*Monday, January 21, 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,

Every time I read an *After Action Report*, I remember Confucius, who believed that the superior man acts before he speaks, and afterwards speaks according to his action.

The *Cyber Europe 2018 After Action Report* of the European Network and Information Security Agency (ENISA) is very interesting. It describes the simulation of an intense realistic crisis caused by a large-number of cybersecurity incidents that occurred during the two-days, 6-7 June 2018.

The detailed scenario of the exercise consisted of numerous materials including:

- Structured and unstructured, useful and misleading data scattered in simulated online blogs, magazines, forums and file storage infrastructure;

- Thousands of simulated personal and professional social media profiles on multiple simulated platforms;

- A simulated news channel, depicting the event through filmed news in a realistic fashion, supported by simulated formal news websites containing hundreds of news articles and formal news websites;

- Hundreds of tailor-made documents supporting the scenario for participants to analyse, from technical incident material to legal and public affairs documents.

During the exercise, live media pressure was simulated by real journalists who were continually contacting players to ask for information. Real-time

response by the experts was noted, while dynamic media reactions in simulated social media were added by the journalists.

The scenario was set around the concept of the worldwide rise of extremism. This 'virtually invisible' phenomenon has turned into an open and widespread one with several different facets, from religion to political beliefs, engaging thousands of followers and millions of supporters.

The number of radical websites has increased exponentially since 2013 and extremists are utilising social media to recruit and organise.

The increase of the followers of this extremism lead to their engagement in cyber-attacks. Radical groups could use advanced or less advanced techniques to strike at any time as they revealed the internet to be a hotbed of radicalisation.

A new radicalistic movement, without a central organisation has a powerful arsenal of cyber-attack techniques with capabilities, such as exfiltration, traffic capturing and logging, keylogging, ransomware, hybrid attacks with drones, IoT infectors, worms, etc.

Read more at Number 8 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 7)*

## PCAOB Adopts New Estimates Standard and Amendments Related to Using the Work of Specialists

The Public Company Accounting Oversight Board has adopted a new standard to enhance the requirements that apply when auditing accounting estimates, including fair value measurements.

*Number 2 (Page 10)*

## National Money Laundering Risk Assessment, 2018

The 2018 National Money Laundering Risk Assessment (2018 NMLRA) identifies the money laundering threats, vulnerabilities, and risks that the United States currently faces, updating the 2015 National Money Laundering Risk Assessment (2015 NMLRA).

*Number 3 (Page 12)*

## Treasury Publishes National Illicit Finance Strategy and Supporting Risk Assessments

The U.S. Department of the Treasury has issued the National Strategy for Combating Terrorist and Other Illicit Financing (National Illicit Finance

Strategy), pursuant to Sections 261 and 262 of the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA).

The Strategy describes and assesses current U.S. government efforts to combat illicit finance threats and risks and identifies priorities, objectives, and potential areas for future improvement.

*Number 4 (Page 15)*

## Reminder to firms on their MiFID obligations on disclosure of information to clients in the context of the United Kingdom withdrawing from the European Union

esma European Securities and Markets Authority

The European Securities and Markets Authority (ESMA) is issuing this Statement to remind investment firms and credit institutions providing investment services (collectively referred to as "firms") of their obligations to provide clients with accurate disclosure on the impact on the provision of services and investors' rights that may emerge from the withdrawal of the United Kingdom from the European Union (EU).

*Number 5 (Page 17)*

## CP18/44: Brexit – Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication

FCA FINANCIAL CONDUCT AUTHORITY

In this Consultation Paper we propose to make regulatory technical standards for strong customer authentication and common and secure open standards of communication, which will apply in the UK from 14 September 2019 in the event of a no-deal exit by the UK from the EU.

A number of provisions of the SCA-RTS are effective from 14 March 2019, including the requirement to make testing facilities available if providing access to account information or payment initiation service providers. The remainder of the SCA-RTS will take effect on 14 September 2019.

*Number 6 (Page 19)*

## FINMA publishes ICO guidelines

*Revisiting the guidelines after one year*

In guidelines published, the Swiss Financial Market Supervisory Authority FINMA sets out how it intends to apply financial market legislation in handling enquiries from ICO organisers.

The guidelines also define the information FINMA requires to deal with such enquiries and the principles upon which it will base its responses, creating clarity for market participants.

*Number 7 (Page 23)*

## Rogue fitness apps help you to lose money not weight

Three malicious apps have recently been identified and removed from Apple's app store.

The apps had a health theme and purported to check heart rate, calorie count or BMI index. "Fitness Balance", "Calories Tracker" and "Heart Rate Monitor" were discovered to be fraudulent and have been removed.

*Number 8 (Page 24)*

## Cyber Europe 2018 - After Action Report

Cyber Europe 2018 was the fifth pan-European cyber crisis exercise organised by the European Union Agency for Network and Information Security (ENISA).

*Number 9 (Page 27)*

## The State of IT Security in Germany 2018

Federal Office for Information Security

Towards the end of 2017, the BSI received indications of a successful cyber attack via the National Cyber Defence Centre, which purported to affect individual German federal authorities.

The BSI started the incident handling process in coordination with the authorities involved in the National Cyber Defence Centre, informed the authorities that were potentially affected and began the analysis and verification of the information initially available.

*Number 10 (Page 29)*

## Brief summary, 2017 Report on the Protection of the Constitution Facts and Trends

Federal Ministry of the Interior, Building and Community

## Espionage and other intelligence activities

States which strive to gain a knowledge edge in military (particularly strategic) or economic and technological contexts do not hesitate to procure the necessary information secretly and illegally by violating applicable law.

In this context, their governments political agenda dictates the priority areas of the individual intelligence services‘ activities.

Germany is of interest in its role as a geopolitical player, as a member of NATO and the EU and on account of its economic strength and innovative businesses.

*Number 1*

## PCAOB Adopts New Estimates Standard and Amendments Related to Using the Work of Specialists

PCAOB
Public Company Accounting Oversight Board

The Public Company Accounting Oversight Board has adopted a new standard to enhance the requirements that apply when auditing accounting estimates, including fair value measurements.

PCAOB
Public Company Accounting Oversight Board

1666 K Street, NW
Washington, D.C. 20006
Telephone: (202) 207-9100
Facsimile: (202) 862-8430
www.pcaobus.org

| | |
|---|---|
| AUDITING ACCOUNTING ESTIMATES, INCLUDING FAIR VALUE MEASUREMENTS | PCAOB Release No. 2018-005<br>December 20, 2018 |
| AND AMENDMENTS TO PCAOB AUDITING STANDARDS | PCAOB Rulemaking<br>Docket Matter No. 043 |

The Board also adopted amendments to its auditing standards to strengthen requirements that apply when auditors use the work of specialists in an audit.

PCAOB
Public Company Accounting Oversight Board

1666 K Street, NW
Washington, DC 20006
Telephone: (202) 207-9100
Facsimile: (202) 862-8430
www.pcaobus.org

| | |
|---|---|
| AMENDMENTS TO AUDITING STANDARDS FOR AUDITOR'S USE OF THE WORK OF SPECIALISTS | PCAOB Release No. 2018-006<br>December 20, 2018 |
| | PCAOB Rulemaking<br>Docket Matter No. 044 |

The new estimates standard replaces three standards with a single, uniform standard that sets forth an updated approach to auditing accounting estimates.

It emphasizes that auditors need to apply professional skepticism, including addressing potential management bias, when auditing accounting estimates.

Additionally, the new standard provides more specific direction on auditing fair values of financial instruments that are based on information from third-party pricing sources.

The amendments adopted by the Board strengthen the requirements for evaluating the work of a company's specialist, whether employed or engaged by the company.

They also apply a supervisory approach to both auditor-employed and auditor-engaged specialists.

“The Board’s action today comes after thoughtful analysis and extensive external engagement on the prevalent use of accounting estimates and the auditor’s use of the work of specialists, recognizing that these are both challenging areas of the audit that needed to be addressed,” said PCAOB Chairman William D. Duhnke III. “These two standard-setting projects align with the PCAOB’s strategic priorities by enhancing our efforts to protect investors and strengthen auditing practices.”

More on the history of the projects, including historical documents, can be found in Rulemaking Docket 043 for the estimates standard and Rulemaking Docket 044 for the amendments.

Fact sheets on the new estimates standard and amendments for auditor's use of the work of specialists in an audit also provide additional information and resources.

Subject to approval by the Securities and Exchange Commission, the new estimates standard and amendments on the auditor’s use of the work of specialists will be effective for audits of financial statements for fiscal years ending on or after December 15, 2020.

Both standard-setting projects apply to audits conducted under PCAOB standards.

The standard:

https://pcaobus.org/Rulemaking/Docket043/2018-005-estimates-final-rule.pdf

The amendments to auditing standards:
https://pcaobus.org/Rulemaking/Docket044/2018-006-specialists-final-rule.pdf

*Number 2*

## National Money Laundering Risk Assessment, 2018

The 2018 National Money Laundering Risk Assessment (2018 NMLRA) identifies the money laundering threats, vulnerabilities, and risks that the United States currently faces, updating the 2015 National Money Laundering Risk Assessment (2015 NMLRA).

Relevant component agencies, bureaus, and offices of Treasury, the Department of Justice (DOJ), the Department of Homeland Security (DHS), as well as U.S. regulatory agencies, participated in the development of the risk assessment.

The 2018 NMLRA is based on interviews with relevant authorities as well as a review of federal and state public sector actions and analysis, and private sector research, issued since the 2015 NMLRA.

The United States continues to estimate that domestic financial crime, excluding tax evasion, generates approximately $300 billion of proceeds for potential laundering, based on the sources and analysis cited in the 2015 NMLRA.

Criminal prosecutions and law enforcement investigations indicate that most of the money earned from crime in the United States stays in the United States, but also that the United States is an attractive destination for illicit funds generated abroad.

The crimes that generate the bulk of illicit proceeds in the United States are fraud, drug trafficking, human smuggling, human trafficking, organized crime, and corruption.

The many varieties of fraud, including bank fraud, consumer fraud, healthcare fraud, securities fraud, and tax refund fraud, are believed to generate the largest share of illicit proceeds.

Healthcare fraud alone generates proceeds of approximately $100 billion annually.

Prosecutions indicate that healthcare fraud often involves complicit healthcare professionals submitting fraudulent bills to insurers.

Insurance payments and subsequent transactions may flow through the banking system and look indistinguishable from legitimate funds transfers.

When payments are made by check the laundering can involve the help of complicit check cashers.

Law enforcement agencies have seen an increase in cybercrime, which encompasses a variety of illicit activity including phishing, malware attacks, and cyber-enabled crime such as credit card fraud, business e-mail compromise; and various types of consumer scams, including fake romance and lottery schemes, and employment offers that all inevitably involve the victim receiving requests for money.

These internet-based crimes can be perpetrated from anywhere in the world, which, along with the universal presence of drug trafficking networks, has contributed to the rise of global money laundering syndicates that employ complicit merchants, financial services professionals, and individuals to launder illicit proceeds on behalf of a variety of criminals.

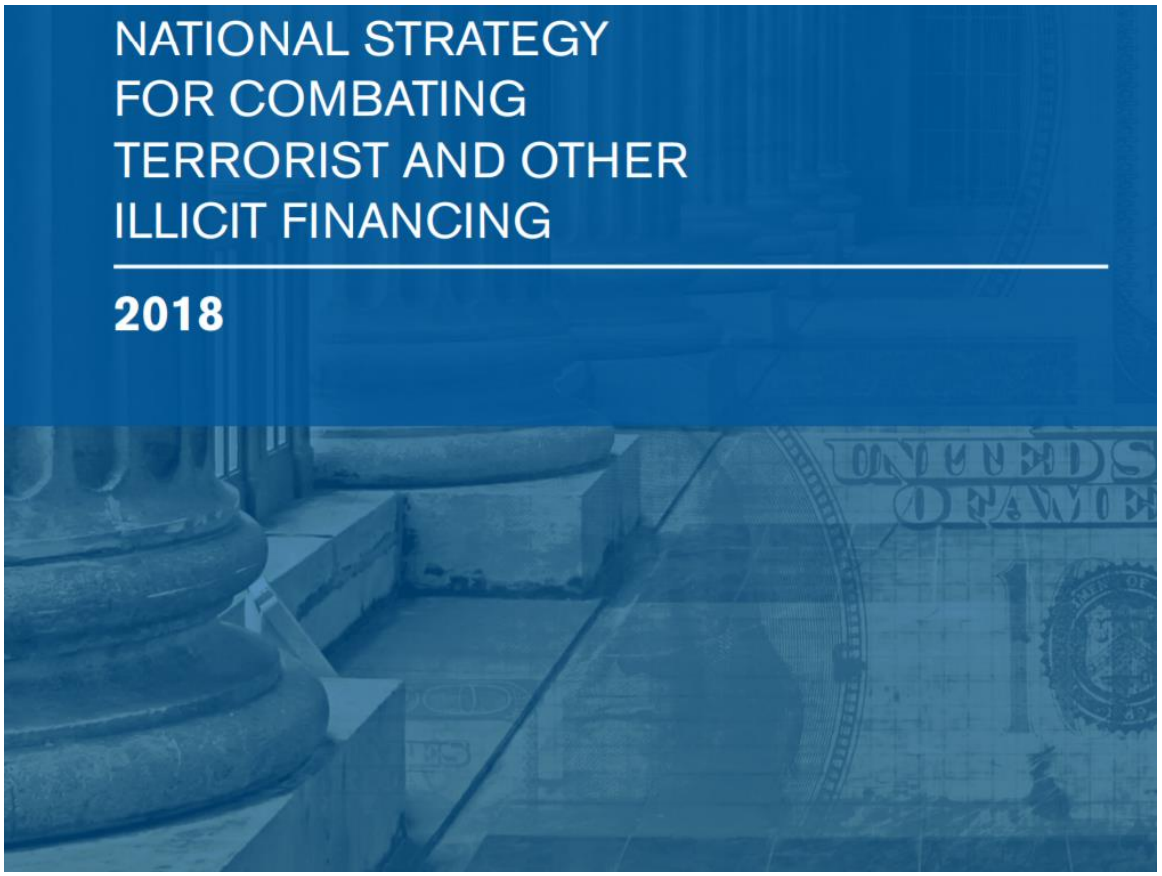
These professional money launderers and networks then subsist independently of the criminals they serve, making them dangerous due to their adaptability.

To read more:
https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf

*Number 3*

## Treasury Publishes National Illicit Finance Strategy and Supporting Risk Assessments

The U.S. Department of the Treasury has issued the National Strategy for Combating Terrorist and Other Illicit Financing (National Illicit Finance Strategy), pursuant to Sections 261 and 262 of the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA).




The Strategy describes and assesses current U.S. government efforts to combat illicit finance threats and risks and identifies priorities, objectives, and potential areas for future improvement.

It also highlights U.S. interagency and intergovernmental efforts to combat illicit finance domestically and internationally, including enforcement measures that include sanctions, prosecutions, and asset forfeiture, as well as improvements in information sharing mechanisms and updated guidance to aid financial institutions in detecting and combating illicit finance threats.

The National Illicit Finance Strategy addresses the threats and risks to the U.S. financial system that were identified in three separate risk assessments, also released today: the National Proliferation Financing Risk Assessment, the National Terrorist Financing Risk Assessment, and the National Money Laundering Risk Assessment.

This is the first National Proliferation Financing Risk Assessment, and the terrorist financing and money laundering risk assessments build and expand on previous Treasury-led risk assessments issued in 2015.

Together, these assessments help the public and private sectors understand the terrorist financing, proliferation financing, and money laundering methods used in the United States, the threat actors behind these methods and vulnerabilities exploited, and the risks that these activities pose to the U.S. financial system and national security.

In doing so, these assessments enable U.S. Government agencies to better understand and therefore more effectively combat illicit actors seeking to exploit the U.S. financial system.

They also assist the private sector in detecting the exploitative tactics used by these threat actors, allowing financial institutions and other private sector stakeholders to better mitigate their illicit finance risk.

The National Illicit Finance Strategy describes the strengths of U.S. counter-illicit finance efforts, including a robust legal and regulatory framework; authorities, capabilities, and initiatives by U.S. departments and agencies, and highlights efforts underway to improve the effectiveness of national safeguards in place in light of changes in technology and emerging threats.

Such efforts include a working group formed by Treasury's Office of Terrorism and Financial Intelligence and the Federal depository institutions regulators on Bank Secrecy Act/Anti-Money Laundering (BSA/AML) that is exploring ways to modernize the regulatory regime in ways that support innovative efforts by financial institutions to devote their resources towards addressing the areas of highest risk for illicit finance activities.

The National Illicit Finance Strategy and risk assessments were prepared by the Office of Terrorist Financing and Financial Crimes, an office within Treasury's Office of Terrorism and Financial Intelligence, in consultation with the many agencies, bureaus, and departments of the federal government that also have roles in combating illicit finance.

To learn more:
https://home.treasury.gov/system/files/136/nationalstrategyforcombatingterroristandotherillicitfinancing.pdf

*Number 4*

## Reminder to firms on their MiFID obligations on disclosure of information to clients in the context of the United Kingdom withdrawing from the European Union

esma European Securities and Markets Authority

1. The European Securities and Markets Authority (ESMA) is issuing this Statement to remind investment firms and credit institutions providing investment services (collectively referred to as "firms") of their obligations to provide clients with accurate disclosure on the impact on the provision of services and investors' rights that may emerge from the withdrawal of the United Kingdom from the European Union (EU).

### Background

2. On 29 March 2017, the British government notified the European Council of its intentions to withdraw from the European Union. From that day, a two-year process has started to reach an agreement on the terms of the UK's departure from the EU (so called 'Brexit'). This process is currently on-going.

3. In preparation for Brexit, ESMA has issued:

- In May 2017, an Opinion1 on the general principles to support supervisory convergence in the context of the United Kingdom withdrawing from the European Union.

- In July 2017, three Opinions setting out sector-specific principles in the areas of investment firms, investment management and secondary markets, aimed at fostering consistency in authorisation, supervision and enforcement related to the relocation of entities, activities and functions from the United Kingdom. These three Opinions provide guidance to NCAs aimed at ensuring a consistent interpretation of the requirements relating to authorisation, supervision and enforcement in order to avoid the development of regulatory and supervisory arbitrage risks.

- In July 2018, a Statement on the timely submission of requests for authorisation in the context of the United Kingdom withdrawing from the European Union. Within this Statement, ESMA has already

reminded firms that, as there is no assurance that a transition period will be agreed upon, entities need to be prepared for the scenario where a no-deal Brexit would take place on 30 March 2019.

4. In order to increase investors' awareness in this unprecedented situation, ESMA believes that, beyond the Opinions and Statement that have already been issued, it is important to remind firms of their legal obligation to provide clients with

(i) information on the implications of Brexit on existing and new contracts and

(ii) the impact of Brexit-related measures that a firm has taken or planned.

5. In this regard, ESMA has also conducted analyses, in cooperation with national competent authorities, on the state of preparedness of firms whose activity might be impacted by the UK withdrawal from the EU.

In light of these observations, ESMA believes that there is a need to remind relevant firms to finalise and implement suitable plans in order to mitigate any risks stemming from the UK withdrawal in a suitable timeframe and to provide appropriate information to their clients.

6. This Statement is addressed to the UK firms that provide services to the EU-27 countries (whether directly or through a branch), as well as to EU-27 firms that interact with clients based in the UK (whether directly or through of a branch).

To read more:
https://www.esma.europa.eu/sites/default/files/library/esma35-43-1328_brexit_statement_information_to_clients.pdf

*Number 5*

## CP18/44: Brexit – Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication

In this Consultation Paper we propose to make regulatory technical standards for strong customer authentication and common and secure open standards of communication, which will apply in the UK from 14 September 2019 in the event of a no-deal exit by the UK from the EU.

### Why we are consulting

A number of provisions of the SCA-RTS are effective from 14 March 2019, including the requirement to make testing facilities available if providing access to account information or payment initiation service providers. The remainder of the SCA-RTS will take effect on 14 September 2019.

On 29 March 2019, the UK will leave the EU. If the UK leaves the EU without a withdrawal agreement (a 'no-deal exit'), the SCA-RTS will be left partially converted into UK law.

This would leave a gap in the UK's regulatory framework, causing potential disruption and considerable regulatory uncertainty.

Despite the investments made by banks and other payment service providers to meet the 14 March 2019 deadline, consumer protections for the security and safety of payments would be at risk.

In our consultation paper, we propose to make regulatory technical standards for strong customer authentication and common and secure open standards of communication.

These standards will be substantially the same as the SCA-RTS, and will apply in the event of a no-deal exit.

### Who this applies to and who should read the consultation

This consultation applies to all payment service providers, including banks, building societies, e-money issuers, payment institutions, registered

account information service providers and payment initiation service providers.

The consultation will also be of interest to consumer bodies and relevant trade bodies, retailers, consumers, micro-enterprises and those involved in open banking initiatives.

To read more:
https://www.fca.org.uk/publications/consultation-papers/cp18-44-brexit-regulatory-technical-standards-strong-customer-authentication

*Number 6*

## FINMA publishes ICO guidelines

*Revisiting the guidelines after one year*

In guidelines published, the Swiss Financial Market Supervisory Authority FINMA sets out how it intends to apply financial market legislation in handling enquiries from ICO organisers.

The guidelines also define the information FINMA requires to deal with such enquiries and the principles upon which it will base its responses, creating clarity for market participants.

FINMA has seen a sharp increase in the number of initial coin offerings (ICOs) planned or executed in Switzerland and a corresponding increase in the number of enquiries about the applicability of regulation.

ICOs are a digital blockchain-based form of public fund-raising for entrepreneurial purposes.

Given a legal and regulatory framework with partially unclear applicability, FINMA is publishing guidelines, which complement its earlier FINMA Guidance 04/2017, setting out how it intends to treat enquiries from ICO organisers.

Creating transparency at this time is important given the dynamic market and the high level of demand.

### Each case must be decided on its individual merits

Financial market law and regulation are not applicable to all ICOs. Depending on the manner in which ICOs are designed, they may not in all cases be subject to regulatory requirements.

Circumstances must be considered on a case-by-case basis.

As set out in FINMA Guidance 04/2017, there are several areas in which ICOs are potentially impacted by financial market regulation. At present, there is no ICO-specific regulation, nor is there relevant case law or consistent legal doctrine.

## FINMA's principles focus on the function and transferability of tokens

In assessing ICOs, FINMA will focus on the economic function and purpose of the tokens (i.e. the blockchain-based units) issued by the ICO organiser.

The key factors are the underlying purpose of the tokens and whether they are already tradeable or transferable.

At present, there is no generally recognised terminology for the classification of tokens either in Switzerland or internationally.

FINMA categorises tokens into three types, but hybrid forms are possible:

- Payment tokens are synonymous with cryptocurrencies and have no further functions or links to other development projects. Tokens may in some cases only develop the necessary functionality and become accepted as a means of payment over a period of time.

- Utility tokens are tokens which are intended to provide digital access to an application or service.

- Asset tokens represent assets such as participations in real physical underlyings, companies, or earnings streams, or an entitlement to dividends or interest payments. In terms of their economic function, the tokens are analogous to equities, bonds or derivatives.

Focus on anti-money laundering and securities regulation
FINMA's analysis indicates that money laundering and securities regulation are the most relevant to ICOs.

Projects which would fall under the Banking Act (governing deposit-taking) or the Collective Investment Schemes Act (governing investment fund products) are not typical.

The Anti-Money Laundering Act contains requirements for financial intermediaries including, for example, the need to establish the identity of beneficial owners.

The law aims to protect the financial system against the risks of money laundering and the financing of terrorism.

Money laundering risks are especially high in a decentralised blockchain-based system, in which assets can be transferred anonymously and without any regulated intermediaries.
Securities regulation is intended to ensure that market participants can base their decisions about investments on a reliable minimum set of information. Moreover, trading should be fair, reliable and offer efficient price formation.

On the basis of the above-mentioned criteria (function and transferability), FINMA will handle ICO enquiries as follows:

- Payment ICOs: For ICOs where the token is intended to function as a means of payment and can already be transferred, FINMA will require compliance with anti-money laundering regulations. FINMA will not, however, treat such tokens as securities.

- Utility ICOs: These tokens do not qualify as securities only if their sole purpose is to confer digital access rights to an application or service and if the utility token can already be used in this way at the point of issue. If a utility token functions solely or partially as an investment in economic terms, FINMA will treat such tokens as securities (i.e. in the same way as asset tokens).

- Asset ICOs: FINMA regards asset tokens as securities, which means that there are securities law requirements for trading in such tokens, as well as civil law requirements under the Swiss Code of Obligations (e.g. prospectus requirements).

ICOs can also exist in hybrid forms of the above categories. For example, anti-money laundering regulation would apply to utility tokens that can also be widely used as a means of payment or are intended to be used as such.

## Blockchain technology has innovative potential

Following further consolidation of this supervisory practice, FINMA may in future decide to publish its interpretation in the form of a circular.

FINMA recognises the innovative potential of blockchain technology and therefore supports the federal government's Blockchain/ICO Working Group in which it is participating.

Clarity about the underlying civil law framework will be a decisive factor in establishing this technology sustainably and successfully in Switzerland.

FINMA CEO, Mark Branson comments: "The application of blockchain technology has innovative potential within and far beyond the financial markets. However, blockchain-based projects conducted analogously to regulated activities cannot simply circumvent the tried and tested regulatory framework.

Our balanced approach to handling ICO projects and enquiries allows legitimate innovators to navigate the regulatory landscape and so launch their projects in a way consistent with our laws protecting investors and the integrity of the financial system."

## Information for investors

FINMA has several times drawn attention to the risks that ICOs can pose for investors.

Tokens acquired in the context of an ICO are likely to be subject to high price volatility. Since many ICO projects are at an early stage of development, they are subject to numerous uncertainties.

Furthermore, it is uncertain under current civil law whether contracts executed via blockchain technology are legally binding.

*Number 7*

## Rogue fitness apps help you to lose money not weight

National Cyber Security Centre
a part of GCHQ

Three malicious apps have recently been identified and removed from Apple's app store.

The apps had a health theme and purported to check heart rate, calorie count or BMI index. "Fitness Balance", "Calories Tracker" and "Heart Rate Monitor" were discovered to be fraudulent and have been removed.

When the apps asked for a fingerprint scan to access information of interest, the identification method was instead employed to authorise a payment of up to $120.

If the user has a credit or debit card linked to an Apple account, the transaction was approved.

The apps would then continue to prompt the user to use the finger scanner before continuing to use the app. The scale of losses is unknown.

The existence of these apps in an eco-system generally considered as secure indicates that despite rigorous checks carried out by official app stores, some malicious apps do evade detection.

The malicious apps were spotted and have now been removed. When downloading apps, consumers should check reviews and any available information about the app and its developer.

You should also be alert to permissions that the app is requesting - these can be checked in the app settings.

This scam affects iPhone 8 or earlier models. Newer models have a feature called "Double click to pay" which, when activated, requires users to double click the side button to verify a payment.

Further advice can be found on the Cyber Aware and Get Safe Online websites at:
https://www.cyberaware.gov.uk/

https://www.getsafeonline.org/smartphones-tablets/mobile-apps/

*Number 8*

## Cyber Europe 2018 - After Action Report


Cyber Europe 2018 was the fifth pan-European cyber crisis exercise organised by the European Union Agency for Network and Information Security (ENISA).

The exercise engaged around 900 participants, from the public authorities and private companies, mainly in the Aviation sector, from all 28 EU Member States as well as two European Free Trade Association (EFTA) countries, Norway and Switzerland.

The exercise simulated an intense realistic crisis caused by a large-number (over 600 hundred) of cybersecurity incidents that occurred during the two-days, 6-7 June 2018.

The exercise was built on three main pillars:

- The sound use of business continuity and crisis management plans within an organisation

- National-level cooperation and use of contingency plans

- Cross-country cooperation and information exchange

In addition, the exercise gave the opportunity to the technical teams to test their skills in cybersecurity with a vast variety of technical challenges, including malware analysis, forensics, mobile malware, APT attacks, network attacks, IoT device infection, etc.

The exercise brought up the importance of cooperation between the different actors (victims and authorities) of simulated cybersecurity incidents, security providers and national authorities.

It proved to the participants that only by information exchange and collaboration, it is possible to respond to such extreme situations with a large number of simultaneous incidents.

We have witnessed a large number of instances of public–private and private–private cooperation.

Participants had to follow existing business processes, agreements, communication protocols and regulations to mitigate effectively the situations presented to them.

Nevertheless, the level of preparedness varied significantly between participants, the information flow felt sometimes to be unidirectional and structured private-public cooperation procedures were immature or non-existent.

The EU Network and Information Security (NIS) directive identifies many of the associated shortcomings and proposes measures to improve the situation.

The EU-level cooperation has been undoubtedly improved over the last years.

In particular, the technical-level cooperation has proven mature and effective.

The introduction of the CSIRTs Network (CNW) as defined in the NIS directive has provided EU Member States with an effective formal structure to exchange technical information but also to collaborate in order to resolve complex, large-scale incidents.

The exercise proved that at this level EU is well equipped to respond.

Some minor gaps were identified and have been already tackled by those involved.

On the other hand, the operational-level cooperation was exercised to a lesser extent. It is not so obvious how in real-life these levels will interact and furthermore how they will implement the strategic vision of the political leaders.

Future exercises shall try to test these aspects as well.

Finally, the technical incidents of the exercise provided an excellent opportunity for the cybersecurity teams to enhance their capabilities and expertise to deal with a variety of cybersecurity challenges.

The operational capacity as well as the technical skills in all participating organisation proved to be at the highest level.

Participating teams from non cybersecurity private companies in the Aviation sector analysed the majority of incidents successfully, and proved that their skillset in certainly very high.

The only shortcoming in some cases was not the lack of skills but the actual number of available resources for IT security.

This is a challenge that has be tackled by the higher management, since the return on investment (ROI) in cybersecurity expertise is definitely high for such critical sectors.

To read more:
https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report

*Number 9*

# The State of IT Security in Germany 2018

Federal Office
for Information Security

## Cyber attack on German authorities

### Situation

Towards the end of 2017, the BSI received indications of a successful cyber attack via the National Cyber Defence Centre, which purported to affect individual German federal authorities.

The BSI started the incident handling process in coordination with the authorities involved in the National Cyber Defence Centre, informed the authorities that were potentially affected and began the analysis and verification of the information initially available.

### Cause and Damage

The primary target of the attack was the Foreign Office. A learning platform operated by the Federal University of Applied Sciences was attacked in order to gain access to the Federal Foreign Office network via this intermediate step. This was  because established protection measures had prevented attackers from accessing the network of the Foreign Office directly.

This put the attacker in a position to successfully infect some client systems at the German Foreign Office and to extract internal documents in small numbers. However, the attack was not directed against the government networks as a whole.

### Reaction

In close cooperation between the authorities concerned, the National Cyber Defence Centre and BSI responded with the following measures, among others:

- analysis of the impact
- identification and protection of infected systems
- forensic analysis

• protocols and log data evaluation for those affected and at central points in government networks

In addition, the BSI has deployed a mobile incident response team (MIRT, within the meaning of Section 5a of the BSIG) to support incident handling on site for those affected, at weekends as well.

In consultation with those affected, the attack was observed undercover in order to first analyse the attackers‘ actions and then to maximise the effectiveness of the measures to be taken.

The findings gained have already been incorporated into the Federal Administration‘s protective measures during the analysis.

After press reports had publicised CLASSIFIED information on the incident on 28 February 2018, immediate corrective action was taken.

Additional protective measures to prevent attacker communication have been established.

The affected systems of the Federal University of Applied Sciences were subsequently also switched off.

## Recommendation

The situation clearly shows the current threat potential posed by targeted attacks on the Federal Administration.

The financial, time and technical resources invested by the attacker in the preparation and execution of the attack demonstrate the attacker‘s great interest in its target.

The incident underscores the need for multi-level protection concepts and consistent implementation of protection measures against targeted attacks.

However, the incident also proves the effectiveness of these measures: Similar incidents have had a far more serious impact on those affected in the past.

To read more:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=3

*Number 10*

# Brief summary, 2017 Report on the Protection of the Constitution Facts and Trends

Federal Ministry
of the Interior, Building
and Community

## Espionage and other intelligence activities

States which strive to gain a knowledge edge in military (particularly strategic) or economic and technological contexts do not hesitate to procure the necessary information secretly and illegally by violating applicable law.

In this context, their governments political agenda dictates the priority areas of the individual intelligence services‘ activities.

Germany is of interest in its role as a geopolitical player, as a member of NATO and the EU and on account of its economic strength and innovative businesses.

Oppositional groups from foreign intelligence services’ home countries in Germany are another target of espionage activities.

The consequences for Germany range from a weakening of its negotiating position to high material and economic damage and a potential impairment of its national sovereignty.

The Russian Federation, the People’s Republic of China and the Islamic Republic of Iran are the major players behind espionage activitiesthat are directed against Germany.

Apart from that, other countries (including western countries) also play a role.

The Russian intelligence services invest a lot of organisational and financial effort to engage in espionage activities against Germany.

With the use of cyberspace the extent of espionage has increased many times over.

It is targeted at all areas of politics, economy, research and technology, with a focus on the political position of the Federal Government vis-à-vis the Russian Federation.

The efforts of the Russian intelligence services focus in particular on those policy areas where decisions with a potential impact on Russian interests are taken.

These policy areas include the alliance policy within NATO and the EU and Germany's foreign policy.

The tense relationship between the EU and Turkey and the resulting potential impact on the accession negotiations and the future of the EU – in particular after the so-called BREXIT vote – and the orientation of the Common Foreign and Security policy have been of particular interest to the Russian intelligence services.

Owing not least to the dwindling public interest, the Ukraine crisis which was very much in the fore in 2014 and 2015,has been overshadowed by other areas of tension such as the conflict in Syria.

Nevertheless the question as to whether the political and economic sanctions which were imposed on Russia in the course of the Ukraine crisis in 2014, are going to be lifted or extended continues to be of high interest to the Russian intelligence services.

As regards German home affairs policy, the services tried to gather information on party-political structures and developments, on the views of individual political parties and on the potential impact of electoral outcomes.

Apart from their espionage interests the Russian services strive to influence the political and public opinion in Germany.

As in previous years, pro-Russian propaganda was disseminated in numerous ways.

Important tools include social networks, the microblogging service Twitter, government-funded and private institutes (such as think tanks) and Russian state media.

TV, radio and Internet channels which broadcast around the world run targeted propaganda and disinformation campaigns.

Such disinformation and propaganda campaigns are aimed at destabilising the Federal Republic of Germany and at weakening its position as an advocate for an extension of the EU-sanctionsimposed on Russia.

The situation in Russia, by contrast, is being glossed over while the sole responsibility for the economic and social hardships is attributed to the western governments.

The focus of Chinese intelligence activities is shifting towards political espionage.

They are now making great efforts to obtain information about supranational entities such as the EU and about international conferences such as the G20 Summit.

Moreover, the country is very interested in policy positions on China, e.g. recognition as a market economy or territorial disputes in the region of the South China Sea.

In Germany, Chinese intelligence services continue to focus on industry, research, technology and the armed forces (in particular information on the structure, armament and training of the Bundeswehr and on modern weapons technology) as well as on policies which– from the Chinese perspective – threaten national unity and the Communist Party's monopoly on power ("Five Poisons").

To read more:
https://www.verfassungsschutz.de/en/download-manager/_annual-report-2017-summary.pdf

## 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.

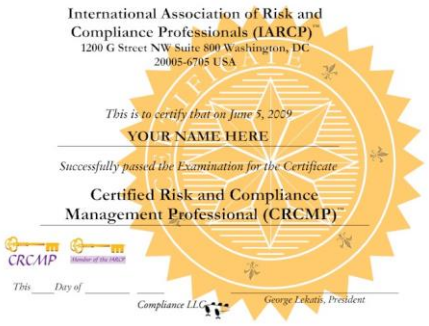
You may visit:
www.risk-compliance-association.com/How_to_become_member.htm

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.



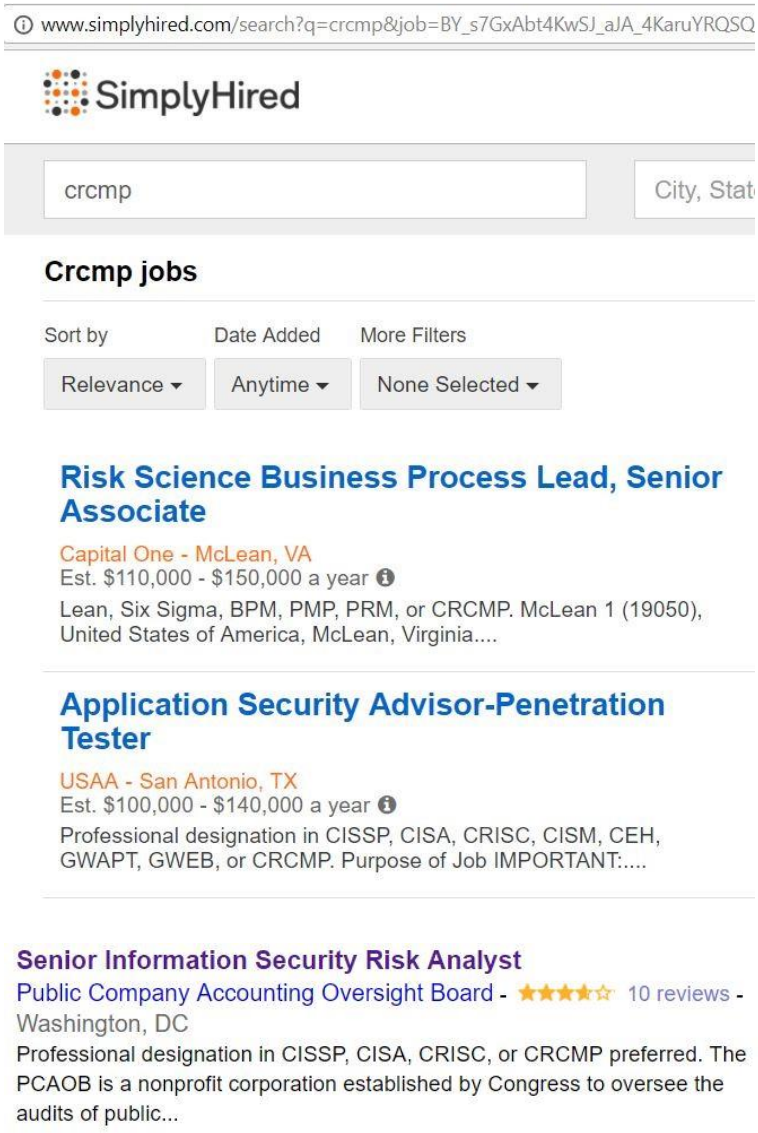

There are CRCMPs in 32 countries around the world. Companies and organizations like Accenture, American Express, USAA etc. consider the CRCMP a preferred certificate.

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