Computational propaganda is the use of technology for political manipulation.

It becomes increasingly easy to influence emotions, attitudes, opinions, and actions of an audience for ideological or political purposes, through the transmission of messages (factual or not) using technology.

State-sponsored trolling and disinformation have proved to be very effective, and the cost of the implementation is very low, as “bots” are a common type of autonomous agents used in computational propaganda.

But today we have some good news. Do you remember Executive Order 13800, about “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” calling for “resilience against botnets and other automated, distributed threats”?

According to the Executive Order, the Secretary of Commerce and the Secretary of Homeland Security must “lead an open and transparent process to identify and promote action by appropriate stakeholders” with the goal of “dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets).”
Automated and distributed attacks form a threat that reaches beyond any single country, company or sector. These threats are used for a variety of malicious activities, including distributed denial of service (DDoS) attacks that overwhelm networked resources, ransomware attacks that hold systems and data hostage, and computational propaganda campaigns to manipulate and intimidate communities through social media.

*Today we have a draft report* to the President, that was developed by the Departments of Commerce and Homeland Security in response to Executive Order 13800. The Departments determined that the opportunities and challenges in working toward dramatically reducing threats from automated, distributed attacks can be summarized in six principal themes:

1. Automated, distributed attacks are a global problem.
2. Effective tools exist, but are not widely used.
3. Products should be secured during all stages of the lifecycle.
4. Education and awareness is needed.
5. Market incentives are misaligned.
6. This is an ecosystem-wide challenge.

The Departments identified five complementary and mutually supportive goals that would dramatically reduce the threat of automated, distributed attacks and improve the resilience of the ecosystem.

A list of suggested actions for key stakeholders reinforces each goal.

The goals are:

**Goal 1:** Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace.

**Goal 2:** Promote innovation in the infrastructure for dynamic adaptation to evolving threats.

**Goal 3:** Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior.
Goal 4: Build coalitions between the security, infrastructure, and operational technology communities domestically and around the world.

Goal 5: Increase awareness and education across the ecosystem.

Read more at Number 1 below. Welcome to the Top 10 list.

Best Regards,

George Lekatis
President of the IARCP
General Manager, Compliance LLC
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)


Number 2 (Page 10)

Argentina to host over 45 G20 meetings in 2018

Around 20,000 people will visit Argentina in 2018 for the G20. The final event will be the Leaders' Summit on 30 November and 1 December.

Argentina took over the presidency of the G20 on 1 December 2017, with the forum’s main activities taking place over the course of 2018: more than 45 meetings in 11 cities across the country.

Number 3 (Page 12)

Opinion on the supervisory assessment of internal models including a dynamic volatility adjustment
What is a common supervisory culture?

A common supervisory culture is one where there is a common understanding of the way supervisors think, behave, and work within their community.

Key Attributes Assessment Methodology for the Insurance Sector: Consultative Document

This consultation sets out a proposed methodology for assessing the implementation of the Key Attributes of Effective Resolution Regimes for Financial Institutions (“Key Attributes”) in the insurance sector.

Configuration Security Program to Make Network-Connected Systems Less Vulnerable

The rise of network-connected systems that are becoming embedded seemingly everywhere—from industrial control systems to aircraft avionics—is opening up a host of rich technical capabilities in deployed systems.
Number 7 (Page 19)
eIDAS Regulation, on electronic identification and trust services for electronic transactions

Technical guidelines on trust services

Regulation (EU) No 910/20141 (hereafter the eIDAS Regulation), on electronic identification and trust services for electronic transactions in the internal market, provides a regulatory environment for electronic identification of natural and legal persons and for a set of electronic trust services, namely electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.

Number 8 (Page 21)
A blind spot in today's macroeconomics?

Panel remarks by Mr Claudio Borio, Head of the Monetary and Economic Department of the BIS, at the BIS-IMF-OECD Joint Conference on "Weak productivity: the role of financial factors and policies", Paris.

“A standard presumption in today's macroeconomics is that when making sense of first-order macroeconomic outcomes we can treat the economy as if its output were a single good produced by a single firm.

This means that issues of resource misallocation can be safely ignored.

But the link between resource misallocations and macroeconomic outcomes may well be tighter than we think.”
Current developments in the area of financial stability in Switzerland

Introductory remarks by Mr Fritz Zurbrügg, Member of the Governing Board of the Swiss National Bank, at the Media News Conference of the Swiss National Bank, Berne.

“In my remarks today, I would like to address some of the developments currently taking place in the field of financial stability.

I shall look at the big banks first before turning to the domestically focused banks. I will conclude with a few words on the new banknote series.”

ENISA and eu-LISA boost cooperation

The European Union Agency for Network and Information Security (ENISA) and the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) signed a Memorandum of Understanding (MoU) to strengthen their cooperation.
Number 1


“Cybersecurity is perhaps one of the most serious threats we face,” said Secretary Ross. “President Trump understands the necessity of strengthening our networks and this Administration is doing everything in its power to prevent bad actors from infiltrating our critical cyber infrastructure.”

The report, which was created with broad input from stakeholders and experts, summarizes the opportunities and challenges in reducing the botnet threat, and offers supporting actions to be taken by both the government and private sector in order to reduce the threat of automated cyber-attacks.

The report lists five complementary goals that would improve the resilience of the ecosystem:

1. Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace.

2. Promote innovation in the infrastructure for dynamic adaptation to evolving threats.

3. Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior.

4. Build coalitions between the security, infrastructure, and operational technology communities domestically and around the world.

5. Increase awareness and education across the ecosystem.
“Botnets represent a system-wide threat that no single stakeholder, not even the federal government, can address alone,” said Walter G. Copan, Under Secretary of Commerce for Standards and Technology and Director of the National Institute of Standards and Technology.

“The report recommends a comprehensive way for the public and private sectors, as well as our international partners, to work together and strengthen our defenses.”

You may visit:

Argentina to host over 45 G20 meetings in 2018

Around 20,000 people will visit Argentina in 2018 for the G20. The final event will be the Leaders' Summit on 30 November and 1 December.

Argentina took over the presidency of the G20 on 1 December 2017, with the forum’s main activities taking place over the course of 2018: more than 45 meetings in 11 cities across the country.

Argentina will play host to over 20,000 participants from abroad, mainly officials from G20 member governments and international organizations, and members of the press.

The G20 meetings will cover a number of issues, including agriculture, the digital economy, education, employment, energy, finance, trade & investment, amongst others.

The three main priorities of the Argentine presidency – the future of work, infrastructure for development and a sustainable food future – are themes that will cut across the entire G20 agenda, as will other important transversal issues, such as gender equality.

The Argentine presidency’s objective is to build consensus amongst the world’s major powers for development that is both fair and sustainable, and that will generate opportunities for everyone.

It is closely in line with the concerns and aspirations of the region of Latin America and the Caribbean to harness its populations’ great economic potential and boost efforts to eradicate poverty.
The first G20 meeting of the year is on the Data Gaps Initiative (DGI) and will take place on **29 and 30 January** in Buenos Aires.

Organized by the National Institute of Statistics and Census of Argentina (INDEC), the meeting will address issues relating to collecting and disseminating comparable, integrated and standardized statistics of high quality to craft public policies.

The G20 agenda includes a further five meetings in February, also in the Argentine capital. On 12-13 March, the city of Rosario will become the third city after Bariloche and Buenos Aires to host a G20 meeting, in this case, the first meeting of Agriculture Deputies.

In the lead up to the annual Leaders' Summit, numerous meetings will take place at technical (‘working group’), deputy minister, and minister levels.

The latter is the most important of these, attended by ministers of G20 countries and their equivalents in G20 partner organizations. The **first minister-level meeting** of the year will be the first of five meetings of Finance Ministers and Central Bank Governors, taking place on 19-20 March in Buenos Aires.

Other cities across Argentina will host G20 ministerial, deputy and working group meetings. These are Salta, San Salvador de Jujuy and San Miguel de Tucumán in the northwest; Puerto Iguazú in the northeast; Mendoza in the west; Rosario and Córdoba in the centre; Mar del Plata and Buenos Aires in the east; and Bariloche and Ushuaia in the south.

The G20 working year concludes in Buenos Aires with the Leaders' Summit on 30 November and 1 December, which will **close with a joint declaration** of the G20 heads of state and government.

The calendar:
[https://www.g20.org/en/calendar](https://www.g20.org/en/calendar)
Opinion on the supervisory assessment of internal models including a dynamic volatility adjustment

The European Insurance and Occupational Pensions Authority (EIOPA) issues this opinion on the basis of Article 29(1)(a) of Regulation (EU) No 1094/20101.

According to this article, EIOPA shall play an active role in building a common supervisory culture and consistent supervisory practices and approaches throughout the Union.

This opinion is based on Directive 2009/138/EC (Solvency II Directive), Commission Delegated Regulation (EU) 2015/35 (Delegated Regulation), and EIOPA’s guidelines and other relevant instruments.

To read more: https://eiopa.europa.eu/Publications/Opinions/2017-12-20%20EIOPA-BoS-17-366_Internal_model_DVA_Opinion.pdf
What is a common supervisory culture?

A common supervisory culture is one where there is a common understanding of the way supervisors think, behave, and work within their community.

The culture manifests itself in processes, procedures and behaviours.

To learn more:

Key Attributes Assessment Methodology for the Insurance Sector: Consultative Document

This consultation sets out a proposed methodology for assessing the implementation of the Key Attributes of Effective Resolution Regimes for Financial Institutions (“Key Attributes”) in the insurance sector.

The Key Attributes Assessment Methodology for the Insurance Sector sets out essential criteria to guide the assessment of the compliance of a jurisdiction’s insurance resolution frameworks with the Key Attributes.

It is designed to promote consistent assessments across jurisdictions and to provide guidance to jurisdictions when adopting or reforming insurance resolution regimes to implement the Key Attributes.

It will also be used by the International Monetary Fund (IMF) and the World Bank as part of the regulatory assessments they undertake.

The Key Attributes remain the umbrella standard for resolution regimes covering financial institutions of all types that could be systemic in failure.

The FSB decided to adopt a ‘modular approach’ and develop self-contained and free-standing methodologies tailored to the particular features of each sector in order to facilitate sector-specific assessments of the Key Attributes.

In October 2016 it published the Key Attributes Assessment Methodology for the Banking Sector. You may visit: http://www.fsb.org/wp-content/uploads/Key-Attributes-Assessment-Meth

odology-for-the-Banking-Sector.pdf

Following that, the FSB has now developed in close cooperation with the IMF, World Bank and the International Association of Insurance Supervisors a Key Attributes Assessment Methodology for the Insurance Sector.

Key Attributes Assessment Methodology for the Insurance Sector

Methodology for Assessing the Implementation of the Key Attributes of Effective Resolution Regimes for Financial Institutions in the Insurance Sector

Consultative Document

Note: The Financial Stability Board (FSB) is established to coordinate at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies.

Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations under the FSB’s Articles of Association.
Configuration Security Program to Make Network-Connected Systems Less Vulnerable

The rise of network-connected systems that are becoming embedded seemingly everywhere—from industrial control systems to aircraft avionics—is opening up a host of rich technical capabilities in deployed systems.

Even so, as the collective technology project underlying this massive deployment of connectivity unfolds, more consumer, industrial, and military players are turning to inexpensive, commodity off-the-shelf (COTS) devices with general-purpose designs applicable for a range of functionalities and deployment options. While less costly and more flexible, commodity components are inherently less secure than the single-purpose, custom devices they are replacing.

“With commodity devices, software and configuration settings now govern behaviors that were physically impossible in special-purpose hardware, creating security risks and increasing system vulnerability,” said Jacob Torrey, program manager in DARPA’s Information Innovation Office (I2O).

“Certain functionality built into COTS components may not be necessary for all users or applications, and unwanted functionality can be hard to detect and turned-off. For instance, an unneeded maintenance or diagnostic service left enabled could create an opportunity for an attacker to circumvent other security controls and use the system’s as-deployed functionality to generate a malicious effect.

This opaqueness is creating challenges for system operators who must rely on component configurations to reduce attack surfaces created by unnecessary functionality.”

To address the challenges created by the proliferation of COTS devices and help harden the security surface of network-connected composed systems, DARPA has launched a new program called Configuration Security (ConSec).
The program, just announced today, aims to develop a system to automatically generate, deploy, and manage inherently more secure configurations of components and subsystems for use in military platforms.

“Through ConSec we hope to gain a better understanding of the available functionality across COTS devices and what’s needed for the task at hand and then use system configurations to create the functionality that’s actually required while minimizing the excess that can be used as an attack surface,” said Torrey.

“While our objective is to build this capability for military platforms, there is the potential for the program to have broader applications for commercial and industrial systems as well.”

Prospective performers are tasked with finding ways to automate the traditionally more manual process of system configuration. To tackle this feat, the program is divided into two technical areas.

The first area focuses on reducing the amount of human-in-the-loop time required to understand what capabilities a system needs to deliver across different operating environments, the functionality required to achieve its mission in each operating environment, and the possible component configurations needed to create the desired functionality.

“Consider, for example, a naval vessel. Its functionality when at sea is likely different than what’s required of it while at port, or in dry-dock undergoing maintenance,” said Torrey. “Our aim is to automate the process of identifying these different operating environments, the system’s expected functionality in each scenario, and the components needed to make it all happen, which is currently a manual, labor intensive process.”

To accomplish this, DARPA is asking researchers to develop models and functional specifications of systems based on human-friendly information formats—such as checklists, operating manuals, and other written human standard operating procedures (SOPs)—as well as an analysis of the system’s underlying components’ hardware and firmware.

Input from these analyses should help determine how settings in a component’s configuration space might impact its functionality, how the behavior of human operators impacts system behavior, and what operational and mission contexts pertain for the full, composed system.
The ConSec program’s second technical area focuses on uncovering component configurations that will enable the composed system to achieve its mission under different, relevant operational contexts.

Here proposers are asked to leverage the models and functional specifications that emerge from work in the first technical area to find ways of identifying secure configurations that eliminate unused and unnecessary functionality as a way to shrink the system’s vulnerabilities to attack.

“Essentially we’re asking potential performers to determine how to take all of the best pieces and functionality and combine them to fulfill the requirements of a high-level composed system while turning off all of the things we don’t need,” said Torrey.

Torrey expects that the program will roll out in three phases over the next three-and-a-half years.

The deadline for proposals for the ConSec program is February 8, 2018.

Additional details about the program can be found via the DARPA Broad Agency Announcement, found at:

https://www.fbo.gov/index?s=opportunity&mode=form&id=c889999b044a8b485da8884d7fbab391&tab=core&_cview=1
eIDAS Regulation, on electronic identification and trust services for electronic transactions

Technical guidelines on trust services

Regulation (EU) No 910/20141 (hereafter the eIDAS Regulation), on electronic identification and trust services for electronic transactions in the internal market, provides a regulatory environment for electronic identification of natural and legal persons and for a set of electronic trust services, namely electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.

It is possible to use those trust services as well as electronic documents as evidence in legal proceedings in all EU Member States contributing to their general cross-border use.

Courts (or other bodies in charge of legal proceedings) cannot discard them as evidence only because they are electronic but have to assess these electronic tools in the same way they would do for their paper equivalent.

To further enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the eIDAS Regulation introduces the notions of qualified trust service and qualified trust service provider with a view to indicating requirements and obligations that ensure high-level security and a higher presumption of their legal effect.

Following the publication of the eIDAS Regulation, a set of secondary and co-regulatory acts had to be published in order to provide technical guidance on how to implement the specific requirements of the eIDAS Regulation (in the TSP part of eIDAS, the European Commission decided to publish only the mandatory ones).
ENISA aimed to develop a concise set of technical guidelines implementing the eIDAS Regulation in the non-mandatory articles, for voluntary use of all stakeholders, including Trust Service Providers, Supervisory Bodies and Conformity Assessment Bodies.

The objective of this document is to provide guidelines for fulfilling requirements originating from the following articles of the eIDAS Regulation:

- Art. 24.5 – Requirements for qualified trust service providers;
- Art. 28.6 – Qualified certificates for electronic signatures;
- Art. 32.3 – Requirements for the validation of qualified electronic signatures;
- Art. 33.2 – Qualified validation service for qualified electronic signatures;
- Art. 34.2 – Qualified preservation service for qualified electronic signatures;
- Art. 38.6 – Qualified certificates for electronic seals;
- Art. 42.2 – Requirements for qualified electronic time stamps;
- Art. 44.2 – Requirements for qualified electronic registered delivery services;
- Art. 45.2 – Requirements for qualified certificates for website authentication

To learn more:
A blind spot in today’s macroeconomics?

Panel remarks by Mr Claudio Borio, Head of the Monetary and Economic Department of the BIS, at the BIS-IMF-OECD Joint Conference on "Weak productivity: the role of financial factors and policies", Paris.

A standard presumption in today's macroeconomics is that when making sense of first-order macroeconomic outcomes we can treat the economy as if its output were a single good produced by a single firm.

This means that issues of resource misallocation can be safely ignored.

But the link between resource misallocations and macroeconomic outcomes may well be tighter than we think.

This speech illustrates the point with reference to two examples that highlight the link between finance and macroeconomics: the impact of resource misallocations induced by financial booms and busts on productivity growth, and an intriguingly close relationship between the growing incidence of "zombie" firms and declining interest rates since the 1980s.

To read more: https://www.bis.org/speeches/sp180110.pdf
Current developments in the area of financial stability in Switzerland

Introductory remarks by Mr Fritz Zurbrügg, Member of the Governing Board of the Swiss National Bank, at the Media News Conference of the Swiss National Bank, Berne.

In my remarks today, I would like to address some of the developments currently taking place in the field of financial stability.

I shall look at the big banks first before turning to the domestically focused banks. I will conclude with a few words on the new banknote series.

Big banks

As Thomas Jordan has already noted, the international economic environment has continued to improve since the last news conference in June.

Conditions on the financial markets have remained stable.

Premia for bank credit default swaps, for instance, have barely changed since June. Premia have thus settled at lower levels again following the turbulence in 2016.

Against this positive backdrop, both of Switzerland’s big banks remain on track to meet the requirements of the ‘too big to fail’ regulations with respect to resilience.

This first pillar of the regulations covers requirements pertaining to the going-concern loss-absorbing capacity of systemically important banks. Both Credit Suisse and UBS already comply fully with the final1, risk-weighted requirements.
However, further improvement is needed with respect to the leverage ratio. Both of the big banks have also made progress on the second pillar of the regulations, ‘resolution’, which covers the orderly restructuring and wind-down of a bank that can no longer function as a going concern and is thus deemed to have become a gone concern.

With a view to managing such a crisis scenario, Credit Suisse as well as UBS have increased their gone-concern loss-absorbing capacity by issuing further bail-in instruments, which can be converted into equity in the event of impending insolvency.

As we explained in our Financial Stability Report published in June, since the ‘too big to fail’ regulations came into force, Credit Suisse and UBS have also taken important organisational steps to improve their resolvability.

Despite these positive developments, the two big banks still need to make further progress if they are to fully comply with the second-pillar requirements.

This applies both to their gone-concern loss-absorbing capacity and their resolution planning. Full compliance with all of the ‘too big to fail’ requirements will further strengthen the big banks’ going and gone-concern loss-absorbing capacity as well as improve their resolvability in a crisis.

Both of these sets of requirements must be addressed if Switzerland’s ‘too big to fail’ problem is to be solved. Domestically focused banks I would now like to turn to the domestically focused banks. These institutions’ biggest risks continue to stem from the mortgage and real estate markets.

I will make three points in this regard.

First, imbalances on the mortgage and real estate markets persist. Although mortgage growth has remained relatively low in 2017 – as in the previous year – developments on the real estate market show a somewhat different picture: price growth in the residential property segment had been falling since 2013, but recently transaction prices have started to pick up again.

Moreover, with the exception of a few quarters (including the third quarter of 2017), prices in the residential investment property segment have risen markedly since 2013. As prices over this period have increased more strongly than fundamentals such as rents, risks have accumulated in this segment; it is thus especially vulnerable to a substantial correction in the medium term.
This situation is compounded by brisk construction activity in the rental apartments segment, which could lead to oversupply. Signs of this can already be seen in rising vacancy rates.

**Second**, the risk appetite of domestically focused banks remains high. This is particularly evident from the affordability risk data. The share of new mortgages with high loan-to-income ratios has risen significantly in recent years and has reached a historical high.

The interest rate risk of domestically focused banks likewise remains high, while their interest margin continued to decline in the first half of 2017. As long as there is pressure on margins, incentives for domestically focused banks to increase risk-taking will remain substantial.

**Third**, notwithstanding the risks in the macroeconomic environment and the banks’ high risk appetite, SNB stress tests continue to suggest that, overall, domestically focused banks’ resilience remains adequate.

Thanks to robust capitalisation, most of these banks would be able to absorb the losses likely to be incurred in adverse scenarios; given the risks I have outlined, this is welcome.

In the future, too, it will be decisive for the stability of the financial system that banks hold sufficient capital to cover the risks on their books – irrespective of ongoing margin pressure.
ENISA and eu-LISA boost cooperation

The European Union Agency for Network and Information Security (ENISA) and the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) signed a Memorandum of Understanding (MoU) to strengthen their cooperation. The signing took place at ENISA’s premises in Athens, Greece.

Prof. Dr. Udo Helmbrecht, Executive Director of ENISA, said: “We welcome the opportunity to work with eu-LISA and to share our expertise with them. This MoU is another example of EU Agencies sharing resources and working closely together.”

“At today we are all part of a digital revolution that deeply changes all aspects of our daily lives. The very nature of the latest technical and cyber solutions require close cooperation, information sharing and the pooling of expertise in order to make the best use of the existing physical information and networks whilst smartly managing modern cyber threats. The working arrangement with ENISA, signed today, helps us to achieve this,” noted Krum Garkov.

The MoU, signed by the heads of the two agencies Udo HELMBRECHT from ENISA and Krum GARKOV from eu-LISA, takes the ongoing successful teamwork between the two agencies to a new level. The formalised cooperation agreement permits to further increase the added value, which derives from the exchange of expertise and best practices between these trusted agencies.

eu-LISA and ENISA will intensify cooperation in the areas of information security and business continuity, the provision of training for EU Member States and ICT related strategic-administrative matters with the aim to provide the best possible services to the stakeholders of both agencies.

Background:

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. ENISA is
contributing to a high level of network and information security (NIS) within the European Union, by developing and promoting a culture of NIS in society to assist in the proper functioning of the internal market.

The European Agency eu-LISA manages large-scale information systems in the area of freedom, security and justice.

It operates Eurodac, the second generation Schengen Information System (SIS II) and the Visa Information System (VIS).

eu-LISA is responsible for keeping the IT systems under its control fully functional in order to allow continuous and uninterrupted exchange of data between national authorities.

eu-LISA ensures that it applies the highest level of information security and data protection to the information it is entrusted with.
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: 

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.


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