provided.

Once this step has been completed, BaFin checks whether the bank had reasons to refuse to set up the account.

There are very few cases in which a bank may make such a refusal, for example if the applicant already has a payment account at another bank in Germany or has committed a criminal offence against the bank.

If no such grounds exist, the bank must set up the basic payment account. As a general rule, all banks must set up a basic payment account if a consumer wishes to open such an account – this applies, of course, even if the consumer is 64.

Number 9

Millions of fitness app users exposed after data breach

National Cyber Security Centre

It has been reported that a firm behind a fitness app has unintentionally leaked data, including personal information, of millions of customers.

Kinomap, which specialises in indoor training, had inadvertently left its database exposed online, which meant that the records of 42 million users from 80 countries were viewable for at least one month.

The breach exposed full names, home country, email addresses, usernames, gender, and timestamps for exercises.

Kinomap says that the database was secured on the day they were alerted by cyber security researchers.

Large stores of data are a tempting target for attackers.

The NCSC has published advice to businesses on how to adequately protect such information at:
https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data

and how to protect against the phishing threat following data breaches at:
https://www.ncsc.gov.uk/guidance/phishing-threat-following-data-breaches

Anyone concerned about the security of their online accounts should follow the guidance in 'Top tips for staying secure online' at:
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

Number 10

In Glowing Colors: Seeing the Spread of Drug Particles in a Forensic Lab

Black-light videos from NIST will help crime labs manage an invisible risk.

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

When two scientists from the National Institute of Standards and Technology (NIST) brought black lights and glow powder into the Maryland State Police crime lab, they weren't setting up a laser tag studio or nightclub.

Instead, their aim was to study the way drug particles get spread around crime labs when analysts test suspected drug evidence. Their study, recently published in Forensic Chemistry (at: https://www.sciencedirect.com/science/article/abs/pii/S2468170920300205 - note: we are not affiliated, and we have not been paid or received any benefits to promote Forensic Chemistry), addresses safety concerns in an age of super-potent synthetic drugs like fentanyl, which can potentially be hazardous to chemists who handle them frequently.

The spread of drug particles cannot be completely avoided — it is an inevitable result of the forensic analyses that crime labs must perform.

To see how it happens, the two NIST research scientists, Edward Sisco and Matthew Staymates, fabricated a brick made of white flour mixed with a small amount of fluorescent powder.

Under everyday lights the brick looked like evidence from a drug seizure, but under ultraviolet light — also called UV or black light — it glowed a bright orange.

Amber Burns, supervisor of the Maryland State Police forensic chemistry lab and a co-author of the study, examined the brick and its contents as she would real evidence.

With a sheet of butcher paper covering her workspace, she cut open the package with a scalpel, scooped out a sample and transferred that scoop into a glass vial for analysis.

She also removed the powder to weigh it on a digital scale without the packaging. When she was done, the black light revealed that some particles had settled onto surfaces in her workspace.

Some had also adhered to her gloves and were transferred by touch onto a marker and wash bottle.

All chemists clean their workspaces between cases to prevent evidence from one case from contaminating the next. After Burns discarded the butcher paper and cleaned her workspace, the black light showed that her cleanup routine was effective.

Before the emergence of fentanyl and other super-potent drugs, such small amounts of drug residue were not a major concern. But that has changed, and not only for reasons of workplace safety.

Drug dealers often mix small amounts of fentanyl into heroin and cocaine, and some labs are increasing the sensitivity of their instruments to detect those small amounts. Highly sensitive instruments are more likely to detect small amounts of drug residue in the environment, so those labs have to be extra careful about limiting their spread.

This visualization experiment led the authors to suggest several steps that might minimize spread. These include changing gloves frequently, using vials and test tubes with large mouths to limit spillage when transferring material into them, and having two sets of wash bottles, one for casework and one for cleanup.

The researchers' paper is written in such a way that any laboratory can reproduce the black-light experiment.

"This is a great way for labs to see which of their practices contribute to the spread of drug residues, and to make sure that their cleanup routines are effective," Sisco said

To read more:
https://www.nist.gov/news-events/news/2020/04/glowing-colors-seeing-spread-drug-particles-forensic-lab

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.

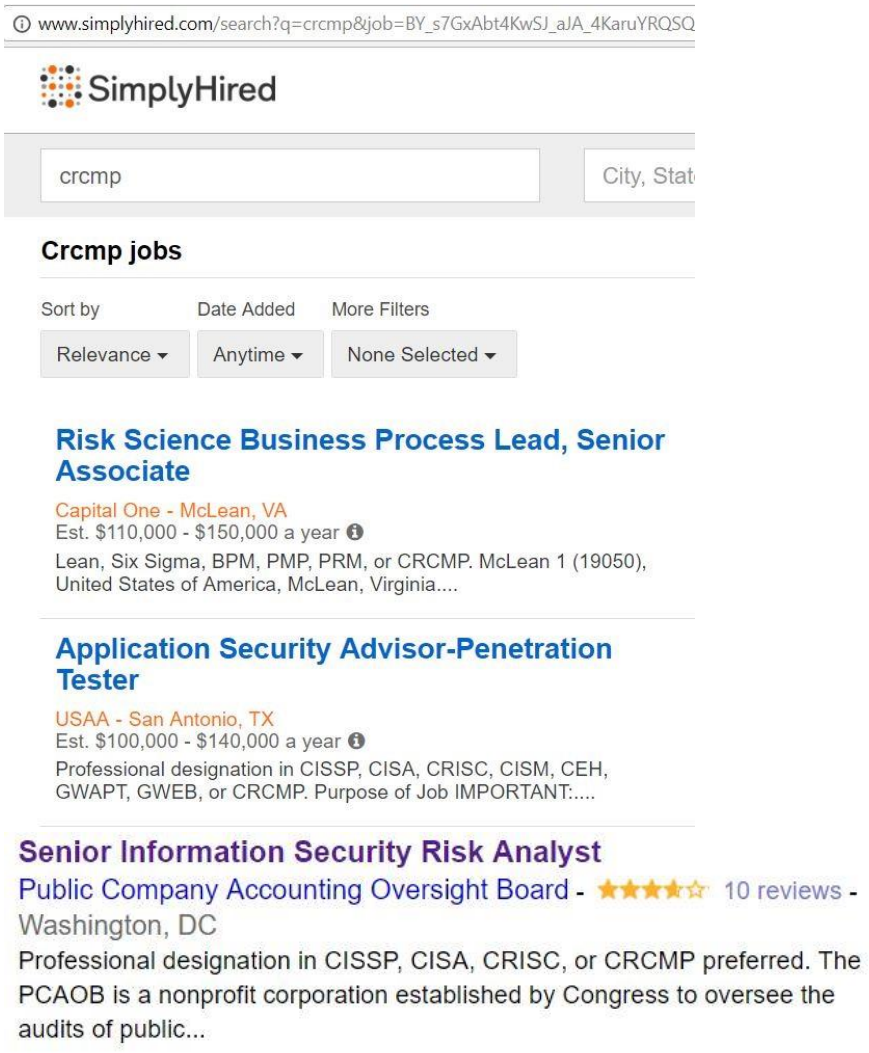
International Association of Risk and Compliance Professionals

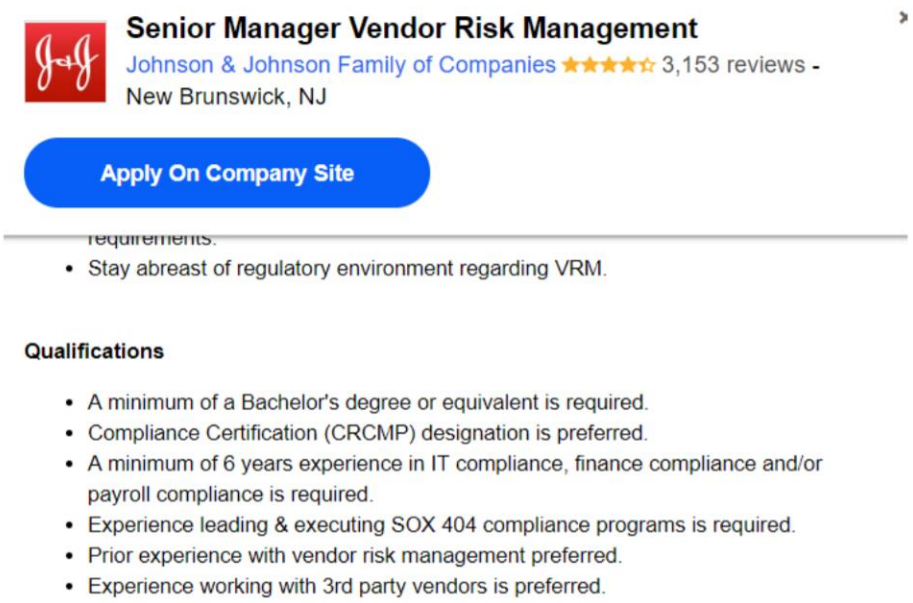
You can explore what we offer to our members:

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