International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW, Suite 800, Washington DC 20005-6705 USA
Tel: 202-449-9750 www.risk-compliance-association.com

Monday, March 5, 2018

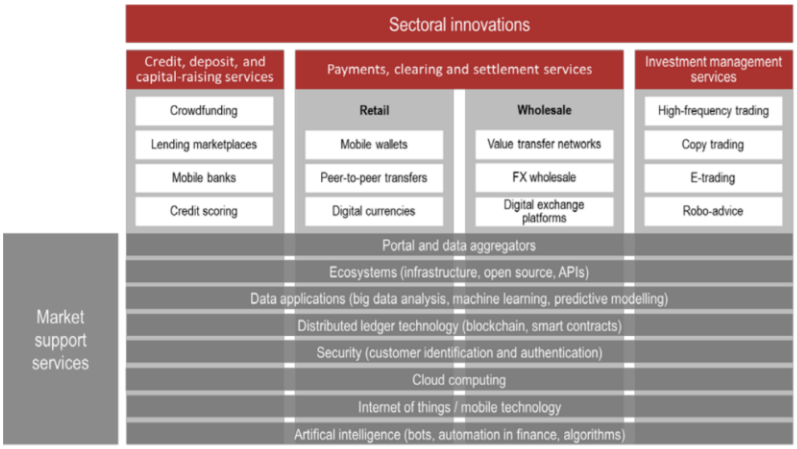
Top 10 risk and compliance management related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

What is fintech?

The Basel Committee has opted to use the Financial Stability Board's working definition for fintech as "technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services".

Graph 1: Sectors of innovative services



Source: BCBS.

The Basel Committee also used a categorisation of fintech innovations.

Graph 1 depicts three product sectors, as well as market support services.

The three sectors relate directly to core banking services, while the market support services relate to innovations and new technologies that are not specific to the financial sector but also play a significant role in fintech developments.

The results of a comparative survey on supervisory approaches indicate that most surveyed agencies have not formally defined fintech, innovation or other similar terms. Some of the reasoning provided for this lack of formal definitions was that other definitions already exist, or that it would be premature to more narrowly define a field that is rapidly evolving.

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 8)

Sound Practices: implications of fintech developments for banks and bank supervisors, February 2018

BANK FOR INTERNATIONAL SETTLEMENTS

The Sound Practices on the implications of fintech developments for banks and bank supervisors assesses how technology-driven innovation in financial services, or "fintech", may affect the banking industry and the activities of supervisors in the near to medium term.

Various future potential scenarios are considered, with their specific risks and opportunities. In addition to the banking industry scenarios, three case studies focus on technology developments (big data, distributed ledger technology and cloud computing) and three on fintech business models (innovative payment services, lending platforms and neo-banks).

Number 2 (Page 10)

Reflections on leadership in a disruptive age

Mark Carney, Governor of the Bank of England and Chairman of the Financial Stability Board, at Regent's University, London.

“I was asked to reflect tonight on leadership and values. This is somewhat dangerous territory, and certainly one that creates a target-rich environment for critics who can spot gaps between preaching and practising.
Indeed, a review of a recent book on leadership and values suggested that it’s very publication signaled overconfidence – the complacency before the storm – and cautioned that CEOs and investors ought to be wary of the ‘curse of authorship’.”

Number 3 (Page 12)

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Ronald S. Ross, Patrick Viscuso, Gary Guissanie, Kelley L. Dempsey, Mark Riddle

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

The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations.

This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI.

Number 4 (Page 13)

Security Recommendations for Hypervisor Deployment on Servers

Ramaswamy Chandramouli, Computer Security Division
Information Technology Laboratory

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

The Hypervisor is a collection of software modules that provides virtualization of hardware resources (such as CPU/GPU, Memory, Network and Storage) and thus enables multiple computing stacks (basically made of an OS and Application programs) called Virtual Machines (VMs) to be run on a single physical host.

Number 5 (Page 14)

EBA launches 2018 EU-wide stress test exercise

The European Banking Authority (EBA) launched its 2018 EU-wide stress test and released the macroeconomic scenarios.

The adverse scenario implies a deviation of EU GDP from its baseline level by 8.3% in 2020, resulting in the most severe scenario to date. The EBA expects to publish the results of the exercise by 2 November 2018.

The stress test is designed to provide supervisors, banks and other market participants with a common analytical framework to consistently compare and assess the resilience of EU banks to economic shocks. For the first time, it incorporates IFRS 9 accounting standards. No pass-fail threshold has been included as the results of the exercise are designed to serve as an input to the Supervisory Review and Evaluation Process (SREP).

Number 6 (Page 16)

Market-based finance - a macroprudential view

Sir Jon Cunliffe, Deputy Governor for Financial Stability of the Bank of England, at the Asset Management Derivatives Forum, Dana Point, California.

"In 1849 Thomas Carlyle branded economics as the 'dismal science'. That was almost certainly unfair. But unfair or not, the tag has undeniably stuck fast; the public's perception of economists is that it is a gloomy profession."

Number 7 (Page 18)

Former employee jailed for intentionally damaging computer network

National Cyber Security Centre
a part of GCHQ

A disgruntled former Canadian Pacific Railway (CPR) employee was sentenced last week to a year in prison for intentionally causing damage to CPR's computer network.

In December 2015, the employee resigned from CPR after being informed that he would be fired for insubordinate behaviour. However, before returning his laptop and remote access authentication token to the organisation, the disgruntled individual accessed CPR's core computer network switches, through which critical data flows.

He strategically deleted files, removed admin accounts or changed their passwords, returning the laptop after wiping its hard drive of any evidence of his actions.

Number 8 (Page 19)

India City Union Bank SWIFT Related Attack

National Cyber Security Centre
a part of GCHQ

In the last week, the Russian Central Bank reported that an undisclosed Russian bank was targeted in late 2017 in a SWIFT related cyber attack.

Since then, India City Union Bank reported that they had suffered a SWIFT fraud style incident over the weekend.

Some local reporting suggested that insider activity led to the heist, however this has been denied by India City Union Bank. They stated that they had been attacked by "international cyber-criminals and there is no evidence of internal staff involvement".

Number 9 (Page 20)

Increasing Product Complexity: What's at Stake?

Commissioner Kara M. Stein, remarks at SEC Speaks

"It's my understanding that this is the 47th year of SEC Speaks. Much has changed in our capital markets since 1972. Computers now allow investors to access a myriad of investment options from common equity to complex financial instruments within minutes.

Both large and small investors have more investment options at their fingertips—and I mean that literally—than ever before."

Number 10 (Page 23)

DARPA Seeks to Expand Real-Time Radiological Threat Detection to Include Other Dangers

Building on SIGMA's advanced capability to sniff out illicit radioactive and nuclear materials, SIGMA+ program aims to create additional sensors and networks to detect biological, chemical, and explosives threats

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Advanced commercially available technologies—such as additive manufacturing (3-D printing), small-scale chemical reactors for pharmaceuticals, and CRISPR gene-manipulation tools—have opened wide access to scientific exploration and discovery.

In the hands of terrorists and rogue nation states, however, these capabilities could be misused to concoct chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) weapons of mass destruction (WMD) in small quantities and in form factors that are hard to detect.

Number 1

Sound Practices: implications of fintech developments for banks and bank supervisors, February 2018

BANK FOR INTERNATIONAL SETTLEMENTS

The Sound Practices on the implications of fintech developments for banks and bank supervisors assesses how technology-driven innovation in financial services, or "fintech", may affect the banking industry and the activities of supervisors in the near to medium term.

Various future potential scenarios are considered, with their specific risks and opportunities. In addition to the banking industry scenarios, three case studies focus on technology developments (big data, distributed ledger technology and cloud computing) and three on fintech business models (innovative payment services, lending platforms and neo-banks).

Against this backdrop, current observations suggest that although the banking industry has undergone multiple innovations in the past, the rapid adoption of enabling technologies and emergence of new business models pose an increasing challenge to incumbent banks in almost all the banking industry scenarios considered.

In addition, the Committee surveyed its members' frameworks and practices in relation to fintech matters, and carried out a public consultation in August 2017.

Building on the supportive feedback, the Committee has further specified the nature and scope of its contribution and has enhanced its 10 key implications and considerations on the following supervisory issues:

- the overarching need to ensure safety and soundness and high compliance standards without inhibiting beneficial innovation in the banking sector

- the key risks for banks related to fintech developments, including strategic/profitability risks, operational, cyber- and compliance risks

- the implications for banks of the use of innovative enabling technologies

- the implications for banks of the growing use of third parties, via outsourcing and/or partnerships

- cross-sectoral cooperation between bank supervisors and other relevant authorities

- international cooperation between bank supervisors

- adaptation of the supervisory skill set

- potential opportunities for supervisors to use innovative technologies ("suptech")

- relevance of existing regulatory frameworks for new innovative business models

- key features of regulatory initiatives set up to facilitate fintech innovation

To read more:
https://www.bis.org/bcbs/publ/d431.pdf

Number 2

Reflections on leadership in a disruptive age

Mark Carney, Governor of the Bank of England and Chairman of the Financial Stability Board, at Regent's University, London.

Introduction

I was asked to reflect tonight on leadership and values. This is somewhat dangerous territory, and certainly one that creates a target-rich environment for critics who can spot gaps between preaching and practising.

Indeed, a review of a recent book on leadership and values suggested that it's very publication signaled overconfidence – the complacency before the storm – and cautioned that CEOs and investors ought to be wary of the 'curse of authorship'.

There are countless examples of pride coming before the fall in finance.

Think of those who dubbed the period before the Global Financial Crisis the 'Great Moderation'. Or the four most expensive words in the English language.

But, because we can learn from experience, and because leadership lies at the heart of Regent's University's mission- literally 'Developing tomorrow's global leaders' - I will forge ahead.

I will begin by reviewing the main activities of leaders and the core attributes of leadership. I will try to address what leadership is and isn't and whether it's inherent or can be developed.

I will conclude with some perspectives on the challenges and opportunities you will face leading in our disruptive age.

Leadership Activities

It's important to distinguish between what leaders do and who they are. Of the many things leaders must do, I would emphasise three:

1. Finding and developing the right people;
2. Setting priorities; and
3. Catalysing action.

To read more:
https://www.bis.org/review/r180220g.pdf

Number 3

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Ronald S. Ross, Patrick Viscuso, Gary Guissanie, Kelley L. Dempsey, Mark Riddle

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

The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations.

This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI:

(i) when the CUI is resident in nonfederal information systems and organizations;

(ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and

(iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.

The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components.

To read more:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Number 4

Security Recommendations for Hypervisor Deployment on Servers

Ramaswamy Chandramouli, Computer Security Division
Information Technology Laboratory

The Hypervisor is a collection of software modules that provides virtualization of hardware resources (such as CPU/GPU, Memory, Network and Storage) and thus enables multiple computing stacks (basically made of an OS and Application programs) called Virtual Machines (VMs) to be run on a single physical host.

In addition, it may have the functionality to define a network within the single physical host (called virtual network) to enable communication among the VMs resident on that host as well as with physical and virtual machines outside the host.

With all this functionality, the hypervisor has the responsibility to mediate access to physical resources, provide run time isolation among resident VMs and enable a virtual network that provides security-preserving communication flow among the VMs and between the VMs and the external network.

The architecture of a hypervisor can be classified in different ways. The security recommendations in this document relate to ensuring the secure execution of baseline functions of the hypervisor and are therefore agnostic to the hypervisor architecture.

Further, the recommendations are in the context of a hypervisor deployed for server virtualization and not for other use cases such as embedded systems and desktops.

To read more:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125A.pdf

Number 5

EBA launches 2018 EU-wide stress test exercise

The European Banking Authority (EBA) launched its 2018 EU-wide stress test and released the macroeconomic scenarios.

The adverse scenario implies a deviation of EU GDP from its baseline level by 8.3% in 2020, resulting in the most severe scenario to date. The EBA expects to publish the results of the exercise by 2 November 2018.

Key features of the exercise

The stress test is designed to provide supervisors, banks and other market participants with a common analytical framework to consistently compare and assess the resilience of EU banks to economic shocks. For the first time, it incorporates IFRS 9 accounting standards. No pass-fail threshold has been included as the results of the exercise are designed to serve as an input to the Supervisory Review and Evaluation Process (SREP).

The EBA's 2018 stress test methodology was published in November 2017 and is to be applied to the scenarios released today.

The baseline scenario is in line with the December forecast published by the European Central Bank (ECB), while the adverse scenario assumes the materialisation of four systemic risks, which are currently deemed as representing the most material threats to the stability of the EU banking sector:

- Abrupt and sizeable repricing of risk premia in global financial markets, which would spill over to the European countries and lead to a tightening of financial conditions;

- Adverse feedback loop between weak bank profitability and low nominal growth resulting from the decline in economic activity in the European Union. This will affect, in particular, banks in those countries facing structural challenges in their banking sector;

- Public and private debt sustainability concerns amid potential repricing of risk premia and increased political uncertainty;

- Liquidity risks in the non-bank financial sector with potential spill-overs to the broader financial system.

The adverse scenario is designed to ensure an adequate level of severity across all EU countries. The implied EU real GDP growth rates under the adverse scenario amount to -1.2%, -2.2% and +0.7%, in 2018, 2019 and 2020 respectively.

Overall, the scenario implies a deviation of EU GDP from its baseline level by 8.3% in 2020, resulting in the most severe scenario in terms of GDP deviation from baseline levels compared with the previous EBA exercises.

Detailed information about the scenario can be found in the note produced by the European Systemic Risk Board (ESRB).

Process

The adverse macroeconomic scenarios have been developed by the ESRB and the ECB in close cooperation with the EBA, competent authorities, and national central banks.

The EBA, which is responsible for coordinating the whole exercise, developed a common methodology and will act as a data hub for the final dissemination of the results, in line with its commitment to enhancing the transparency of the EU banking sector. Competent authorities will assure the quality of the results and decide on any necessary supervisory reaction measure as part of the SREP process.

To read more:
http://www.eba.europa.eu/documents/10180/2106649/2018+EU-wide+stress+test+-+Methodological+Note.pdf

Number 6

Market-based finance - a macroprudential view

Sir Jon Cunliffe, Deputy Governor for Financial Stability of the Bank of England, at the Asset Management Derivatives Forum, Dana Point, California.

In 1849 Thomas Carlyle branded economics as the 'dismal science'. That was almost certainly unfair. But unfair or not, the tag has undeniably stuck fast; the public's perception of economists is that it is a gloomy profession.

Central banking generally has picked up much of that gloomy reputation, along with a reputation for being pretty unintelligible - and occasionally deliberately so.

But within the profession of economists and the community of central bankers in the years since the financial crisis, the prize for gloominess, and perhaps for unintelligibility, probably goes to those of us charged with financial stability and what is now known as macroprudential policy.

The root cause lies in what we do – or perhaps more accurately in what we are trying to achieve which is very different to that other core objective of central banks, monetary stability.

Those of us pursuing monetary policy are essentially concerned with central probabilities. The task is to make the best forecast we can of how the economy and inflation pressures will evolve and to adjust policy to ensure the outcome is consistent with monetary stability.

Financial stability by contrast is more about the tail of the probability distribution than the central probability – about what could happen rather than what is likely to happen.

Our task is to ensure the financial system avoids very bad outcomes. Or, if they cannot be avoided, that the system can weather them without breaking down and without acting as an amplifier of stress.

Though infrequent and unlikely, the events we lived through 10 years ago demonstrated that such breakdowns not only can happen but are also extremely costly when they do happen.

So although it may appear gloomy, we are always looking for the downside risk, always asking what risks could the financial system generate, what risks could it withstand, what risks could it amplify? And, by extension, whether it is worth insuring against those risks crystallising.

The past of course gives us some guide. We know many of the things that have caused financial crises in the past that we need to prevent causing problems in the future.

But our job is not just about preventing the last war; it is also about anticipating and assessing new risks as the financial system grows and evolves. And, where justified, taking action to address them.

It is against that gloomy – some would say dismal – background that I want to discuss today how I view the growth and development of market-based finance in recent years.

To read more:
https://www.bis.org/review/r180221a.pdf

Number 7

Former employee jailed for intentionally damaging computer network

National Cyber Security Centre
a part of GCHQ

A disgruntled former Canadian Pacific Railway (CPR) employee was sentenced last week to a year in prison for intentionally causing damage to CPR's computer network.

It is unclear whether train services were affected, but the incident is reported to have cost the organisation approximately $30,000.

In December 2015, the employee resigned from CPR after being informed that he would be fired for insubordinate behaviour. However, before returning his laptop and remote access authentication token to the organisation, the disgruntled individual accessed CPR's core computer network switches, through which critical data flows.

He strategically deleted files, removed admin accounts or changed their passwords, returning the laptop after wiping its hard drive of any evidence of his actions.

This meant IT staff were unable to access the switches, forcing them to reboot the network, causing a system outage. Forensic investigations of systems allowed the damage to be traced back to the individual concerned.

This case is a good example of how disgruntled, former employees can pose a cyber threat to organisations.

Such insider threats are not unique to the rail sector. Public and private organisations in every sector need to be vigilant to such threats.

It highlights the importance of ensuring IT privileges and account access is suspended when a staff member's employment is due to be terminated, preventing malicious cyber activity from being conducted.

Number 8

India City Union Bank SWIFT Related Attack

National Cyber Security Centre
a part of GCHQ

In the last week, the Russian Central Bank reported that an undisclosed Russian bank was targeted in late 2017 in a SWIFT related cyber attack.

Since then, India City Union Bank reported that they had suffered a SWIFT fraud style incident over the weekend.

Some local reporting suggested that insider activity led to the heist, however this has been denied by India City Union Bank. They stated that they had been attacked by "international cyber-criminals and there is no evidence of internal staff involvement".

In these types of attacks the local infrastructure is targeted and compromised, with local valid operator credentials being used to access the SWIFT system.

The attackers then submit fraudulent payment messages. The SWIFT system itself is not breached. SWIFT increased its security measures in 2017, but this particular attack methodology remains lucrative.

In the case of India City Union Bank, $2 million dollars were fraudulently taken, and funds transferred to Dubai, Turkey and China.

India City Union Bank were able to block some payments but are said to be working to recoup a missing $1 million.

It is notable that some recent victims may have a better security posture than previous victims of SWIFT fraud.

It is possible that increasing sophistication by threat actors is enabling them to target a broader range of organisations, and or, they are exploiting the possibility of the insider threat.

Number 9

Increasing Product Complexity: What's at Stake?

Commissioner Kara M. Stein, remarks at SEC Speaks

Good morning. Thank you, Bill [Hinman] for that kind introduction.

As always, it is a pleasure to be with you today at SEC Speaks.

Before I continue, I will remind you that the views I express here today are my own and may not necessarily reflect those of my fellow Commissioners, or of the staff of the Commission.

It's my understanding that this is the 47th year of SEC Speaks. Much has changed in our capital markets since 1972. Computers now allow investors to access a myriad of investment options from common equity to complex financial instruments within minutes.

Both large and small investors have more investment options at their fingertips—and I mean that literally—than ever before. Computers also allow financial products to be developed and sold more quickly than ever before. This high rate of financial innovation and engineering can be beneficial, but it also can present challenges.

I still remember the ashen faces of the Secretary of the Treasury and the Chair of the Federal Reserve when they came to the Senate Banking Committee seeking authorization for a massive federal government intervention during the financial crisis. Financial engineering of complex institutional investment products (such as credit default swaps and collateralized debt obligations) were at the heart of the financial crisis.

Now, over a decade later, we live in the 'era of the possible.' Advances in financial innovation and engineering have enabled the development of new and even more complex financial products.

These advances have also allowed the rapid proliferation of these products into the hands of retail investors.

We know we can build products that take advantage of our technological and engineering capabilities. But the question should not be: "Can we develop and sell to investors a product that does XYZ?" The question ought to be "Should we develop or sell to investors a product that does XYZ?"

Allow me for a moment, to take you back in time more than 100 million years—to the Jurassic and Cretaceous periods—when dinosaurs roamed the earth. You can imagine that these remarkable forms of life looked spectacular from a distance, but up close they were probably quite frightening. Steven Spielberg's movie, Jurassic Park, paints the picture well.

To the park guests, the prehistoric animals were jaw-droppingly majestic, at least from a distance. Up close, however, some of the dinosaurs were unpredictable, if not outright scary. The scientists that created them did not fully understand their capabilities, the unintended effects, or the collateral damage that would inevitably ensue.

The scientists failed to control the park because of what boiled down to a misunderstanding of their highly engineered breeding process. As Dr. Alan Grant noted in the movie, "life found a way."

By referencing Jurassic Park, I am not suggesting that every complex product is equivalent to a tyrannosaurus rex or velociraptor—that is, something scary, dangerous, and unpredictable. All investments have at least some risk. And I recognize that there is a sliding scale of complexity.

But what I would like to do is ask whether certain products are appropriate for all investors? How are these products being sold, particularly to retail customers? Even if the disclosure is perfectly clear, does it appropriately inform investor decision-making? If the Jurassic Park guests really understood what could go wrong, do you think they would go on the tour?

Although strategies involving derivatives may date back to at least the 6th century B.C., when the Greek philosopher Thales bought options on olive presses, they have gotten much more esoteric and complex since then.

Products, strategies, and structures using derivatives can range in complexity now, from covered call strategies on the "simpler side" to the far more exotic.

Things like straddles, strangles, iron condors, iron butterflies, twin-win notes, worst of notes, and buffered super track notes come to mind. It seems like the more odd the name, the more complex the product.

To read more:
https://www.sec.gov/news/speech/stein-sec-speaks-increasing-product-complexity

Number 10

DARPA Seeks to Expand Real-Time Radiological Threat Detection to Include Other Dangers

Building on SIGMA's advanced capability to sniff out illicit radioactive and nuclear materials, SIGMA+ program aims to create additional sensors and networks to detect biological, chemical, and explosives threats

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Advanced commercially available technologies—such as additive manufacturing (3-D printing), small-scale chemical reactors for pharmaceuticals, and CRISPR gene-manipulation tools—have opened wide access to scientific exploration and discovery.

In the hands of terrorists and rogue nation states, however, these capabilities could be misused to concoct chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) weapons of mass destruction (WMD) in small quantities and in form factors that are hard to detect.

To meet this challenge DARPA today announced its SIGMA+ program, an expansion of the existing SIGMA program, which detects radiological and nuclear materials. SIGMA+ seeks to develop new sensors and networks that alert authorities to chemical, biological, and explosives threats as well.

"The goal of SIGMA+ is to develop and demonstrate a real-time, persistent CBRNE early detection system by leveraging advances in sensing, data fusion, analytics, and social and behavioral modeling to address a spectrum of threats," said Vincent Tang, SIGMA+ program manager in DARPA's Defense Sciences Office (DSO).

"To achieve this, we've pulled together a team of DARPA program managers who bring expertise in chemistry, biology, data analytics, and social science to address the broad and complex CBRNE space."

The program calls for the development of highly sensitive detectors and advanced intelligence analytics to detect minute traces of various substances related to WMD threats. SIGMA+ will use a common network infrastructure and mobile sensing strategy, a concept that was proven effective in the SIGMA program.

The SIGMA+ CBRNE detection network would be scalable to cover a major metropolitan city and its surrounding region.

To uncover chemical and explosives threats, SIGMA+ seeks unprecedented long-range detection of hundreds of chemicals at trace levels to help authorities identify bomb-making safe houses in large urban areas, for example. Successfully developing scalable, long-range chemical sensors would help enable interdiction of improvised chemical and explosive threats or their constituent materials before an attack occurs.

To quickly alert officials of a biological terror attack, such as the release of anthrax, smallpox or plague viruses, SIGMA+ seeks sensors that can detect, in real time, traces of a wide range of pathogens.

The program aims to provide immediate, continuous monitoring of pathogen background levels and spikes, which could indicate malicious release of a biological agent.

New environmental, as well as biomechanical and biochemical sensing methods for detecting threats could provide system sensitivity 10 times greater than the state-of-the-art, which would enable detection of a wider range of biological attacks days earlier, maximizing the effectiveness of countermeasures and prophylaxis.

For natural pandemics, SIGMA+ sensing methods could yield awareness of major outbreaks weeks sooner than currently is possible.

The program is structured around two Phases with two planned Broad Agency Announcement (BAA) solicitations.

The first phase focuses on developing novel sensors for chemicals, explosives, and biological agents. The Phase 1 sensors BAA is expected to be released on FedBizOpps in March.

The second phase focuses on network development, analytics, and integration. The Phase 2 BAA is expected to be released in late 2018.

“If successful, SIGMA+ will demonstrate that automated, distributed networks of sensors, combined with automated intelligence analytics and insights from social science, can be deployed and practically scaled to significantly increase the probability of interdicting CBRNE WMD attacks,” said Tang.

A Proposers Day is scheduled for March 7, 2018 in Arlington, Virginia. Details and registration instructions are available here: https://go.usa.gov/xnFub

A Broad Agency Announcement (BAA) solicitation for the first phase of the program is expected to be available in March on FedBizOpps here: http://go.usa.gov/3W53j

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.

The International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. Membership – Become a standard, premium or lifetime member.

You may visit:
www.risk-compliance-association.com/How_to_become_member.htm

Become a lifetime member of the association, and to continue your journey without interruption and without renewal worries. You will get a lifetime of benefits as well.

You can check the benefits at:
www.risk-compliance-association.com/Lifetime_Membership.htm

2. Weekly Updates - Subscribe to receive every Monday, the Top 10 risk and compliance management related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next:
http://forms.aweber.com/form/02/1254213302.htm

3. Training and Certification - The Certified Risk and Compliance Management Professional (CRCMP) training and certification program has become one of the most recognized programs in risk management and compliance.

There are CRCMPs in 32 countries around the world. Companies and organizations like Accenture, American Express, USAA etc. consider the CRCMP a preferred certificate.

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

For the distance learning programs, you may visit:
www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We can tailor all programs to meet specific requirements. We tailor presentations, awareness and training programs for supervisors, boards of directors, service providers and consultants.

4. IARCP Authorized Certified Trainer (IARCP-ACT) Program - Become a Certified Risk and Compliance Management Professional Trainer (CRCMPT) or Certified Information Systems Risk and Compliance Professional Trainer (CISRCPT).

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:
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 CRCMP and CISRCP 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:
www.risk-compliance-association.com/Approved_Centers.html