Monday, March 25, 2019

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,

According to the Bank for International Settlements (BIS), "crypto-assets present a number of risks for banks, including liquidity risk; credit risk; market risk; operational risk (including fraud and cyber risks); money laundering and terrorist financing risk; and legal and reputation risks." *If you think it looks like a Basel iii nightmare, you are right.*

According to the BIS: "Before acquiring exposures to crypto-assets or providing related services, a bank should conduct comprehensive analyses of the risks noted above. The bank should ensure that it has the relevant and requisite technical expertise to adequately assess the risks stemming from crypto-assets.

The bank should have a clear and robust risk management framework that is appropriate for the risks of its crypto-asset exposures and related services.

Given the anonymity and limited regulatory oversight of many crypto-assets, a bank's risk management framework for crypto-assets should be fully integrated into the overall risk management processes, including those related to anti-money laundering and combating the financing of terrorism and the evasion of sanctions, and heightened fraud monitoring.

Given the risk associated with such exposures and services, banks are expected to implement risk management processes that are consistent with the high degree of risk of crypto-assets. Its relevant senior management functions are expected to be involved in overseeing the risk assessment framework.

Board and senior management should be provided with timely and relevant information related to the bank's crypto-asset risk profile.

An assessment of the risks described above related to direct and indirect crypto-asset exposures and other services should be incorporated into the bank's internal capital and liquidity adequacy assessment processes.

A bank should publicly disclose any material crypto-asset exposures or related services as part of its regular financial disclosures and specify the accounting treatment for such exposures, consistent with domestic laws and regulations.

The bank should inform its supervisory authority of actual and planned crypto-asset exposure or activity in a timely manner and provide assurance that it has fully assessed the permissibility of the activity and the risks associated with the intended exposures and services, and how it has mitigated these risks."

We also read: "While crypto-assets are at times referred to as "crypto - currencies", the Committee is of the view that such assets do not reliably provide the standard functions of money and are unsafe to rely on as a medium of exchange or store of value." (emphasis added).

Read more at Number 1 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 7)

Statement on crypto-assets

BANK FOR INTERNATIONAL SETTLEMENTS

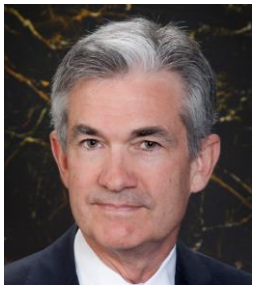
The past few years have seen a growth in crypto-assets. While the crypto-asset market remains small relative to that of the global financial system, and banks currently have very limited direct exposures, the Committee is of the view that the continued growth of crypto-asset trading platforms and new financial products related to crypto-assets has the potential to raise financial stability concerns and increase risks faced by banks.

Number 2 (Page 10)

Cyber Essentials, National Cyber Security Centre, UK

Number 3 (Page 11)

Speech (via prerecorded video) by Jerome H Powell, Chairman of the Board of Governors of the Federal Reserve System, at the "Just Economy Conference", sponsored by the National Community Reinvestment Coalition, Washington DC.



"The National Community Reinvestment Coalition (NCRC) and its member organizations are at the forefront of an important conversation about how to ensure that low- and moderate-income communities are fairly served by the banking industry."

Number 4 (Page 14)

Think Global, Act Global: cyberspace and emerging technology

Ciaran Martin, CEO of the NCSC, speaking at CyberSec in Brussels

"Our commitment to working with partners here on the European continent is unshakeable. Whatever form the future relationship between the UK and the European Union takes beyond 29 March this year, the Prime Minister and her Cabinet have long made clear that our support to European security as a whole is unconditional."

Number 5 (Page 23)

Changing gears - about cycling and the future of banking

Frank Elderson, Executive Director of Supervision of the Netherlands Bank, at the Netherland's Bank banking seminar, Amsterdam.

"You see, I was leading the DNB team responsible for supervising ABN Amro back in 2006. I remember going to the Zuidas by bike, parking it right in front of that huge entrance of the ABN Amro building - which wasn't allowed by the way.

That solitary black bicycle, against the sheer backdrop of one of the tallest sky-scrapers of Amsterdam at that time, in a way that bicycle formed an

early example of transparent supervision: since everybody knew it was my bike, every time they saw it they knew the supervisor was in the building."

Number 6 (Page 25)

Privacy standards for information security

Over the last decade, there has been a significant development of privacy standards, which aim at contributing to the integration of privacy requirements into information processes, systems and services.

enisa European Union Agency for Network and Information Security

Such integration is fundamental to protect personal identifiable information, particularly in digital environments and it may support the implementation of relevant privacy and data protection legislation.

Number 7 (Page 27)

When expectations meet the future

Sir Jon Cunliffe, Deputy Governor for Financial Stability of the Bank of England, at the London School of Economics.

"So I will not today give you my prediction for the origin, shape and extent of the next great crisis. I am however prepared to make one prediction with confidence. Whatever the trigger and the financial services and instruments most affected, the next crisis will have, somewhere at its centre, losses from an overextension of credit and an adjustment in asset prices."

Number 8 (Page 29)

The age of leverage

Carolyn A Wilkins, Senior Deputy Governor of the Bank of Canada, to the UBC Vancouver School of Economics and CFA Society Vancouver, Vancouver, British Columbia.

"What's happening in the global arena has got to be top of mind for people in this room: the trade war between the United States and China, growing geopolitical unrest in many quarters. These issues are top of mind for us at the Bank of Canada too.

The global development that concerns me the most, though, is rising debt. Global debt now totals around US$240 trillion-that's US$100 trillion higher than just before the financial crisis, and more than three times current global gross domestic product (GDP)."

Number 9 (Page 39)

Cybersecurity Disclosure Act of 2019?

Will publicly traded companies be required to disclose to investors whether any members of their board of directors have cybersecurity expertise?

A BILL

To amend the Securities Exchange Act of 1934 to promote transparency in the oversight of cybersecurity risks at publicly traded companies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity Disclosure Act of 2019".

Number 10 (Page 40)

Progress on Lifelong Learning Machines Shows Potential for Bio-Inspired Algorithms

USC milestone on L2M program shows how machines could be capable of learning through experience

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Today's machine learning systems are restricted by their inability to continuously learn or adapt as they encounter new situations; their programs are fixed after training, leaving them unable to react to new, unforeseen circumstances once they are fielded. Adding new information to cover programming deficits overwrites the existing training set. With current technology, this requires taking the system offline and retraining it on a dataset that incorporates the new information.

Number 1

Statement on crypto-assets

BANK FOR INTERNATIONAL SETTLEMENTS

The past few years have seen a growth in crypto-assets. While the crypto-asset market remains small relative to that of the global financial system, and banks currently have very limited direct exposures, the Committee is of the view that the continued growth of crypto-asset trading platforms and new financial products related to crypto-assets has the potential to raise financial stability concerns and increase risks faced by banks.

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

Crypto-assets are not legal tender, and are not backed by any government or public authority.

Through this newsletter, the Basel Committee is setting out its prudential expectations related to banks' exposures to crypto-assets and related services, for those jurisdictions that do not prohibit such exposures and services.

Crypto-assets have exhibited a high degree of volatility and are considered an immature asset class given the lack of standardisation and constant evolution.

They present a number of risks for banks, including liquidity risk; credit risk; market risk; operational risk (including fraud and cyber risks); money laundering and terrorist financing risk; and legal and reputation risks. Accordingly, the Committee expects that if a bank is authorised and decides to acquire crypto-asset exposures or provide related services, the following should be adopted at a minimum:

- Due diligence: Before acquiring exposures to crypto-assets or providing related services, a bank should conduct comprehensive analyses of the risks noted above. The bank should ensure that it has the relevant and requisite technical expertise to adequately assess the risks stemming from crypto-assets.

- Governance and risk management: The bank should have a clear and robust risk management framework that is appropriate for the risks of its crypto-asset exposures and related services.

  Given the anonymity and limited regulatory oversight of many crypto-assets, a bank's risk management framework for crypto-assets should be fully integrated into the overall risk management processes, including those related to anti-money laundering and combating the financing of terrorism and the evasion of sanctions, and heightened fraud monitoring.

  Given the risk associated with such exposures and services, banks are expected to implement risk management processes that are consistent with the high degree of risk of crypto-assets.

  Its relevant senior management functions are expected to be involved in overseeing the risk assessment framework.

  Board and senior management should be provided with timely and relevant information related to the bank's crypto-asset risk profile.

  An assessment of the risks described above related to direct and indirect crypto-asset exposures and other services should be incorporated into the bank's internal capital and liquidity adequacy assessment processes.

- Disclosure: A bank should publicly disclose any material crypto-asset exposures or related services as part of its regular financial disclosures and specify the accounting treatment for such exposures, consistent with domestic laws and regulations.

- Supervisory dialogue: The bank should inform its supervisory authority of actual and planned crypto-asset exposure or activity in a timely manner and provide assurance that it has fully assessed the permissibility of the activity and the risks associated with the intended exposures and services, and how it has mitigated these risks.

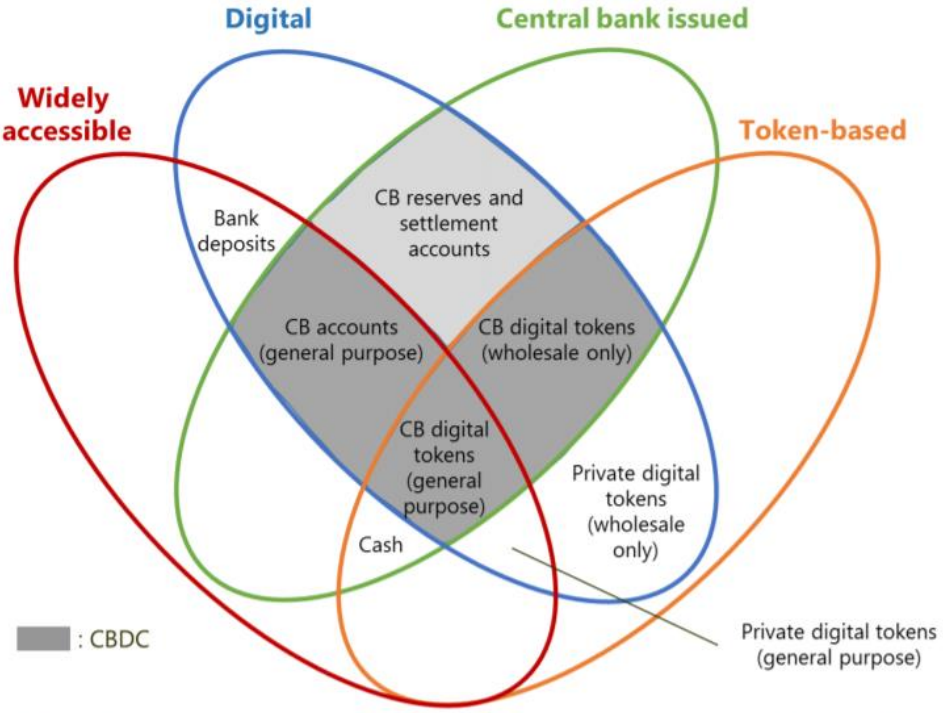
The Committee continues to monitor developments in crypto-assets, including banks' direct and indirect exposures to such assets.

The Committee will in due course clarify the prudential treatment of such exposures to appropriately reflect the high degree of risk of crypto-assets.

It is coordinating its work with other global standard setting bodies and the Financial Stability Board.

Note: Crypto-assets differ from central bank digital currencies. See the report by the Committee on Payments and Market Infrastructures and the Markets Committee, available at:
https://www.bis.org/cpmi/publ/d174.htm

The money flower: a taxonomy of money — Graph 1



Notes: The Venn-diagram illustrates the four key properties of money: *issuer* (central bank or not); *form* (digital or physical); *accessibility* (widely or restricted) and *technology* (account-based or token-based). *CB* = central bank, *CBDC* = central bank digital currency (excluding digital central bank money already available to monetary counterparties and some non-monetary counterparties). *Private digital tokens (general purpose)* include crypto-assets and currencies, such as bitcoin and ethereum. *Bank deposits* are not widely accessible in all jurisdictions. For examples of how other forms of money may fit in the diagram, please refer to the source.

Source: Based on Bech and Garratt (2017).

Number 2

Cyber Essentials, National Cyber Security Centre, UK

Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

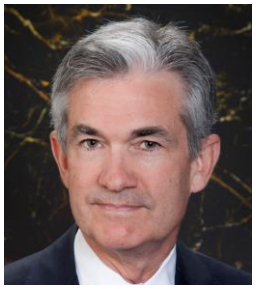
Cyber attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a thief trying your front door to see if it's unlocked. Our advice is designed to prevent these attacks.

You may visit:
https://www.cyberessentials.ncsc.gov.uk/

Number 3

Brief remarks

Speech (via prerecorded video) by Jerome H Powell, Chairman of the Board of Governors of the Federal Reserve System, at the "Just Economy Conference", sponsored by the National Community Reinvestment Coalition, Washington DC.



Good evening, and thank you for inviting me to speak to you today.

The National Community Reinvestment Coalition (NCRC) and its member organizations are at the forefront of an important conversation about how to ensure that low- and moderate-income communities are fairly served by the banking industry.

The work that you do to promote access to basic banking services, affordable housing, and entrepreneurship opportunities supports the Federal Reserve and other agencies that enforce fair lending laws.

The large number and variety of NCRC's local member organizations allow the NCRC to draw a detailed picture of how the Federal Reserve's policies affect lower-income communities, and we deeply appreciate the information that you share with us and the work that it represents.

As you know all too well, the current strength of the overall economy masks the struggles many individuals and families face in lower-income urban and rural communities.

Low- and moderate-income homeowners saw their wealth stripped away as home values dropped during the financial crisis and have not recovered as quickly or completely as others.

Because home equity has been the main source of wealth among low- and moderate-income people, the crisis dealt a particularly severe blow to these households.

Most Americans rely on home equity to send their children to college, invest in their own education and training, or start or grow a business.

These aspirations are the basis upon which a strong economy is built. That is why your work as NCRC member organizations offering financial counseling, homeownership education, and technical assistance for small businesses is as important as ever.

When lower-income individuals and families struggle, it harms their health and well-being and also weakens our economy.

When people are connected to education, training, and other resources that help them secure good jobs and other opportunities, they are better prepared to care for themselves and their families and contribute to a strong economy.

The Federal Reserve has an extensive community development function, related to our responsibilities under the Community Reinvestment Act (CRA), that promotes partnerships between banks and community organizations to address local community and economic development needs.

As you know, the CRA requires federal banking regulators-the Federal Reserve, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation-to encourage banks to help meet the credit needs of the communities they are chartered to serve, including low- and moderate-income neighborhoods.

To complement the work we do with the other regulators to write regulations and guidance implementing CRA, the Federal Reserve System's community development staff help banks understand and meet their responsibilities under the law.

Fed staff members also act as liaisons between banks and community organizations to identify local community development needs and solutions.

I know that you all are very interested in the agencies' activities related to possible revisions to the current CRA regulations.

My colleague, Governor Brainard, who represents the Board in our interagency CRA discussions, will be speaking to you tomorrow, so I will leave it to her to discuss our efforts in detail.

But I do want to express my support for an interagency effort to revise the regulations to promote clarity and consistency in our evaluations of banks, particularly in light of the changes in the way bank products and services are delivered.

We value the CRA's role in meeting the credit needs of low- and moderate-income neighborhoods and want to be very careful that any revisions serve to strengthen the CRA's purpose.

I commend your dedication to ensuring that all Americans have fair access to the economic opportunities that our nation offers. I hope you have a productive conference, and I look forward to our ongoing conversation about how the Federal Reserve can help.

Number 4

Think Global, Act Global: cyberspace and emerging technology

Ciaran Martin, CEO of the NCSC, speaking at CyberSec in Brussels

Thank you to Izabela Albrycht and her colleagues at CyberSec for hosting this excellent conference and for inviting me. CyberSec is an outstanding institution making a very positive contribution to global cyber security.

I'm very proud to represent the UK's National Cyber Security Centre, a part of GCHQ, our signals intelligence agency. It is a pleasure to be among friends discussing our shared aim of improving our digital environment.

Our commitment to working with partners here on the European continent is unshakeable. Whatever form the future relationship between the UK and the European Union takes beyond 29 March this year, the Prime Minister and her Cabinet have long made clear that our support to European security as a whole is unconditional.

More practically, within the cyber security sphere, it is objectively true that nearly all of the functions of the UK's National Cyber Security Centre fall outside the scope of EU competence.

It follows that our enhanced cooperation with European partners, and the EU as a whole, in cyber security over recent years is not automatically affected by the UK's changing relationship with the EU.

Pretty much everything we do now to help European partners, and what you do to help us, on cyber security can, should, and I am confident will continue beyond 29 March.

Over the past few years we have shared classified and other threat data with the vast majority of member states and with the institutions. We have also, we hope, played an important role in the development of European thinking in areas like standards and incident response.

We hope we've helped through our work with CERT-EU on incidents and with ENISA and ETSI on standards.

As the next phase of the UK's relationship with the rest of Europe takes shape, we will want to take these partnerships further and to develop new ones. I am proud of the increasing frequency with which I see my European counterparts and the deepening friendships we have nurtured, the boundaries we are removing and the ground we are breaking.

The protection of our shared values of freedom, democracy and prosperity, all underpinned by the rule of law, is what we strive for.

My theme today is about how we cooperate together in the age of globalised technology. Because whatever final form the UK's relationship with the EU takes, we need, together, to be at the forefront of global efforts to build an internet that remains not just free but safer too.

In this era of truly globalised technology, it is more important than ever that that effort is – truly – global. There are limitations to what even a continent of the size and wealth of Europe can do on its own in an age where the US and China dominate tech development.

I want to deal today with two structural challenges for the future of internet security.

The first is about telecommunications infrastructure, now and in the future. The second is how we improve structural flaws in the wider internet environment.

In both areas, EU and non-EU European nations will need to act with others outside the continent to shape future technology and the security around it.

So first, let's talk about telecommunications infrastructure.

The next generation of telecoms security is particularly important given the sorts of networks dependent on it – there will be large-scale use of autonomous vehicles, desktop experiences from the cloud, high-definition streaming, the underpinning of smart cities.

A hard headed, risk based approach to the policymakers taking decisions

Like many countries, including our five eyes partners, and partners here in Europe, the UK is looking at the right policy approach to 5G security.

That policy process is being led by the Digital Department and its Secretary of State. It concludes its analysis in the spring. The government will then take decisions.

As its public terms of reference make clear, it is a holistic review, taking account of economic, security, quality of service and other factors. It is considering a full range of policy options.

Everything is on the table. Contrary to some reporting no decisions have been taken and no decisions are being announced today.

The National Cyber Security Centre's role is to offer expert, objective, technologically literate input into the security considerations around 5G. That is consistent with the NCSC's wider mission to bring objective rigour to complex technical issues. And today I want to talk to you about the lessons we have learned.

And the first thing to say is that 5G is complicated.

It hugely accelerates the pace of technological change but there is no cliff edge transition.

It will change the way we think about risk because of what will, over time, depend on it. But it doesn't change immutable concepts of security or the laws of science.

And whilst key to the virtual world, it requires a huge amount of complex physical infrastructure. And how that physical infrastructure is configured varies from country to country, not least depending on the size of the country's landmass and is population.

And it is not a fresh start. It has to build on existing telecommunications infrastructure.

Understanding these complexities is essential. The National Cyber Security Centre is an open and transparent organisation. We have set out before our understanding of how telecommunications networks work and what is needed to secure them. And we will continue to publish objective, technically credible, clear-headed and rigorous analyses of cyber security requirements.

And we need to set out telecommunications security in the context of the threat picture. Again, here we are open and transparent about the threats we see and how they impact the UK.

Over the past two years, the UK government has, based on NCSC findings, attributed state-sponsored malicious cyber activity against the UK to Russia, China, North Korea and Iran. There is also a serious and sustained threat from organised cyber crime.

These attacks have come against a range of targets spanning different sectors. Their aims have been different. The methods have been different.

The supply chain, and where suppliers are from, is one issue but it is not the only issue. Last year, the NCSC publicly attributed some attacks on UK networks, including telecoms networks, to Russia. As far as we know, those networks didn't have any Russian kit in them, anywhere.

The techniques the Russians used to target those networks were looking for weaknesses in how they were architected and how they were run.

So we are not naïve. Far from it. In the 1,200 or so significant cyber security incidents the NCSC has managed since we were set up, the country of origin of suppliers has not featured among the main causes for concern in how these attacks are carried out.

Three technical pre-conditions for telecommunications e-security

That's one example of our objective, evidence-based analysis of the threat.

We take a similar objective, evidence-based approach to the technical security requirements for 5G.

Taking threat and requirements together, this leads us to conclude that there are three technical pre-conditions for secure 5G networks.

They are:

First, we must have higher standards of cyber security across the entire telecommunications sector.

The biggest threat to our cyber security is weak cyber security.

Practices must be improved. That is the real lesson of the 1,200 cyber security incidents.

The market does not currently incentivise good cyber security.

That has to change.

The number one pre-condition for safe 5G is better cyber security.

Second, telecoms networks must be more resilient.

We must assume that a global supply chain will have multiple vulnerabilities, whether intentional or, more likely, unintentional. Networks are built by human beings and human beings make mistakes. No network can be totally safe.

From the point of view of managing corporate risk, or, in our case, national risk, it essentially doesn't matter whether the vulnerabilities are deliberate or the result of honest mistakes. What matters is that those vulnerabilities can and will be exploited.

But the networks can and should be designed in a way that will cauterise the damage. That is what we need to do. Put it another way, if you've built a telecommunications network in a way that the compromise of one supplier can cause catastrophic national harm, then you've built it the wrong way.

Resilience is key.

The third pre-condition flows from that. There must be sustainable diversity in the supplier market.

Should the supplier market consolidate to such an extent that there are only a tiny number of viable options, that will not make for good cyber security, whether those options are Western, Chinese, or from anywhere else.

Any company in an excessively dominant market position will not be incentivised to take cyber security seriously. And at the same time that company could also become the prime target for attack for the globe's most potent cyber attackers.

These pre-conditions are technical. They are generic. They are about the technology and the architecture and the structure of our networks.

They are about creating the necessary conditions for a safe 5G network.

As already mentioned, like everywhere else, the UK is not starting from scratch. We have an existing telecommunications infrastructure. It is highly internationalised.

And we already have a framework for managing risk. Again, I stress that this is based on an objective understanding of how telecoms networks work. As our guidance to operators shows, we assume that every bit of kit in any

network can fail. And so what's vital is that the failure of individual bits of kit, either because of a malfunction or because of an attack, will not cause catastrophic harm.

That's the framework we apply at national level. There are things we particularly care about. National security networks, most obviously. And for those, we apply special protections.

Huawei and standards of cyber security

One well-known specific aspect of our current mitigation framework is how we manage Huawei's presence in UK networks.

Huawei's presence is subject to detailed, formal oversight, led by the NCSC. Because of our 15 years of dealings with the company and ten years of a formally agreed mitigation strategy which involves detailed provision of information, we have a wealth of understanding of the company.

We also have strict controls for how Huawei is deployed. It is not in any sensitive networks – including those of the government. Its kit is part of a balanced supply chain with other suppliers.

Our regime is arguably the toughest and most rigorous oversight regime in the world for Huawei.

And it is proving its worth. Last July, our annual Oversight Board downgraded the assurance we could provide to the UK government on mitigating the risks associated with Huawei because of serious problems with their security and engineering processes.

As we said then, and repeat today, these problems are about standard of cyber security; they are not indicators of hostile activity by China.

The company have accepted these findings and have pledged to address them, acknowledging that this will be a process of some years.

We will monitor and report on progress and we will not declare the problems are on the path to being solved unless and until there is clear evidence that this is the case.

We will not compromise on the improvements we need to see from Huawei.

And, based on our hard-headed assessment of risk and our detailed knowledge of how networks work, we are putting in place our own plans for helping our operators to manage these risks.

It's complicated

So today I am setting out how the NCSC is looking to manage the risks now, for example those around Huawei, and how we could seek to manage the risks into the future.

The UK community is united in this effort.

As the head of MI6, Alex Younger, said in Munich last week, it's complicated. As the Director of GCHQ, my boss, Jeremy Fleming, has set out before and will do so again shortly, it is vital that the UK's stance is informed by the most rigorous assessment of threat, risk and technical requirements. GCHQ, of which the NCSC is part, is at the heart of that discussion.

It is the NCSC's job, working with partners in central government, the regulators and elsewhere to make sure the UK can prosper securely in these complex market conditions through a hard-headed, technically informed assessment of the risk.

That will enable government to weigh up those vital decisions on things like suppliers from different countries.

5G is about much more than just cyber security.

Our job is to make sure that the government can be confident that behind whatever decision it takes, there will be a technical framework that works and a competent national technical authority that knows what it is doing.

Whatever decisions are taken will need to ensure that those three essential pre-conditions for cyber security that we have set out today can be met: stronger standards, more resilience and supplier diversity.

Indeed our experience with Huawei, if nothing else, demonstrates the importance of raising standards of performance in cyber security.

5G security is not a simple, binary choice. It is about complex technical functions, a complex global threat environment, and a complex global market.

One thing is clear: the way that market works has to change.

Security must be a bigger consideration in market decisions in the future than it has been to date. We will help fix that.

Active/automated cyber defence

And the push to improve standards in cyber security should be a global effort. So the more we can do with partners to deliver those, the better.

That brings me to the wider issue of how we cooperate to improve the global digital infrastructure more generally.

The internet was not built with security in mind. That's no one's fault. It wasn't malicious. It's just the way it happened. A model evolved over time where the price of entry for online services became the provision of personal data.

It's safe to say that the limitations of that model are becoming more apparent as time passes.

And they also leave us with structural security problems in the way the internet works.

At the National Cyber Security Centre we focus on the technical solutions that the market hasn't provided because of the way the internet environment has evolved.

We aim to make the internet automatically safer for people to use. It's not fair on busy individuals with complicated, rushed lives and other priorities if we expect them to make judgments every day about how trustworthy one of the hundreds or thousands of bits of communication they get every day are.

That is what is behind our active, or automated, cyber defence programme.

Its aim is to provide a framework to take away most of the harm from most of the people most of the time.

Here are some of the early results.

We have developed a system to use our vast quantity of threat data to block connections to malicious sites from government networks. We are now protecting 1.3 million government internet users.

In 2018, we blocked 11,000 unique malicious domains every month. In the course of the year, we blocked 54 million malicious connections. That's 54 million incidents that automatically didn't happen.

We developed an anti-spoofing mechanism to protect government brands. In the first year, we helped our tax authority block half a billion attempts to spoof it. Half a billion fake emails that didn't land in people's inboxes.

We developed a system for automatically taking down known phishing sites. They used to be up for a day on average. Now it's about an hour. And the UK's share of global phishing that we can see has fallen from 5.3 per cent to 2.2 per cent in the past two and a half years.

Think of the potential if we can amplify these sorts of improvements internationally.

None of them has required legislation, and none has been particularly contentious. They are technical improvements – targeted government interventions where commercial solutions can't work. They are low classification – we publish details for most of them. I cannot think of an area more ripe for international cooperation.

So whether it's future telecommunications infrastructure, or digital security more generally, we want to work with everyone across Europe and beyond to push these changes, to deliver the digital world we all want to see, one that is not just free and prosperous, but safer as well.

Thank you.

Number 5

Changing gears - about cycling and the future of banking

Frank Elderson, Executive Director of Supervision of the Netherlands Bank, at the Netherland's Bank banking seminar, Amsterdam.

When I took up this job as chief supervisor for the Dutch banking sector, summer last year, I realized again how much better shape the Dutch banks are in, than the last time I was actively involved in prudential banking supervision.

You see, I was leading the DNB team responsible for supervising ABN Amro back in 2006.

I remember going to the Zuidas by bike, parking it right in front of that huge entrance of the ABN Amro building - which wasn't allowed by the way.

That solitary black bicycle, against the sheer backdrop of one of the tallest sky-scrapers of Amsterdam at that time, in a way that bicycle formed an early example of transparent supervision: since everybody knew it was my bike, every time they saw it they knew the supervisor was in the building.

Of course, it's a story with a tragic undertone.

The years 2006 and 2007 have a fateful ring to them.

We were witnessing the tearing apart of the largest bank in the Netherlands.

Less than a year after the consortium took over ABN Amro, on a sunny day people were leaving the Lehman head offices carrying cardboard boxes.

The rest is history.

How totally different to the picture we observe today!

Today I see a banking sector that has weathered the storm, and has emerged stronger.

Smaller perhaps, but more resilient, more focused and better capitalized.

To read more:
https://www.bis.org/review/r190315c.pdf

DeNederlandscheBank
EUROSYSTEEM

Number 6

Privacy standards for information security

Over the last decade, there has been a significant development of privacy standards, which aim at contributing to the integration of privacy requirements into information processes, systems and services.

Such integration is fundamental to protect personal identifiable information, particularly in digital environments and it may support the implementation of relevant privacy and data protection legislation.

This ENISA study, explores how the standards-developing world has been responding to the fast-changing and demanding realm of privacy. This study provides insights into the state-of-the-art of privacy standards in the information security context by mapping existing standards available and standardisation initiatives alike.

The main findings of this study include the following:

- There is an increasing need to analyse the mapping of international standards and European regulatory requirements, as references to standards in the EU legislation are becoming recurrent and there are considerable differences from jurisdictions outside of the EU;

- Proving compliance with privacy standards in information security is not as straightforward as expected. Some approaches for conformity assessment are available in specific sectors, others are still lacking appropriate mechanisms;

- A coherent analysis of sector-specific needs for privacy standardisation is essential, especially in the context of information security, before moving ahead with the adoption or development of new standards;

- Standardisation focuses mainly on covering technological approaches and solutions. Many such solutions address the introduction of privacy-preserving technologies throughout the whole lifecycle of a product or a system. The concept of privacy-by-design and its implementation are still not presented clearly, despite a general common agreement on perceived benefits.

ENISA complements this information with a range of additional recommendations, which aimed to support the prioritisation of potential areas of action for the near future:

- EU policy makers and European Standards Organisations should promote the development of European content and input to privacy and cybersecurity standards;

- EU policy makers and European Cybersecurity Certification Group members should promote the endorsement and adoption of privacy and information security standards, including conformity assessment standards specific to privacy;

- EU bodies and competent authorities in the Member States should promote the adoption of a structured approach on the analysis of sector-specific needs with regard to privacy standardisation, especially in information security context and then proceed with the adoption or development of new standards;

- EU policy makers and relevant EU bodies need to be further involved in the standardisation process, so as to define, endorse or affirm potential standardisation goals in the areas of privacy and information security;

- Competent bodies at EU and Member State level should further promote their research and standardisation activities to support the meaningful implementation of the 'Privacy by Design' principle.

For full report:
https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation

Number 7

When expectations meet the future

Sir Jon Cunliffe, Deputy Governor for Financial Stability of the Bank of England, at the London School of Economics.

The subject of this symposium is “The Next Great Crisis” by which I think we mean financial crisis.

One of the defining characteristics of humans is our ability to imagine the future, as I shall discuss later.

But though we can imagine the future, we cannot know it.

And I am a cautious central banker.

So I will not today give you my prediction for the origin, shape and extent of the next great crisis.

I am however prepared to make one prediction with confidence.

Whatever the trigger and the financial services and instruments most affected, the next crisis will have, somewhere at its centre, losses from an overextension of credit and an adjustment in asset prices.

And, for me, as Deputy Governor at the Bank of England responsible for Financial Stability, an equally if not more important question is not what will the next great financial crisis look like but whether the next and subsequent financial crises will actually be ‘great’.

Will the correction of asset prices and the losses on credit be amplified by the financial system and cause the economic and social loss we saw 10 years ago?

Or, losses notwithstanding, will the system absorb them without material dislocation to the economy?
I can make the prediction that the next ‘crisis’ will have somewhere at its centre the overextension of credit and asset price adjustment because it is not a particularly bold one.

Since its invention in the temple organisation of bronze age Mesopotamia, interest bearing debt – or credit if you want to see it from the other side of the coin – has had the property of being able to grow beyond the ability, or sometimes the willingness, of the economy to repay it.

Debt contracts are essentially claims on the future and the future, when it arrives, does not always honour them.

The origin of debt and credit are fascinating but unclear.

It may have been an evolution of the reciprocal gift giving social obligations of early tribal societies.

The etymological evidence suggests rather an evolution from the system of fines and compensation for injuries prevalent in such societies.

It has also been suggested that the foundation of debt is the belief that man is born with debt to the heavens and creation and debt between members of society is an extension of this idea.

In economic terms, the early debt systems and the debts themselves, painstakingly recorded in the ledger systems of the temples of bronze age Mesopotamia, appear to be primarily about what we would now call working capital and overdraft facilities in agrarian societies that produced little economic surplus – credit to tide farmers over until the harvest or through bad harvests with the debt repaid in standardised units of agricultural produce.

To read more:
https://www.bis.org/review/r190312d.pdf

Number 8

The age of leverage

Carolyn A Wilkins, Senior Deputy Governor of the Bank of Canada, to the UBC Vancouver School of Economics and CFA Society Vancouver, Vancouver, British Columbia.

Good afternoon. Let me thank the UBC Vancouver School of Economics and the Vancouver CFA Society for the invitation.

Vancouver is truly a global city. More than 70 countries have consular services here to support foreign-based firms doing business in the region. International students flock to the universities here. And, people from all over the world have decided to invest in housing in the region.

What's happening in the global arena has got to be top of mind for people in this room: the trade war between the United States and China, growing geopolitical unrest in many quarters. These issues are top of mind for us at the Bank of Canada too.

The global development that concerns me the most, though, is rising debt. Global debt now totals around US$240 trillion-that's US$100 trillion higher than just before the financial crisis, and more than three times current global gross domestic product (GDP).

Here I'm referring to borrowing by governments, businesses and households. Whether you're a homeowner or a businessperson, you know first-hand that high leverage can leave you in a vulnerable financial position.

It's no different for economies. The world has learned this lesson the hard way on many occasions in my lifetime alone. The budget deficits that the United States incurred in the 1960s-and the excessively loose monetary policy that went along with them-laid the foundation for the "great inflation" of the 1970s and the breakdown of the Bretton Woods system of pegged exchange rates. The recession that followed destroyed many businesses and put many people out of work.

By the 1990s, it appeared we had learned our lesson. Many central banks were adopting some form of inflation-control regime. This not only helped restrain the temptation to inflate away debts, but also contributed to a decade and a half of economic stability.

Yet 2007 saw the beginnings of what would become a global financial crisis. Excess leverage was once again at the root, although this time it was in financial institutions and households. The Great Recession that began that year and lasted into 2009 saw governments, companies and people from all walks of life suffer consequences. Even though Canada was spared the worst of it, we were reminded of how quickly the fallout can spread across borders.

We're now almost 10 years into the global expansion. Many of those who lost their jobs have found work again, asset values have risen, and monetary policy in some countries is no longer at emergency settings. Still, the road that we took to recovery has led us into an era of even higher leverage across many major economies.

Does that mean that the global economy is headed for another period of financial instability? The global financial system is in a better place than it was in 2007 in many ways that reduce risks. There are nonetheless uncertainties that could throw us off track, such as how trade tensions might evolve. In any case, when downturns occur, high leverage is usually an amplifying factor. Let me tell you where I see the trouble spots and what's required to manage them.

Leverage is creating vulnerabilities in many places

So, how did we end up here again?

An important piece of the story is the highly accommodative monetary policies that were needed to clean up the mess and get global growth back on track after the crisis. This, combined with an abundance of global savings, has kept interest rates low.

On top of that, many governments implemented large fiscal stimulus programs.

The downturn would have been even deeper and more painful without these decisive policy responses. What strikes me though is how much overall leverage has grown globally, even as the financial sector has repaired its books. Government debt has skyrocketed over the past 10 years, to close to 90 per cent of global GDP. The debt of non-financial corporations has doubled in nominal terms over the same period.

Of course, not all borrowing is bad. Borrowing makes sound business sense if the funds are spent on productive pursuits.

That said, not all leverage is created equal in terms of risk. The creditworthiness of the borrower and the quality of the instrument are also important considerations. I'll focus on three areas that are of particular concern to me.

Let me start with the type of debt that is most relevant for Canada - household leverage. The Bank has been clear that high household debt, currently at around 178 per cent of disposable income, is our number one domestic financial vulnerability.

Historically low borrowing costs obviously contributed. At the same time, other factors-housing supply constraints, strong interest among offshore investors-contributed to higher house prices and bigger mortgages. People here in Vancouver can relate to that.

Canada doesn't have the same issues around the quality of debt that the United States had before the crisis. It is still a worry, though, because debt can put people in a tough spot if interest rates go up or their incomes fall.

We take this into account when we set monetary policy. Canada is not alone in this. Sweden and Australia, for instance, are facing similar household vulnerabilities.

Now let me turn to public sector debt. There are good reasons for governments to finance some spending through debt.

However, debt can create vulnerabilities if it is not sustainable, or if it prevents fiscal policy from responding to unexpected needs. We saw this in the euro area following the financial crisis.

Limited fiscal space in some countries meant that monetary policy had to bear the burden of reviving the economy. Substantial progress has been made since Europe faced a debt crisis around eight years ago. Still, public debt in certain countries remains a concern.

This is partly because membership in the euro area prevents economic adjustment through exchange rate movements.

Plus, there's no system of fiscal transfers to help smooth country-specific needs. This makes the euro area countries that have weak fundamentals more prone to distress.

The United States and Japan make up the largest share of public debt in advanced economies, but their debt poses less of a worry.

US debt instruments are used as reserve assets because of their high credit quality and because the US government bond market is the world's deepest and most liquid.

So it's no wonder that US government debt benefits from strong global demand, particularly from China. For Japan, most of its public debt is held domestically, which mitigates the risk.

My third concern is about corporate leverage. Growth in corporate debt can be a good thing, especially when companies are borrowing to invest in new capacity. But it has exploded over the past decade and has some risky qualities.

In China alone, non-financial corporate debt totals about US$21 trillion. That's one and a half times China's GDP and much higher than levels in most advanced or developing economies.

This was fuelled in part by very rapid growth in domestic non-bank financial institutions, or the "shadow" banking sector, where there aren't as many safeguards as in the traditional banking sector.

All that debt poses a financial stability risk for China-which could flow to Canada through lower demand for our exports and prices for our commodities, and turbulence in global financial markets.

Non-financial corporate debt in other emerging markets amounts to about US$10 trillion. Around one-third of it is denominated in US dollars. Foreign-currency debt can be riskier than domestic-currency borrowing because it exposes firms to exchange rate risk if they don't have hedges in place.

We saw during the Asian crisis in the 1990s how sovereign debt that was denominated in foreign currency led to financial instability that exchange rate devaluations only exacerbated. In the same way, high levels of foreign-currency corporate debt could limit the scope for exchange rate adjustments to play a stabilizing role.

Non-financial corporate debt is also a concern in some advanced economies. For instance, in the United States and the euro area, the quality of corporate debt has deteriorated. We have seen substantial growth of BBB- and lower-rated bonds and a rapid increase in leveraged loans.

Non-bank financial institutions have played the biggest role in the buildup of all this corporate debt since the crisis.

That's because global bank lending dropped off sharply as banks repaired their balance sheets and complied with stricter regulatory requirements.

The gap has been more than filled by a large increase in bond financing as the investment fund industry capitalized on opportunities created by the retreat in bank lending.

The latest figures from the Financial Stability Board (FSB) put total global assets under management for investment funds at US$45 trillion at the end of 2017.

The growth of these funds means that portfolio flows into equity and debt are now the dominant source of capital flows worldwide. There are two key reasons for this.

First, the low interest rate environment in advanced economies has spurred investors to seek higher returns abroad.

Second, the rising prominence of new products such as exchange-traded funds (ETFs) has made it easy for a broader range of investors to gain exposure to emerging-market debt and high-yield bonds.

The expansion of these products is a natural result of capital markets picking up the slack after bank lending fell off. And these products can offer investors greater diversification of risk.

What concerns me though is we don't know how these funds will react when an adverse shock hits, and how the associated portfolio flows will evolve.

We've seen more uncertainty in markets in recent months, but we haven't seen a broad and sustained increase in risk aversion.

If fund managers were to suddenly shift their asset allocations, the moves could spark a sharp reversal in portfolio debt flows.

The business models of investment funds could further amplify the resulting stresses. For instance, the liquidity of ETF shares is widely thought to be higher than that of the underlying assets.

In a stress situation, herd behaviour among ETF investors could amplify changes in asset prices and lead to widespread contagion.

What will help keep us on track?

All of this is pretty sobering. But let's remind ourselves what is in place to help keep us on track.

First, the global financial system is more resilient than it was 10 years ago.

Under the Basel III reforms, institutions that are active globally-including Canadian banks-are better capitalized. We shouldn't underestimate the importance of this.

These institutions are holding over US$2 trillion more capital than they were at the beginning of 2011 when the reforms started to be phased in. They're also holding more liquid assets and running their businesses with less leverage.

It's critical to be well prepared for rainy days. In fact, in December, Canada's Office of the Superintendent of Financial Institutions (OSFI) increased the capital buffer requirement for Canadian banks by 25 basis points, to 1.75 per cent of total risk-weighted assets.

Stress tests of the Canadian banks are a useful way to assess how much pressure could be placed on their capital in very tough but plausible scenarios. Last autumn, we published results from a hypothetical scenario that involved falling house prices. The exercise showed that our banks could handle such a shock.

We'll show more of this kind of work in the next Financial System Review, to be published in May.

OSFI's B-20 mortgage underwriting guidelines are also adding to resilience. The guidelines have improved the quality of new lending by limiting the number of new mortgage holders that are highly indebted.

Along with higher interest rates, the new guidelines have also limited growth in credit. As a result, we're finally seeing the ratio of household debt to income stabilize.

Second, China is deleveraging, which is critical for its economy and for the world.

China has taken meaningful action, including more stringent regulation and supervision of the financial sector. This strategy has helped to slow credit growth. It's also shrinking certain parts of the non-bank financial sector.

This is a good thing because that sector is less capitalized, less liquid and much more opaque than traditional banks.

All of this is contributing to slower growth in China, but it's the right path to more sustainable growth in the future. Unfortunately, the trade conflict is making what was already a delicate balancing act for the Chinese authorities even tougher.

Finally, economic growth will make public debt more sustainable-if we play our cards right.

Research has found that the costs of public debt are low when a country's economic growth rate is higher than the inflation-adjusted interest rate on its public debt.

It's just arithmetic. In this situation, growth will keep debt as a percentage of GDP on a stable or declining path, even if a country is running a limited budget deficit.

If new borrowing follows the golden rule of fiscal policy-borrowing to make investments that support stronger long-term growth, such as infrastructure-then there is even more scope for debt to grow while remaining sustainable.

According to Bank estimates, many countries could grow over the medium term at a rate that exceeds the interest rate on their debt. Should countries stay on this growth path and governments limit new borrowing, current public debt loads could be more sustainable.

It's important to remember that a stable debt-to-GDP ratio does not guarantee sustainability.

A credible macroeconomic framework is critical to maintaining faith in a government's creditworthiness, achieving growth and avoiding instability.

Sound fiscal and monetary policies are at the core of this.

That includes maintaining or building some fiscal space for when it's needed.

This was the case in Canada when fiscal stimulus was used to respond to the global financial crisis and to the oil price shock a few years ago.

This helps central banks achieve their inflation objectives, which is our part in supporting strong and sustainable growth.

We also saw the importance of sound policy frameworks late last year as capital flowed out of emerging-market economies. Investors clearly differentiated between countries that had sound frameworks and those that didn't, which limited the spillovers.

What else still needs to happen?

We're in a better place than you might glean from the news. But that doesn't mean there is nothing left to do-there certainly is.

High leverage will always be an important vulnerability because of its hooks into the rest of the global financial system. We need to better understand these linkages to determine if additional safeguards are needed.

The best way is to keep running stress tests on different aspects of the financial system. The auto industry has tested air bags in cars for a long time for how they perform in different types of collisions. "Crash-testing" for banks only became standard practice relatively recently.

More needs to be done to extend this type of analysis to newer players in the system, such as asset managers and other non-bank financial institutions. This is quite challenging because their activity often crosses borders, and the ecosystem that needs to be modelled is very complex.

The Bank of Canada and the FSB are both looking at how to model these interlinkages.

I find work to stress-test the system particularly worthwhile because it helps identify where safeguards should be maintained or strengthened.

Regulators around the world also need to continue to make good use of macroprudential policies to address localized vulnerabilities as they emerge.

Even if these types of policies slow economic growth in the short term, they'll help avoid more painful adjustments in the long run. This is important for both advanced and emerging-market economies.

Individuals play a role as well. As I said at the beginning, high leverage can leave any of us in a vulnerable financial position.

I'm hoping that prospective homeowners and other borrowers do their own stress tests so that they can be confident that the debt they take on will be manageable over time.

Before I conclude, let me take a minute to say what we should absolutely not do: have a trade war.

Advocates of protectionist measures say that imposing barriers like tariffs on countries with trade surpluses will help reduce disparities in international trade and lead to more domestic production and jobs.

This logic may be seductive, but it's misguided. In a trade war, no one gains and everyone loses. Tariffs lower GDP for everyone because they harm investment and productivity.

That's why it would be good for everyone if the United States and China resolved their dispute. An end to US tariffs on steel and aluminum would also be a welcome relief to many businesses and workers in Canada and other affected countries. And, of course, the Canada-United States-Mexico Agreement still needs to be ratified.

Even with these steps, getting over the general malaise around trade policies will require some tangible commitment and a plan to modernize the World Trade Organization's trade rules-including for intellectual property-and its dispute settlement mechanism.

This would pave the way for higher global growth and a more sustainable debt burden.

Conclusion

It's time for me to conclude.

Global debt is now more than three times global GDP. That is a headwind to growth and makes us vulnerable to another period of financial instability.

The good news for Canadian businesses and households is that the financial system-globally and here at home-is safer than it was a decade ago thanks to much stronger safeguards. And, the global expansion is expected to continue even though it has slowed in recent quarters.

For Canada, the economy is likely to be weaker in the first half of this year than we had forecast in January, but we still expect GDP growth to pick up later in the year.

That said, more needs to be done to further reduce the downside risks. A long-lasting resolution to the current trade war is at the top of my list because the conflict is threatening growth around the world right now.

Credible fiscal and monetary policies, and nimble financial system safeguards, are at the core of limiting vulnerabilities and promoting longer-term resilience for all countries.

What's at stake is the future prosperity of many people, at a time when stability is sorely needed.

I would like to thank Rhys Mendes, Gitanjali Kumar and Grahame Johnson for their help in preparing this speech.

Number 9

Cybersecurity Disclosure Act of 2019?

Will publicly traded companies be required to disclose to investors whether any members of their board of directors have cybersecurity expertise?

A BILL

To amend the Securities Exchange Act of 1934 to promote transparency in the oversight of cybersecurity risks at publicly traded companies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity Disclosure Act of 2019".

To read more:
https://www.congress.gov/116/bills/s592/BILLS-116s592is.pdf

Number 10

Progress on Lifelong Learning Machines Shows Potential for Bio-Inspired Algorithms

USC milestone on L2M program shows how machines could be capable of learning through experience

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Today's machine learning systems are restricted by their inability to continuously learn or adapt as they encounter new situations; their programs are fixed after training, leaving them unable to react to new, unforeseen circumstances once they are fielded.

Adding new information to cover programming deficits overwrites the existing training set.

With current technology, this requires taking the system offline and retraining it on a dataset that incorporates the new information.

It is a long and arduous process that DARPA's Lifelong Learning Machines (L2M) program is working to overcome.

"The L2M program's prime objective is to develop systems that can learn continuously during execution and become increasingly expert while performing tasks, are subject to safety limits, and capable of applying previous skills and knowledge to new situations, without forgetting previous learning," said Dr. Hava Siegelmann, program manager in DARPA's Information Innovation Office (I2O). "Though complex, it is an area where we are making significant progress."

First announced in 2017, L2M is over a year into research and development of next generation AI systems and their components, as well as learning mechanisms in biological organisms capable of translation into computational processes. L2M supports a large base of 30 performer groups via grants and contracts of different duration and size.

Today, L2M researcher Francisco J. Valero-Cuevas, professor of biomedical engineering and biokinesiology at USC Viterbi School of Engineering, along with USC Viterbi School of Engineering doctoral students Ali Marjaninejad, Dario Urbina-Melendez and Brian Cohn published results regarding exploration into bio-inspired AI algorithms. In an article outlined in the March cover of Nature Machine Intelligence, Valero-Cuevas' team details their successful creation of an AI-controlled robotic limb driven by

animal-like tendons capable of teaching itself a walking task, even automatically recovering from a disruption to its balance.

Behind the USC researchers' robotic limb is a bio-inspired algorithm that can learn a walking task on its own after only five minutes of "unstructured play" – or conducting random movements that enable the robot to learn its own structure as well as its surrounding environment.

The robot's ability to learn-by-doing is a significant advancement towards lifelong learning in machines. The current machine learning approaches rely on pre-programming a system for all potential scenarios, which is complex, labor intensive, and inefficient.

What the USC researchers have accomplished shows that it is possible for AI systems to learn from relevant experience, finding and adapting solutions to challenges overtime.

Siegelmann noted, "We're at a major moment of transition in the field of AI. Current fixed methods underlying today's smart systems will quickly give way to systems capable of learning in the field. The missing ingredients to safer, more flexible, and more useful AI are the abilities to both learn while in operation and to apply learning to new circumstances for which the system was not previously trained. These abilities are necessary, for instance, for complex systems like self-driving cars to become truly functional. Incorporating L2M technologies will allow them to become increasingly expert as they drive in different conditions and will make them safer than human-driven cars. Professor Valero-Curevas and his team have successfully taken us closer to that goal; that's what the L2M project is about."

The full article: https://www.nature.com/articles/s42256-019-0029-0

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.

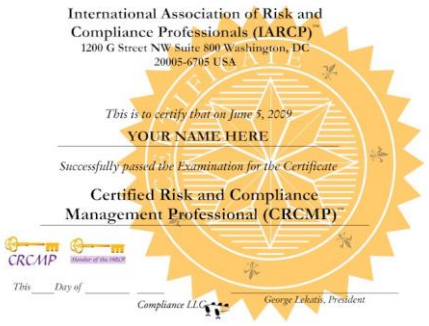
You may visit:
www.risk-compliance-association.com/How_to_become_member.htm

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.



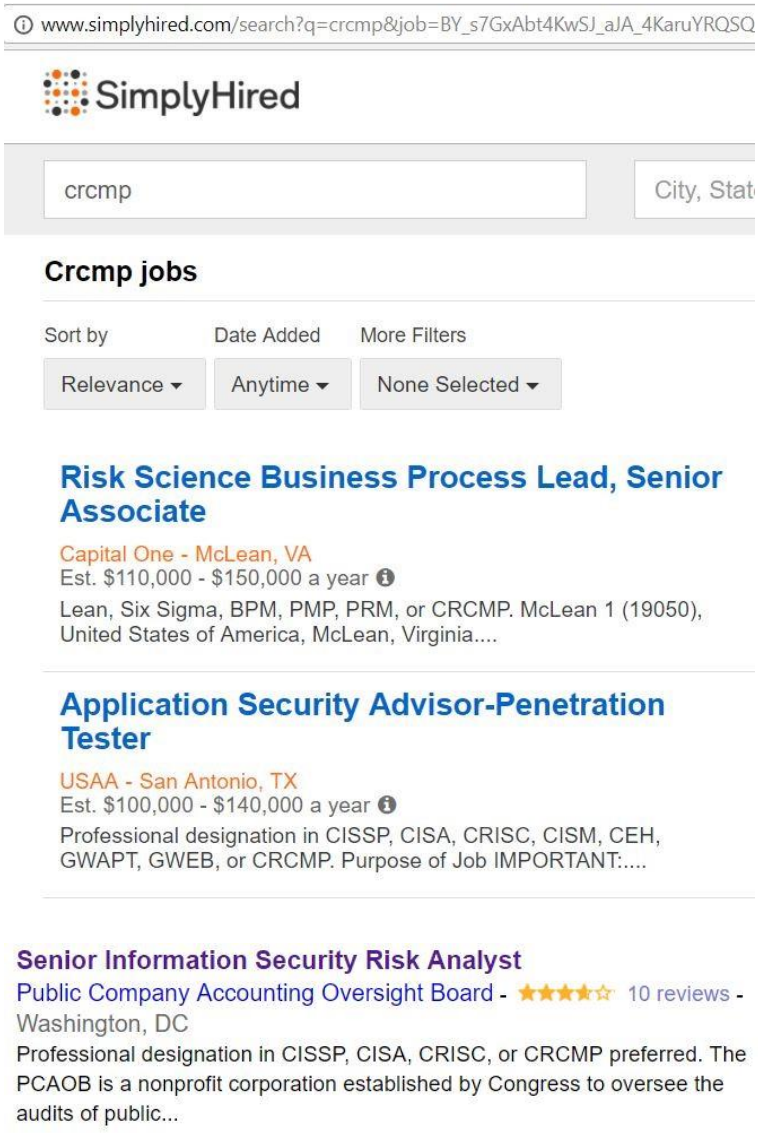
There are CRCMPs in 32 countries around the world. Companies and organizations like Accenture, American Express, USAA etc. consider the CRCMP a preferred certificate.

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.

Some CRCMP jobs:



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