Monday, February 24, 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,

Napoleon Bonaparte has said: "I am sometimes a fox and sometimes a lion. The whole secret of government lies in knowing when to be the one or the other."

Well, we cannot use this approach in corporate governance.

Sir Jon Cunliffe, Deputy Governor Financial Stability (UK), has given a great presentation in Berlin. He said:

"I have used the word "governance". The word is of course closely related to the word "government". But while related, they are not the same thing. We can have governance of the global financial system even though we do not have global government.

Governance can mean legislation, regulation and the institutions of government. But it also encompasses broader frameworks of standards, norms and conventions, international organisations and agreements that fall short of hard law.

Indeed, in a world of nation states and national legislatures and governments, it is on these broader frameworks that we need to depend for the governance of financial globalisation, and the management of cross border risk.

This challenge is not of course confined to the financial sector. International governance structures are required in many economic and non-economic spheres. But since the liberation of global capital flows and liberalisation of international financial markets which began 50 years ago, financial authorities in multiple jurisdictions have sought together to build

the necessary governance frameworks to enable the benefits of financial globalisation while managing the risks."

He continues: "Crisis concentrates minds. It is perhaps inevitable that as time passes and memories fade, there is less political focus on these issues and less will among jurisdictions to ensure governance keeps pace with the risks.

Fatigue sets in. For example:

- Before the crisis Basel II, which was not particularly ambitious, took 10 years to agree.

- By contrast, post-crisis the key elements of Basel III, which was a significant step-change, took just 2 years.

- But as the crisis receded and fatigue developed, it took a further 5 years to finalise Basel 3.1, which implemented less sweeping changes.

The lesson fades that in an integrated global economy we are all ultimately in the same boat or in the words of Benjamin Franklin that "if we do not hang together we will most assuredly hang separately".

Read more at number 3 below. Welcome to the Top 10 list.

Best regards,

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

Number 1 (Page 6)

Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services

Number 2 (Page 10)

Basel III: the implementation imperative

Keynote address by Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, at the 15th BCBS-FSI High-level Meeting for Africa on Strengthening financial sector supervision and current regulatory priorities, Cape Town.

Number 3 (Page 12)

Governance of financial globalisation

Sir Jon Cunliffe, Deputy Governor for Financial Stability of the Bank of England, at the German Economic Council Annual Finance Conference, Berlin.

Number 4 (Page 15)

Spontaneity and order - transparency, accountability and fairness in bank supervision

Randal K Quarles, Vice Chair for Supervision of the Board of Governors of the Federal Reserve System, Yale Law School, New Haven, Connecticut.

Number 5 (Page 23)

Attackers using the Coronavirus as a phishing trap

Number 6 (Page 24)

Supervisory Convergence Plan for 2020

Number 7 (Page 26)

Cyber underwriting: In Brief

Number 8 (Page 28)

"Stronger Together" Cyber Europe 2020.

The EU Agency for Cybersecurity (ENISA), is pleased to announce that the Cyber Europe 2020 (CE2020) exercise will take place in June and focus on the theme of health.

Number 9 (Page 30)

The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections

Michael A. Specter, MIT, James Koppel, MIT, Daniel Weitzner, MIT

Internet Policy Research Initiative
Massachusetts Institute of Technology

Number 10 (Page 31)

The Atmosphere as Global Sensor

Fundamental science effort to explore if disturbances on earth can be sensed throughout the atmosphere

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. The national and economic security of the United States depends on the reliable and efficient functioning of critical infrastructure.

Since the United States made the Global Positioning System available worldwide, positioning, navigation, and timing (PNT) services provided by space-based systems have become a largely invisible utility for technology and infrastructure, including the electrical power grid, communications infrastructure and mobile devices, all modes of transportation, precision agriculture, weather forecasting, and emergency response.

Because of the widespread adoption of PNT services, the disruption or manipulation of these services has the potential to adversely affect the national and economic security of the United States. To strengthen national resilience, the Federal Government must foster the responsible use of PNT services by critical infrastructure owners and operators.

Sec. 2. Definitions. As used in this order:

(a) "PNT services" means any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof.

(b) "Responsible use of PNT services" means the deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government.

(c) "Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national

security, national economic security, national public health or safety, or on any combination of those matters.

(d) "PNT profile" means a description of the responsible use of PNT services — aligned to standards, guidelines, and sector-specific requirements — selected for a particular system to address the potential disruption or manipulation of PNT services.

(e) "Sector-Specific Agency" (SSA) is the executive department or agency that is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

The SSAs are those identified in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).

Sec. 3. Policy. It is the policy of the United States to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure.

The Federal Government must increase the Nation's awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services, and it must ensure critical infrastructure can withstand disruption or manipulation of PNT services.

To this end, the Federal Government shall engage the public and private sectors to identify and promote the responsible use of PNT services.

Sec. 4. Implementation. (a) Within 1 year of the date of this order, the Secretary of Commerce, in coordination with the heads of SSAs and in consultation, as appropriate, with the private sector, shall develop and make available, to at least the appropriate agencies and private sector users, PNT profiles.

The PNT profiles will enable the public and private sectors to identify systems, networks, and assets dependent on PNT services; identify appropriate PNT services; detect the disruption and manipulation of PNT services; and manage the associated risks to the systems, networks, and assets dependent on PNT services. Once made available, the PNT profiles shall be reviewed every 2 years and, as necessary, updated.

(b) The Secretary of Defense, Secretary of Transportation, and Secretary of Homeland Security shall refer to the PNT profiles created pursuant to

subsection (a) of this section in updates to the Federal Radionavigation Plan.

(c) Within 1 year of the date of this order, the Secretary of Homeland Security, in coordination with the heads of SSAs, shall develop a plan to test the vulnerabilities of critical infrastructure systems, networks, and assets in the event of disruption and manipulation of PNT services.

The results of the tests carried out under that plan shall be used to inform updates to the PNT profiles identified in subsection (a) of this section.

(d) Within 90 days of the PNT profiles being made available, the heads of SSAs and the heads of other executive departments and agencies (agencies), as appropriate, through the Secretary of Homeland Security, shall develop contractual language for inclusion of the relevant information from the PNT profiles in the requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services. The heads of SSAs and the heads of other agencies, as appropriate, shall update the requirements as necessary.

(e) Within 180 days of the completion of any of the duties described in subsection (d) of this section, and consistent with applicable law and to the maximum extent practicable, the Federal Acquisition Regulatory Council, in consultation with the heads of SSAs and the heads of other agencies, as appropriate, shall incorporate the requirements developed under subsection (d) of this section into Federal contracts for products, systems, and services that integrate or use PNT services.

(f) Within 1 year of the PNT profiles being made available, and biennially thereafter, the heads of SSAs and the heads of other agencies, as appropriate, through the Secretary of Homeland Security, shall submit a report to the Assistant to the President for National Security Affairs and the Director of the Office of Science and Technology Policy (OSTP) on the extent to which the PNT profiles have been adopted in their respective agencies' acquisitions and, to the extent possible, the extent to which PNT profiles have been adopted by owners and operators of critical infrastructure.

(g) Within 180 days of the date of this order, the Secretary of Transportation, Secretary of Energy, and Secretary of Homeland Security shall each develop plans to engage with critical infrastructure owners or operators to evaluate the responsible use of PNT services. Each pilot program shall be completed within 1 year of developing the plan, and the

results shall be used to inform the development of the relevant PNT profile and research and development (R&D) opportunities.

(h) Within 1 year of the date of this order, the Director of OSTP shall coordinate the development of a national plan, which shall be informed by existing initiatives, for the R&D and pilot testing of additional, robust, and secure PNT services that are not dependent on global navigation satellite systems (GNSS).

The plan shall also include approaches to integrate and use multiple PNT services to enhance the resilience of critical infrastructure. Once the plan is published, the Director of OSTP shall coordinate updates to the plan every 4 years, or as appropriate.

(i) Within 180 days of the date of this order, the Secretary of Commerce shall make available a GNSS-independent source of Coordinated Universal Time, to support the needs of critical infrastructure owners and operators, for the public and private sectors to access.

Sec. 5. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP
THE WHITE HOUSE,
February 12, 2020.

Number 2

Basel III: the implementation imperative

Keynote address by Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, at the 15th BCBS-FSI High-level Meeting for Africa on Strengthening financial sector supervision and current regulatory priorities, Cape Town.

Good morning, and welcome to the 15th BCBS-FSI High-level Meeting for Africa. Let me start by thanking Governor Kganyago and the South African Reserve Bank (SARB) for hosting this meeting in Cape Town.

As the global standard setter for banks, the Basel Committee places great importance on reaching out to a wide range of stakeholders to inform its work. Events such as these high-level meetings are of particular value to the Committee in seeking the views of central banks and supervisory authorities across different regions of the world.

With a population of over 1.2 billion and a median age of 19 years, Africa will play an increasingly important role in shaping the future world economy. The average annual GDP growth in Africa has exceeded the global average over the past several years, and six of the world's 10 fastest-growing economies hail from this continent.

These growth prospects are also reflected in Africa's banking systems, which are among the fastest-growing and most profitable of any region. During the period 2012–17, African banks' revenue grew at a compound annual rate of 11%, and these institutions are projected to continue to be among the fastest-growing banking systems over the coming years.

Indeed, with a retail banking penetration of just under 40% of GDP, there is incredible potential for African banks to continue to grow. And Africa has been at the forefront of using technology for banking services, long before "fintech" become a household term.

Whether it is established fintech companies such as Kenya's M-Pesa mobile money service or Nigeria's Interswitch digital payments – which were set up over 15 years ago – or more recent fintech startups, there are now over 250 active fintech companies operating in sub-Saharan Africa.

There is much that we can learn from Africa's rich history of fintech. But these tantalising prospects for Africa's banking systems will require a robust and resilient regulatory foundation. Such a foundation helps deliver

sustainable and healthy banking systems that can serve the real economies at all points of the financial cycle.

So, my remarks today will focus primarily on the imperative of implementing the Basel Committee's post-crisis reforms.

I'm pleased to note that the SARB takes this imperative seriously: it has a strong track record of implementing the Basel III standards in a timely and consistent manner.

And Governor Kganyago's chairmanship of the Financial Stability Board's Standing Committee on Standards Implementation underscores the SARB's commitment to this imperative.

I will frame my remarks around four questions:

(i) Why does implementation matter?
(ii) What has the Basel Committee done to meet the implementation imperative?
(iii) What have we seen to date among our members?
(iv) Where does this leave us?

To read more:
https://www.bis.org/speeches/sp200130.pdf

Number 3

Governance of financial globalisation

Sir Jon Cunliffe, Deputy Governor for Financial Stability of the Bank of England, at the German Economic Council Annual Finance Conference, Berlin.

Thank you for inviting me to address you today.

It is now nearly two weeks since the UK left the European Union.

Our status as a non-member of the EU, what is called a 'third country', is now quite clear.

The future relationship between the UK and the EU, of course, is not yet fixed. It will depend on the outcomes of the negotiation that has now commenced.

Those negotiations are for the UK government and the EU authorities and member states.

Our job as the Bank of England is to deliver monetary and financial stability within the mandates that are set for us.

So I will not – and indeed I could not – talk today about the trade negotiations or hazard guesses about the outcome.

But while we are not responsible for trade negotiations and while all decisions about the future relationship are for governments, the governance of the UK's financial links with the rest of the world, the EU included, is important to us given our responsibility for financial stability in the UK.

I want to talk today in part about the governance of financial globalisation, the progress we have made, and the challenges we face.

That is a subject that is crucially important to the UK and to the EU, given our integration into the global economy.

Financial globalisation – an integrated global capital market and cross-border financial services – mean that our economies can benefit from better matching of saving and investment, from greater choice and from risk sharing and diversification.

But, of course, it also means that we import and export financial risk from across borders.

We saw just over a decade ago the damage that can come from financial globalisation if we do not have appropriate governance at the international level.

This question of governance, and of the import and export of financial risk, is a subject of crucial importance to me, and not just because I am still scarred by the great financial crisis.

I am Deputy Governor for Financial Stability at the Bank of England. We are responsible for the largest and I think most complex international financial centre in the world.

And I also want today to talk specifically, from the particular perspective of financial stability about how, in the light of the current governance of financial globalisation, we build the new arrangements for the governance of the financial sector connections between the EU and the UK.

Governance of financial globalisation

I have used the word "governance". The word is of course closely related to the word "government". But while related, they are not the same thing.

We can have governance of the global financial system even though we do not have global government.

Governance can mean legislation, regulation and the institutions of government. But it also encompasses broader frameworks of standards, norms and conventions, international organisations and agreements that fall short of hard law.

Indeed, in a world of nation states and national legislatures and governments, it is on these broader frameworks that we need to depend for the governance of financial globalisation, and the management of cross border risk.

This challenge is not of course confined to the financial sector. International governance structures are required in many economic and

non-economic spheres. But since the liberation of global capital flows and liberalisation of international financial markets which began 50 years ago, financial authorities in multiple jurisdictions have sought together to build the necessary governance frameworks to enable the benefits of financial globalisation while managing the risks.

The first Basel Banking Accords of the early 1980s were motivated by the need to ensure that banks involved in cross border services were made subject by their home authorities to minimum standards.

In other words, to ensure that the benefits of cross border flows were accompanied by assurance on the risks that might be imported.

Financial globalisation accelerated through the last decade of the last century and up until the great financial crisis. External financial assets and liabilities increased from 60% of GDP in the 1980s to 400% of GDP in 2008.

In advanced economies, this was 6 times the level of exports and imports as a % of GDP.

This helped to drive unprecedented growth and poverty reduction in the global economy, with the share of the world population living extreme poverty falling over 60% since the 1980s. But financial globalisation also gave rise to a series of regional capital and financial crises that exposed the risks; and the international governance structures did not keep up.

It took the great financial crisis and the near-death experience of the global economy to bring home the lesson that a step change in governance was needed. And to create the political will to make it happen.

To read more:
https://www.bis.org/review/r200211e.pdf

Number 4

Spontaneity and order - transparency, accountability and fairness in bank supervision

Randal K Quarles, Vice Chair for Supervision of the Board of Governors of the Federal Reserve System, Yale Law School, New Haven, Connecticut.

It's a great pleasure to be with you today at Yale Law School to deliver this Dean's Lecture.

I first arrived here at the Yale Law School on a sunny September afternoon almost 40 years ago, and I have a very clear memory of the first time I sat in this hall, not long after, to hear a lecture from a worthy public servant come to deliver wisdom to those who thought they might one day follow in his footsteps.

It was Gene Rostow, former Dean of the Law School, former Under Secretary of State, then serving as head of the Arms Control and Disarmament Agency in the Reagan Administration. I remember the impression of erudition and experience he conveyed. I remember the sense of tradition, sitting here in these wood-paneled surroundings, being addressed with respect on issues of consequence.

There was a sense then, in the early 1980's-which turned out to be correct - that the Cold War could be reaching its climax, and widespread concern among the great and good in the country (not least among them the Yale Law School faculty) that the more aggressive stance of the Reaganites (not least among them Gene Rostow) greatly increased the odds of a miscalculation. And here was the man himself, patiently but boldly discussing the state of the world with a group of first-year law students.

I remember that he referred more than once to Don Quixote, and this Brooklyn-born American pronounced it in the British way-Dun Quixit-which I found oddly both affected and endearing at the same time. And I remember absolutely nothing else of what he said. Not a word. Which puts me in a properly humble frame of mind for my own remarks today.

You won't remember for very long anything I say here today, but I hope your time at the Law School gives you the same experience of patiently but boldly examining matters of consequence that I found to be the most valuable and lasting legacy of my own time here in New Haven.

The themes and goals of this speech are objectives I will be pursuing over the next year and should resonate for this audience. I trust they will be helpful to you all and foster further discussions about the importance of transparency, accountability, and fairness in regulation generally and also in the increasingly important and increasingly consequential topic of bank supervision.

Twenty years ago when I was in private practice, a lecture on bank supervision would have been my cue to pull out my BlackBerry and start checking my emails.

The structure and content of regulation was both intellectually interesting and professionally meaningful; I considered bank supervision, by contrast, as both too workaday and too straightforward to merit the commitment of much legal horsepower or personal attention. I could perhaps have been excused by the callowness of youth, yet it was a common view at the time.

Having now been immersed for the last two years both in the practice of supervision and in the complementary relationship between the regulatory and supervisory processes, I realize that this wasn't true then, and is certainly not true now.

It is not a drafting accident that the Dodd Frank Act gave my position at the Federal Reserve the title of Vice Chairman for Supervision.

Notwithstanding the extensive reform of bank regulation after the crisis, which has had much consequence for the industry (most of it salutary), it is the process of examination and supervision that constitutes the bulk of our ongoing engagement with the industry and through which our policy objectives are given effect.

This division of labor is important for lawyers and policymakers to think about deeply because the processes of regulation and supervision are necessarily different in crucial respects. Regulation establishes a binding public framework implementing relevant statutory imperatives.

Because a rule is designed to apply generally, rules must be based on general principles intended to achieve general aims, rather than reverse-engineered to generate specific effects for specific institutions.

Given their general applicability, there must be a general process for all those with an interest-industry, academics, citizens, Congress-to have notice of, and opportunity to comment on all rules, ensuring that all potential effects and points of view are taken into account in the rule's crafting. And given their general function, rules must be clear and public: those affected must know what to expect and what is expected.

Supervision, by contrast, implements the regulatory framework through close engagement with the particular facts about particular firms: their individual capital and liquidity positions, the diverse composition of their distinct portfolios of assets, their business strategies, the nature of their operations, and the strengths and weaknesses of their management.

Bank supervisors review and analyze bank information and interact with bank management, enabling them to make necessary judgments about the bank's safety and soundness.

Much of the granular information used by supervisors is, accordingly, proprietary and confidential, and many of their judgments and decisions are closely tailored to specific circumstances.

Given the strong public interest in the safe, sound, and efficient operation of the financial industry and the potential for hair-raising and widespread adverse social consequences of private misjudgment or misconduct in that industry, close and regular supervision of this sort can help us all sleep restfully.

Yet, the confidential and tailored nature of supervision sits uncomfortably with the responsibilities of government in a democracy. In the United States, we have a long-standing, well-articulated framework for ensuring that regulations conform with the principles of generality, predictability, publicity, and consultation described above.

Supervision-for good reason, in my view-is not subject to this formal framework. But it is currently not subject to any specific process constraint promoting publicity or universality. This leaves it open to the charge, and sometimes to the fact, of capriciousness, unaccountability, unequal application, and excessive burden.

Here, then, is a conundrum. We have a public interest in a confidential, tailored, rapid-acting, and closely informed system of bank supervision.

And we have a public interest in all governmental processes being fair, predictable, efficient, and accountable. How do we square this circle? In my

time with you today, we will not do more than scratch the surface of this question.

It is a complex and consequential issue that, for decades now, has received far too little attention from practitioners, academics, policymakers, and the public.

Evaluating this question will be a significant focus of mine going forward, and I hope that there will be much discussion in many fora from which we at the Fed, and at other regulators, can learn.

So today, I simply want to open the exploration of some these conceptual issues, and then offer some specific suggestions-by no means comprehensive-on some obvious and immediate ways that supervision can become more transparent, efficient, and effective.

The Importance of Transparency

Let me begin by delving a little more deeply into the distinction between regulation and supervision and the process applicable to both. In granting to agencies such as the Fed the significant power to write regulations, Congress has codified a regulatory process that emphasizes transparency.

This process was born in the 1930s, in the tumult of government expansion that was the New Deal, when Congress began a decade-long debate over how to manage the new regulatory state. The result was the Administrative Procedure Act (APA).

The APA continues to serve as the basis for the public disclosure and participation required for agency rule-writing and for the judicial review affected parties are guaranteed to challenge rules.

This transparency is intended to prevent arbitrary, capricious, and thus ineffective regulation by inviting broad public participation and mandating a deliberate public debate over the content of proposed rules.

One obvious purpose of this transparency is to provide clarity and predictability: it helps make clear how agencies are considering exercising their discretion. The significant process protections in laws such as the APA are also meant to ensure fairness.

The wisdom behind this approach is that fairness both helps bring forth more considered and effective regulations and builds respect for and adherence to the law, which is essential for enforcement. Transparency is central to our ability to assert that our rules are fair.

Not everything that government does, however, can be accomplished in exactly the same way that regulations are written. One of these things is bank supervision.

Bank Supervision

Banks are subjected to supervision, in addition to regulation, as an additional form of government oversight because of their complexity, opacity, vulnerability to runs, and indispensable role in the economy, enabling payments, transmitting monetary policy, and providing credit.

The government provides a safety net to banks in the form of deposit insurance, and in return, banks are subject to government oversight that mimics some of the monitoring that the private sector would provide, absent the government safety net.

The bank regulatory framework sets the core architectural requirements for the banking system, but it isn't enough to set the rules and walk away like Voltaire's god.

The potential consequences of disruption in the financial system are so far-reaching, and the erosion of market discipline resulting from the government safety net sufficiently material, that it is neither safe nor reasonable to rely entirely on after-the-fact enforcement to ensure regulatory compliance.

Supervisors are in a good position to monitor individual firms' idiosyncratic risks. And in addition to what they do at individual banks, supervisors monitor for risk that may be building among clusters of banks or across the banking system.

These "horizontal" exams across multiple banks help highlight new or emerging risks and help examiners understand how banks are managing these risks.

Through their engagement with banks, supervisors promote good risk management and thus help banks preemptively avert excessive risk taking that would be costly and inefficient to correct after the fact.

Where banks fall materially out of compliance with a regulatory framework or act in a manner that poses a threat to their safety and soundness, supervisors can act rapidly to address the failures that led to the lack of compliance or threat to safety and soundness.

This is a crucial point: supervision is most effective when expectations are clear and supervision promotes an approach to risk management that deters bad behavior and decisions by banks. Clearly communicating those expectations is essential to effective supervision, and in a larger sense, clear two-way communication is the essence of effective supervision.

Supervisors rely on banks to be frank and forthcoming, and supervisors in turn can help secure that frankness by explaining what their expectations are and why their expectations are reasonable, not arbitrary or capricious.

Greater transparency in supervision about the content of our expectations and about how we form our expectations and judgments can make supervision more effective by building trust and respect for the fairness and rationality of supervision.

I don't believe the Federal Reserve has communicated as clearly as it could with the banks we supervise. More transparency and more clarity about what we want to achieve as supervisors and how we approach our work will improve supervision, and I have several specific proposals, which I have discussed in more detail than I will get into today and plan to implement expeditiously.

Broadly speaking, these actions fall into three categories:

(1) large bank supervision,
(2) transparency improvements, and
(3) overall supervisory process improvements.

Let me briefly touch on some of the specific changes I will pursue, and which flow from the themes I have just discussed. And as a disclaimer, I should note that previously I have mentioned more specifics, so this abbreviated list should not be taken as a ranking or indication that certain ideas have fallen out of favor.

First, I would mention that we should pursue a clear and transparent standard that aligns our supervisory portfolios, and by extension the intensity of our supervision, with categories established in our recent regulatory tailoring rules. Last fall, we completed a cornerstone of the recent banking legislation to tailor our rules for large banks.

This change would be entirely consistent with a principle at the heart of our existing work: Firms that pose greater risks should meet higher standards and receive more scrutiny.

To carry forward this work aligning supervision with the regulatory tailoring rules, I believe there is a compelling justification to make changes today to the composition of foreign banks in our portfolio of the largest banks, known as LISCC.

Second, as I have discussed throughout my time at the Board, I continue to look for ways to make our stress tests more transparent without making them game-able and without diluting their potency as a supervisory tool. I expect that we will continue to provide more transparency on the models we use for the stress tests, and on the hypothetical scenarios.

Additionally, I am advocating changes to our capital plan rule that will allow banks to receive and study their supervisory stress testing results prior to submitting their capital plans. Currently, banks have a very limited time to adjust their capital distribution plans and only under limited circumstance.

Third, and principally as a transparency endeavor, I would endorse creating a word-searchable database on the Board's website with the historical interpretations by the Board and its staff of all significant rules.

Regulatory interpretations by Board staff have grown piecemeal over the decades and haven't consistently been treated as the valuable resource they are. The Board's website has select interpretations of many laws but does not provide a comprehensive, user-friendly collection of regulatory interpretations, FAQs, and commentary.

Fourth, I endorse putting significant supervisory guidance out for public comment. The Board already invites comments on its regulations, as required under the APA, and regularly invites comment on some supervisory guidance and statements of policy.

This practice of seeking comment on significant guidance leads to better, more informed supervision and better engagement by banks.

And fifth, the Board should adopt a rule on how we use guidance in the supervisory process. I would expect the rule to state that the Board will follow and respect the limits of administrative law in carrying out its supervisory responsibilities.

In particular, consistent with the September 2018 interagency statement on guidance, we would affirm the sensible principles that guidance is not binding and "non-compliance" with guidance may not form the basis for an enforcement action (such as a cease-and-desist order) or supervisory criticism (such as a Matter Requiring Attention (MRA)).

This rule would be binding on the Board and on all staff of the Federal Reserve System, including bank examiners.

There are of course other ideas I have mentioned and will be pursuing, but this partial list should be informative and helpful in illustrating the earlier themes I mentioned.

Conclusion

The changes to supervision since the crisis have made the financial system stronger and more resilient than it was before. The incremental changes I am considering, to increase transparency, accountability, and fairness, would make supervision more efficient and effective, and our financial system stronger and more stable.

Obviously, the incremental changes to our supervisory processes I am considering do not completely answer the question with which I began my remarks today: how can we square the public interest in agile supervision with the public interest in transparency and accountability?

This should be an ongoing question of high priority, both at the Fed and more broadly among those who care about our system of financial regulation.

Equally obviously, however, these suggestions would strengthen our practice of supervision and increase the vigor and credibility of our supervisors.

Number 5

Attackers using the Coronavirus as a phishing trap

National Cyber Security Centre

The coronavirus outbreak is being used in phishing attacks according to researchers at Proofpoint.

Attackers are taking advantage of the widespread concern about the virus to lure people into phishing traps using conspiracy theories about "unreleased" cures.

One example describes a 'confidential cure solution' before giving users the option to follow a link through to a fake website asking for credentials.

Proofpoint's report has other examples of phishing traps being utilized – you may visit:
https://www.proofpoint.com/us/corporate-blog/post/attackers-expand-coronavirus-themed-attacks-and-prey-conspiracy-theories

Phishing attacks are untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Unfortunately, it is relatively common for cyber criminals to take advantage of situations like the coronavirus outbreak to prey upon people's concerns. If you want to learn more about spotting and dealing with phishing emails, then the NCSC's suspicious email advice is well worth reading at:
https://www.ncsc.gov.uk/guidance/suspicious-email-actions

Number 6

Supervisory Convergence Plan for 2020

Convergence of supervisory practices should be built on a common interpretation of laws and regulations, and without prejudice to the application of supervisory judgment or the proportionality principle.

One of the main goals of the European Insurance and Occupational Pensions Authority (EIOPA) is to ensure a high, effective and consistent level of supervision across Europe.

Convergence of supervisory practices is not only achieved or assessed by outputs, i.e. by the number, quality and impact of opinions or assessments. Convergence is also about working together.

The process of developing common benchmarks for supervisory practices, performing reviews and engaging in challenging interactions in itself leads to supervisory convergence. Supervisory convergence does not mean a full harmonisation of the supervisory framework.

NCAs may need to tailor the approach by considering the national specificities of their markets.

Therefore, to achieve a high, effective and consistent level of supervision across Europe, EIOPA identified supervisory convergence as its main strategic goal for the years to come.

Supervisory convergence work is a collective effort by all NCAs and EIOPA staff to deliver on this strategic goal.

Common supervisory culture

As with any strong structure, the framework of supervisory convergence needs to be built upon clear, well-known and commonly understood foundations.

EIOPA's booklet, A common supervisory culture — Key characteristics of high quality and effective supervision, was the first step in building this framework.

The booklet defines the following five key characteristics of high-quality and effective supervision: risk-based and proportionate, forward-looking, preventive and proactive, challenging, sceptical and engaged, comprehensive and conclusive.

A common supervisory culture cannot be built overnight. It is a long journey where, step by step, by working together, being focused and challenging each other along the way, supervisors will build a strong and fair supervisory culture that promotes consumer protection and enhances the stability of the financial system for the benefit of Europe's business, economy and citizens.

As processes and procedures are easier to align than behaviour, convergence will occur at different paces.

The implementation of a common supervisory culture requires change.

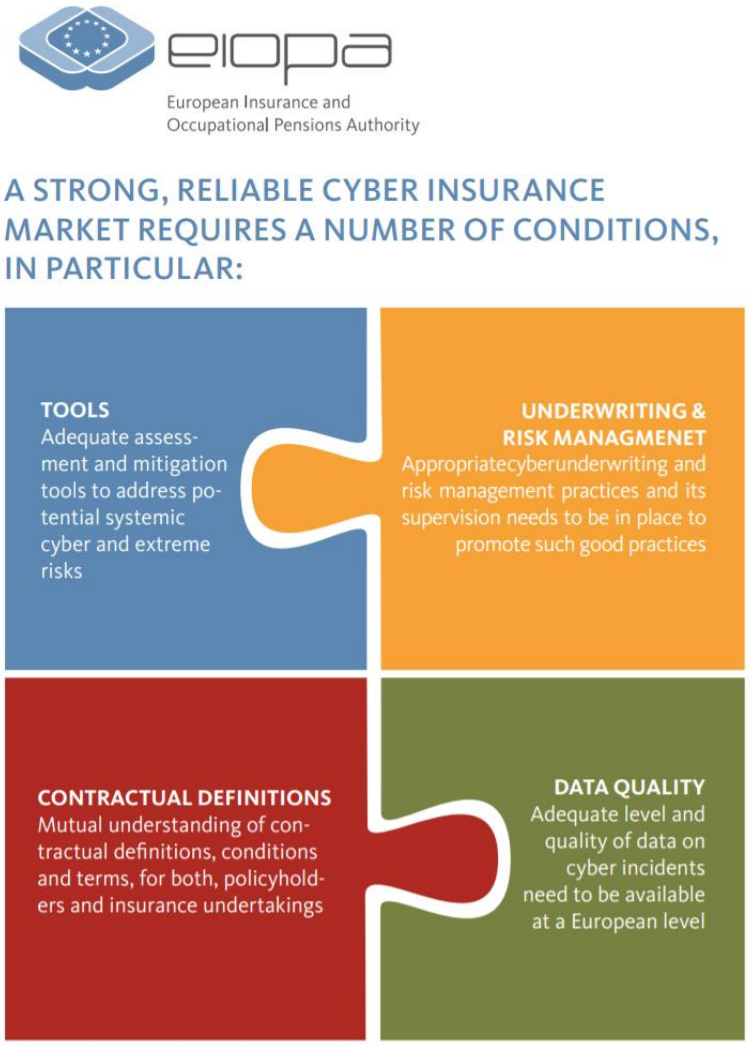
Going forward it is important to consider different and innovative tools, such as cooperation within supervisory networks and specific cooperation platforms to share information and experiences within the supervisory community.

It is of utmost importance that the supervisory community has, at all levels, easy access to EIOPA tools as well as the ability and willingness to use them.

To read more:
https://www.eiopa.europa.eu/content/supervisory-convergence-plan-2020_en

Number 7

Cyber underwriting: In Brief



Cyber risk is a top risk for many businesses. Digitalisation of the economy makes it one of the main sources of operational risk faced by organisations.

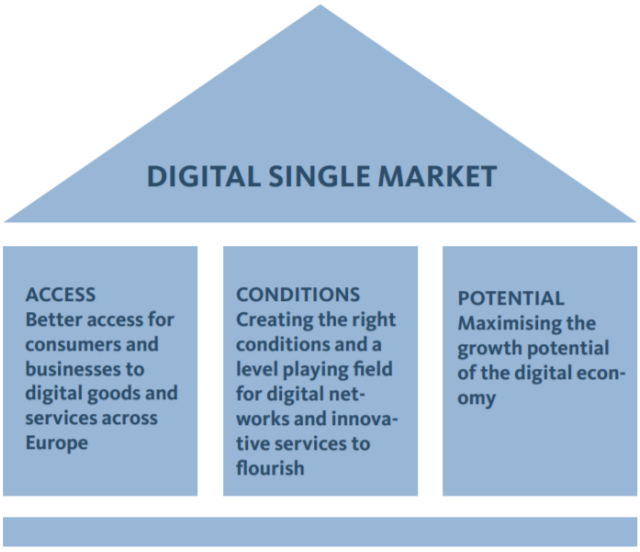
The increasing frequency and sophistication of cyber attacks and the continued digital transformation also make insurers increasingly vulnerable to cyber threats, as more and more insurers embrace new technologies and make use of big data.

This needs to be done while safeguarding financial stability, market integrity and investors' protection.

EIOPA aims at promoting sound technological progress for the benefit of the European Union economy and its citizens.

Monitoring cyber threats and ensuring robust resilience through a well-developed European cyber insurance market is a strategic priority for EIOPA.

EIOPA's strategic priorities take into account the European Commission's Digital Strategy, Cybersecurity Strategy and FinTech Action Plan and support its ambition for a Digital Single Market.



The Digital Single Market is built on 3 pillars.

EIOPA works closely with national supervisors, industry and other stakeholders to identify risks and trends, including best practices, related to cyber security.

EIOPA also works closely with the other European Supervisory Authorities on this issue. EIOPA's strategy for cyber underwriting is an essential part of its work on cyber risks and insurance, and essential for building overall resilience at European level.

EIOPA's supervisory and regulatory priorities in cyber risk are:

- Appropriate cyber underwriting and cyber risk management practices and how its supervision needs to be in place to promote such good practices.
- Adequate assessment and mitigation tools to address potential systemic cyber and extreme risks.

To read more:
https://www.eiopa.europa.eu/content/cyber-underwriting-brief_en

Number 8

"Stronger Together" Cyber Europe 2020.

The EU Agency for Cybersecurity (ENISA), is pleased to announce that the Cyber Europe 2020 (CE2020) exercise will take place in June and focus on the theme of health.

Cyber Europe 2020 is the sixth large-scale pan-european cyber exercise facilitated by the EU Agency for Cybersecurity (ENISA). This year marks 10 years of cybersecurity exercises in Europe, a milestone for this unique initiative.

Keeping Europe safe is a shared responsibility. In this spirit the exercise aims to build cybersecurity capacities, strengthen EU cooperation and increase cybersecurity awareness and preparedness in the healthcare sector.

The participation to the exercise is open; if you are interested in getting involved you can find more information here:

Cyber Europe official website:
https://www.cyber-europe.eu/

ENISA Cyber Europe webpage:
https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2020/

For any question on the Cyber Europe 2020 exercise, please contact:
exercises@enisa.europa.eu

To read more:
https://www.cyber-europe.eu/img/CE2020_presentation.pdf

Number 9

The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections

Michael A. Specter, MIT, James Koppel, MIT, Daniel Weitzner, MIT

Internet Policy Research Initiative
Massachusetts Institute of Technology

In the 2018 midterm elections, West Virginia became the first state in the U.S. to allow select voters to cast their ballot on a mobile phone via a proprietary app called "Voatz."

Although there is no public formal description of Voatz's security model, the company claims that election security and integrity are maintained through the use of a permissioned blockchain, biometrics, a mixnet, and hardware-backed key storage modules on the user's device.

In this work, we present the first public security analysis of Voatz, based on a reverse engineering of their Android application and the minimal available documentation of the system.

We performed a cleanroom reimplementation of Voatz's server and present an analysis of the election process as visible from the app itself.

We find that Voatz has vulnerabilities that allow different kinds of adversaries to alter, stop, or expose a user's vote, including a side channel attack in which a completely passive network adversary can potentially recover a user's secret ballot.

We additionally find that Voatz has a number of privacy issues stemming from their use of third party services for crucial app functionality.

Our findings serve as a concrete illustration of the common wisdom against Internet voting, and of the importance of transparency to the legitimacy of elections. To read more: https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

Number 10

The Atmosphere as Global Sensor

Fundamental science effort to explore if disturbances on earth can be sensed throughout the atmosphere

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Sensors are usually thought of in terms of physical devices that receive and respond to electromagnetic signals – from everyday sensors in our smartphones and connected home appliances to more advanced sensors in buildings, cars, airplanes and spacecraft.

No physical sensor or aggregation of electronic sensors, however, can continuously and globally detect disturbances that take place on or above the earth's surface. But the physical atmosphere itself may offer such a sensing capability, if it can be understood and tapped into.

To that end, DARPA recently announced its Atmosphere as a Sensor (AtmoSense) program, whose goal is to understand the fundamentals of energy propagation from the ground to the ionosphere to determine if the atmosphere can be used as a sensor.

A Proposers Day was scheduled for February 14, 2020, in Arlington, Virginia.

It's well known that energy propagates from the Earth's surface to the ionosphere, but the specifics of how that happens is not currently known enough to use the atmosphere as a sensor.

Scientific literature has clearly documented that events like thunderstorms, tornadoes, volcanos, and tsunamis make big "three-dimensional wakes" that propagate to the upper reaches of the ionosphere and leave a mark there.

Since that energy traverses several other layers of atmosphere – the troposphere, stratosphere, and mesosphere – on its way up to the ionosphere, the idea is to try and identify the disturbances the "wake" is making along its way to see if researchers can capture information to indicate what type of event caused it.

"Maybe I don't have to directly observe events like an earthquake or tsunami," said Air Force Major C. David Lewis who is the AtmoSense program manager in DARPA's Defense Sciences Office.

"Perhaps I can learn what occurred from information in the atmosphere. I want to find out how much information is available, and if I can disaggregate the signal I'm interested in from other natural phenomena creating noise in the background."

The AtmoSense program seeks proposers from the atmospheric science community, who have extensive experience in atmospheric modeling and simulation.

Also of interest are experts offering very unique ways to measure atmospheric properties, such as the basic PV=nRT variables – pressure, volume, density, temperature, or derivatives of such.

Beyond these basic atmospheric variables, the mesosphere and lower ionosphere provide electromagnetic opportunities for measurement due to their charged nature.

"We typically model, simulate, and measure properties in the troposphere, which is where terrestrial weather happens," Lewis said. "But we don't really make those measurements in the stratosphere or the mesosphere, or the bottom part of the ionosphere, because no one has really been keenly interested in it and it's hard to get up there.

Sometimes the mesosphere is even called the 'ignorosphere,' but we know that information traverses it, so we're really looking for scientists and engineers with unique ways of potentially measuring different aspects of the atmosphere."

Another key area for the program is measuring and understanding background noise that weakens or destroys signals of interest.

"When we think about the possible background entropy, there are jet streams, compression of the fluid, shear forces, Coriolis forces, etc.; all those things trigger some sort of turbulence that destroys information," Lewis said.

"When it comes to geophysical and meteorological sources of atmospheric disturbance there's a frequency spectrum emitted from infrasound all the way up to the ultrasound. Some of those frequencies are more immune to atmospheric entropy than others, and those are what we'd like to capture."

The program calls for two phases. The first phase is concept development (27 months), and the second phase is proof of principle field testing (12 months).

If successful, AtmoSense could enable new ways in the future to identify and give insight into events such as earthquakes, tsunamis, storms, tornados, and asteroid activity.

For details on the Atmosense Proposers Day you may visit:
https://go.usa.gov/xd843
A Broad Agency Announcement solicitation is expected to be posted on beta.SAM.gov in the coming weeks.

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.

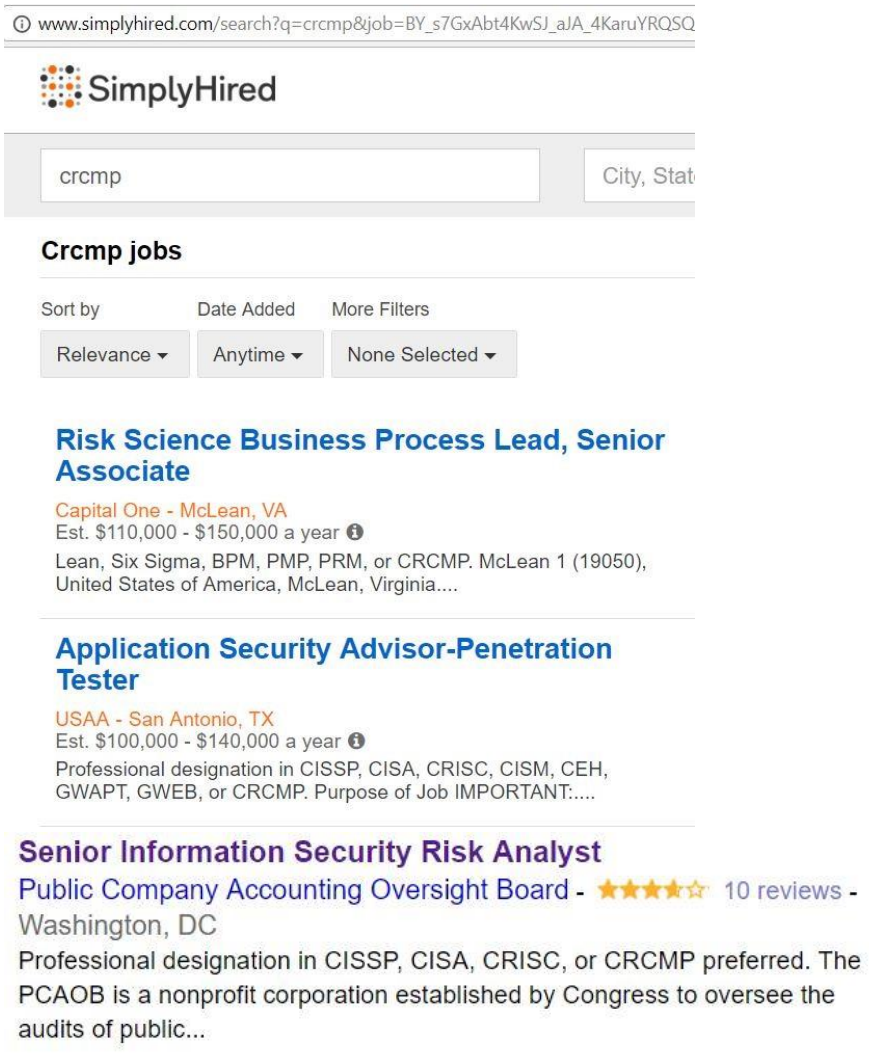
International Association of Risk and Compliance Professionals

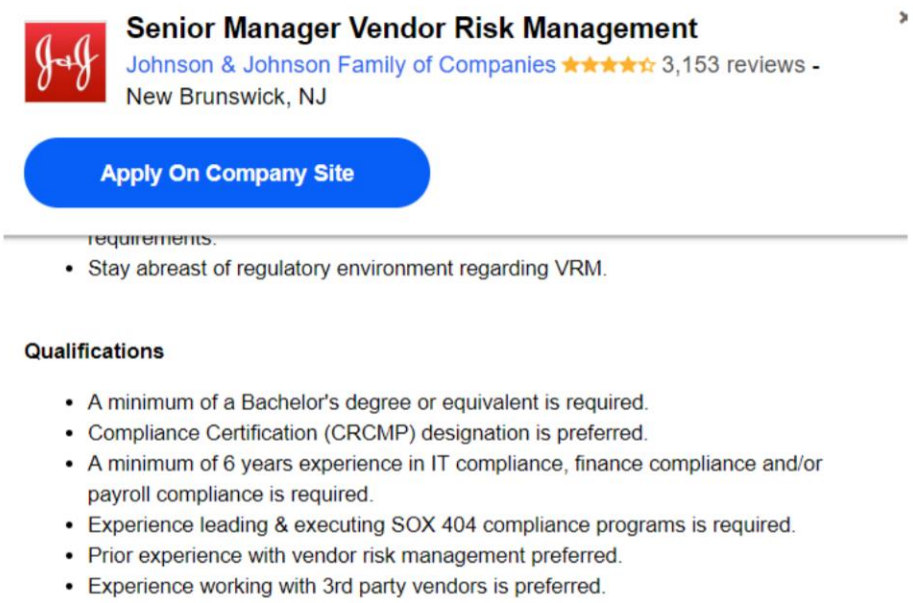
You can explore what we offer to our members:

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