Monday, November 2, 2020

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

Dear members and friends,

According to the Cyber Lexicon from the Financial Stability Board (November 2018):

"A *cyber incident* is a cyber event that:
(i) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or
(ii) violates the security policies, security procedures or acceptable use policies, *whether resulting from malicious activity or not*."

This is a very good definition.

The UK's National Cyber Security Center (NCSC) defines a *cyber incident* as "a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990).

In general, types of activity that are commonly recognised as being breaches of a typical security policy are:

1. Attempts to gain unauthorised access to a system and/or to data.
2. The unauthorised use of systems for the processing or storing of data.
3. Changes to a systems firmware, software, or hardware without the system owners consent.
4. Malicious disruption and/or denial of service."

According to the Computer Security Resource Center (CSRC), National Institute of Standards and Technology (NIST), an *incident* is "an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the

system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."

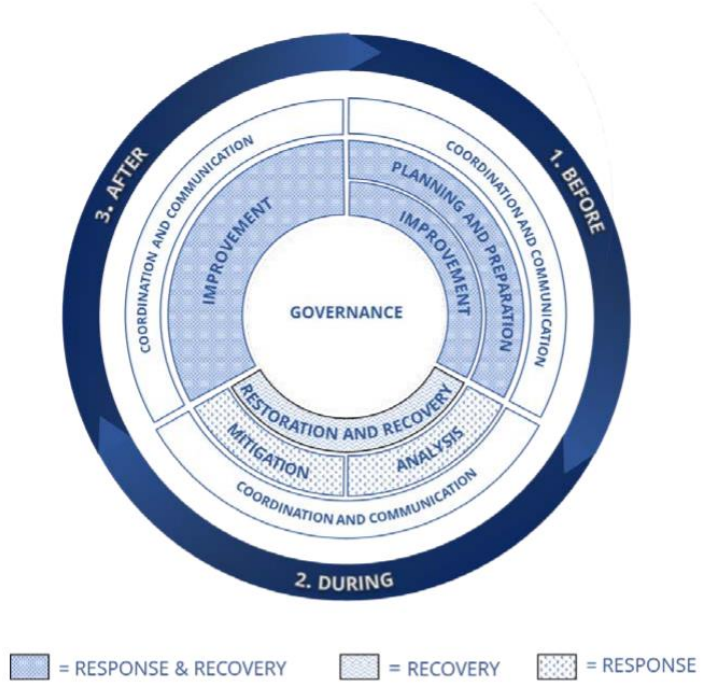
We have different definitions, and this is a major problem, because we cannot have *incident response international standards* if we cannot have a consistent definition of the term *incident*.

I have just read the new paper *"Effective Practices for Cyber Incident Response and Recovery - Final Report"* from the Financial Stability Board (FSB). We read at the first paragraph:

"Cyber incidents pose a threat to the stability of the global financial system. In recent years, there have been a number of cyber incidents that have significantly impacted financial institutions and the ecosystems in which they operate.

A significant cyber incident, if not properly contained, could seriously disrupt the financial system, including critical financial infrastructure, leading to broader financial stability implications."

Figure 1: Illustration of CIRR components



There is an interesting "toolkit" in this paper:

"The toolkit, structured across seven components, comprises 49 effective practices that organisations have adopted while taking into account

jurisdictions' legislative, judicial and regulatory frameworks, the size of the organisation, the organisation's role in the financial ecosystem and the extent to which stakeholders are affected by a cyber incident.

The toolkit is composed as a resource and reference guide for effective practices using common cyber taxonomies in a manner aligned to industry standards accessible to senior management, board of directors or other governance or compliance, risk, and legal professionals that interface with cybersecurity technical experts within the organisation, the SSBs or authorities.

While many of these effective practices are already in use by larger organisations, they could also be valuable for smaller and less complex organisations to help strengthen their cyber resilience.

The toolkit provides a range of effective practices and organisations can choose to adopt some or all of the effective practices that are suitable for their respective business models, taking into account their size, complexity and risks to the financial ecosystem."

Read more at number 1 below. Welcome to our Top 10 list.

Best regards,

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

Number 1 (Page 6)

Effective Practices for Cyber Incident Response and Recovery Final Report

FSB FINANCIAL STABILITY BOARD

Number 2 (Page 8)

Covid-19 and banking supervision: where do we go from here?

Keynote speech by Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, at the 21st International Conference of Banking Supervisors.

Number 3 (Page 11)

How we're tackling evolving online threats

Shane Huntley, Threat Analysis Group

Google

Number 4 (Page 13)

ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected

enisa European Network and Information Security Agency

Number 5 (Page 16)

CLARIFYING DIGITAL TERMS

NATO StratCom COE Terminology Working Group

Number 6 (Page 21)

European Insurance Overview 2020
Solo undertakings - Year-end 2019

Number 7 (Page 22)

Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm

United States Government Accountability Office (GAO), Report to the Republican Leader, Committee on Education and Labor, House of Representatives

Number 8 (Page 24)

BIS international banking statistics at end-June 2020

Number 9 (Page 25)

SEC Updates Auditor Independence Rules

Amendments Reflect Staff Experience Applying the Auditor Independence Framework

Number 10 (Page 30)

Alert (AA20-283A) - APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations

Number 1

Effective Practices for Cyber Incident Response and Recovery Final Report

FSB FINANCIAL STABILITY BOARD

Cyber incidents pose a threat to the stability of the global financial system.

In recent years, there have been a number of cyber incidents that have significantly impacted financial institutions and the ecosystems in which they operate.

A significant cyber incident, if not properly contained, could seriously disrupt the financial system, including critical financial infrastructure, leading to broader financial stability implications.

Efficient and effective response to and recovery from a cyber incident by organisations in the financial ecosystem are essential to limit any related financial stability risks.

Such risks could arise, for example, from interconnected IT systems between multiple financial institutions or between financial institutions and third-party service providers, from loss of confidence in a major financial institution or group of financial institutions, or from impacts on capital arising from losses due to the incident.

The cyber resilience of organisations is crucial for the smooth functioning of the financial system and in engendering financial stability.

Enhancing cyber incident response and recovery (CIRR) at organisations is an important focus for national authorities.

National authorities are in a unique position to gain insights on effective CIRR activities in financial institutions from their supervisory work, and their observations across multiple organisations can help suggest areas for enhancement.

Authorities also have an important role to play in responding to cyber incidents that present potential risks to financial stability.

Authorities can consider the sector-wide implications of a cyber incident or series of cyber incidents, including any market confidence issues and reactions resulting from information from public market data, news and

social media, or from partial or inaccurate information, possibly proliferated by fraudulent sources.

Authorities may also, as appropriate, support organisations in sharing information to protect against threats that could have a detrimental impact on financial stability.

The FSB has developed a toolkit of effective practices that aims to assist organisations in their cyber incident response and recovery activities.

In this regard, organisations' respond function executes the appropriate activities in reaction to a detected or reported cyber incident, while the recover function carries out the appropriate activities to restore any systems, capabilities or resume services or operations that were impaired due to a cyber incident.

The FSB encourages authorities and organisations to use the toolkit to enhance their CIRR activities.

To read more: https://www.fsb.org/wp-content/uploads/P191020-1.pdf

Number 2

Covid-19 and banking supervision: where do we go from here?

Keynote speech by Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, at the 21st International Conference of Banking Supervisors.

Introduction

Good morning, good afternoon and good evening. Welcome to the 21st International Conference of Banking Supervisors (ICBS).

This is my first ICBS, following my appointment as Chairman of the Committee in March of last year. But I had long heard about its reputation as the premier global banking conference for central banks and supervisory authorities.

For over 40 years since its inception, the ICBS has been a key forum for senior central bankers and bank supervisors from more than 100 countries to discuss topical supervisory issues.

Its enduring success is a testament to the ongoing importance that we all attach to cross-border cooperation, a theme which I will return to.

While this year's ICBS is being held in a somewhat different format, I have no doubt that it will continue to build on its historical achievements.

I would like to start by thanking Governor Macklem, Superintendent Rudin and their teams at the Bank of Canada and the Office of the Superintendent of Financial Institutions for hosting this year's ICBS virtually.

I am sure that I speak on behalf of all participants in saying that we would have loved to be in Vancouver, the vibrant heart of beautiful British Columbia.

But we can still recognise the fitting choice of this virtual venue. Vancouver has long been the financial centre of British Columbia's resource economy. A recent history of this role vividly depicts how "stock brokers, financial agents and bankers played essential roles as intermediaries in the fluid commercial life of early twentieth-century Vancouver".

What's more, the Vancouver Stock Exchange was incorporated in 1907 – almost 30 years before the Bank of Canada was founded! Tiff and Jeremy, while we may be physically distanced around the world at this year's ICBS, you and your organisations have done an excellent job at ensuring that we remain socially together this week. Thank you.

The overarching theme for this year's ICBS - the future of supervision in a changing world – is perhaps more relevant than ever before.

The world has changed profoundly since the outbreak of Covid19 seven months ago.

The uniqueness of the sudden stop to the global economy in response to the tragic health crisis is only matched by the sheer uncertainty about the outlook.

To borrow a sports metaphor, we still do not know if we are in the first inning, quarter or half of this crisis. Uncertainty is the only certainty there is.

So what is the future of supervision in this changing world, and what can we learn from the current crisis?

When the former Chinese premier Zhou Enlai was asked in 1972 about the impact of the French Revolution of 1789 – or, as is now generally accepted, the civil unrest of May 1968 – he famously replied that it was "too early to say".

Given that we've yet to reach the four year mark since the start of the pandemic – let alone the 184th anniversary! – it would be premature to provide a definitive discourse at this stage.

Yet we have already seen fundamental changes to the way we live and work.

For example, we witnessed a tremendously rapid shift to remote working arrangements across many sectors.

Professor Prithwiraj Choudhury will discuss the implications of the 'working from anywhere' geographic flexibility in more detail on Wednesday, and we will have the opportunity to discuss what this means for supervision.

These changes, whether temporary or permanent, offer some clues about the future landscape.

So there is merit in starting a discussion about what we have learned to date and, more importantly, the future and changes that we want to see in banking supervision.

Allow me to outline some personal thoughts on these issues, which may not necessarily represent the view of the Basel Committee.

To read more: https://www.bis.org/speeches/sp201019.pdf

Number 3

How we're tackling evolving online threats

Shane Huntley, Threat Analysis Group

Google

Major events like elections and COVID-19 present opportunities for threat actors, and Google's Threat Analysis Group (TAG) is working to thwart these threats and protect our products and the people using them.

As we head into the U.S. election, we wanted to share an update on what we're seeing and how threat actors are changing their tactics.

What we're seeing around the U.S. elections

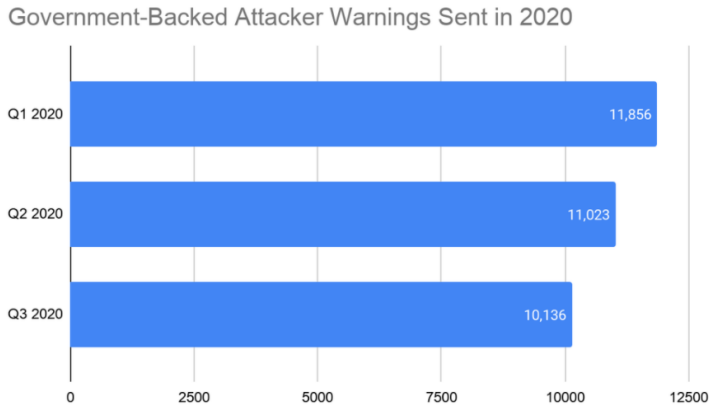
In June, we announced that we saw phishing attempts against the personal email accounts of staffers on the Biden and Trump campaigns by Chinese and Iranian APTs (Advanced Persistent Threats) respectively. We haven't seen any evidence of such attempts being successful.

The Iranian attacker group (APT35) and the Chinese attacker group (APT31) targeted campaign staffers' personal emails with credential phishing emails and emails containing tracking links. As part of our wider tracking of APT31 activity, we've also seen them deploy targeted malware campaigns.

One APT31 campaign was based on emailing links that would ultimately download malware hosted on GitHub. The malware was a python-based implant using Dropbox for command and control. It would allow the attacker to upload and download files as well as execute arbitrary commands. Every malicious piece of this attack was hosted on legitimate services, making it harder for defenders to rely on network signals for detection.

In one example, attackers impersonated McAfee. The targets would be prompted to install a legitimate version of McAfee anti-virus software from GitHub, while malware was simultaneously silently installed to the system.

When we detect that a user is the target of a government-backed attack, we send them a prominent warning. In these cases, we also shared our findings with the campaigns and the Federal Bureau of Investigation. This targeting is consistent with what others have subsequently reported.



Number of "government backed attacker" warnings sent in 2020

Overall, we've seen increased attention on the threats posed by APTs in the context of the U.S. election.

U.S government agencies have warned about different threat actors, and we've worked closely with those agencies and others in the tech industry to share leads and intelligence about what we're seeing across the ecosystem.

This has resulted in action on our platforms, as well as others.

Shortly after the U.S. Treasury sanctioned Ukrainian Parliament member Andrii Derkach for attempting to influence the U.S. electoral process, we removed 14 Google accounts that were linked to him.

To read more:
https://blog.google/threat-analysis-group/how-were-tackling-evolving-online-threats

Number 4

ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected

Apart from indicating adversaries' motivations, it provides evidence about the most common attack techniques and threat exposure applying to a particular sector, thus indicate protection requirements and priorities.

With respect to themes, the analysis of threats and challenges associated with specific emerging technologies contributes to the process of assessing, evaluating and mitigating future risks.

Contextualised cyber threat intelligence (CTI) for sectors is an important preparedness tool for drawing conclusions on expected cyberattacks within a specific sector.

Contextualisation of sectoral CTI is mainly based on cybersecurity incidents encountered in a sector.

Although this is a standard method for existing and established IT components and digital services, it does not cover emerging technologies.

This is mainly because no incident information exists for technologies that are only at a pilot or experimental phase.

SECTOR	MOST POPULAR THREATS/ATTACKS	INCIDENTS TRENDS
Individual	• Phishing • Malware • Information leakage • Data theft	Stable
Multiple industries	• Web application attacks • Phishing • Malware	Increasing
Public Administration, Defence, Social Services	• Malware • Phishing • Web based attack	Stable slightly decreasing
Financial/Banking/ Insurance	• Web application attacks • Insider threat (unintentional abuse) • Malware • Data theft	Stable
Health/Medical	• Malware • Insider threat (unintentional abuse/error) • Web application attacks	Increasing
Education	• Malware • Ransomware • Web based attacks	Stable slightly decreasing
Information and Communication	• Web application attacks • Insider threat (unintentional abuse/error) • Malware	Stable
Professional/Digital Services	• Web application attack • Insider threat (unintentional abuse/error) • Malware	Stable
Arts, Entertainment and gaming[8]	• Web application attacks • Malware • Phishing	Stable
Manufacturing	• Malware • Web application attacks • Insider threat (unintentional abuse/error)	Stable

CTI for emerging technologies is contextualised through threat assessments of asset categories pertinent to a specific sector.

ENISA performs such assessments for emerging sectors such as 5G, IoT and smart cars . Sectorial and thematic threat landscapes and assessments of baseline protection are the methods used by ENISA to contextualise CTI.

In this report, besides sectorial CTI relying on incident-based statistics, we present a summary of assessed CTI for emerging technology sectors based on ENISA work.

To read more:
https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

Number 5

CLARIFYING DIGITAL TERMS

NATO StratCom COE Terminology Working Group

Digital technologies and means of communication have become a central part of politics and social organisation.

The role of AI, big data, and machine learning is growing, as are ethical, privacy, and security concerns which these technologies bring with them.

The purpose of this glossary is to encourage the use of precise and simple language that bridges the terminological divide between policymakers, soldiers, tech companies, academics, and programmers.

It is at the intersection of their respective fields, that digitalisation's potential for positive change as well as ensuing challenges can be recognised and addressed.

Sharing a common vocabulary is the first step.

As digitalisation continues to transform our societies, it has also influenced the language used to describe this process.

Terms related to the developments and possibilities brought on by digitalisation can seem confusing.

Digital vs. cyber vs. online, AI and machine learning lack distinction in popular usage and understanding.

An additional layer of complexity is added by the multiplicity of language communities that exist in this field: from programmers and computer scientists, to communicators, politicians, militaries, academics, and the general public. Many terms become the subject of fashion.

After all, no one goes to cybercafes to do their cybershopping anymore. Terms initially used in a purely technical sense, and in the field of computer science, evolve and may change their meaning when they are imported into the context of political communications and conflict.

Frequently, terms appear to be used interchangeably without a second thought by its user ('online'/'cyber'/'digital').

Some terms are outdated but remain in use (certain 'cyber'- compounds). Some terms require more specificity ('artificial intelligence'), while others are more useful when defined in broader terms ('attribution').

The 'Digital Terms' publication sits within the framework of thinking and follows the same methodology that has been guiding the Terminology Working Group since 2017.

The definitions were deliberately kept at a general strategic communications level and do not reflect nuances that might be used or understood only in a niche language community of computer scientists.

This glossary's selection of terms and their definitions were guided by political, security, and, above all, strategic communications perspectives.

As a first step, the NATO Strategic Communications Centre of Excellence's (COE's) Terminology Working Group created a comprehensive list of terms together with experts from the policymaking, commercial, technology, and military (NATO SHAPE, COE) sectors.

The collection of terms was then narrowed down. Some terms were judged overly technical for the present publication. Such terms were deemed to squarely belong in the field of computer science, where they are already well-defined.

The Terminology Working Group prioritised 'digital' and 'cyber' language which relates to the main concerns of the international security field; namely, power and influence.

This glossary is not exhaustive, but helps clarify the language we use in our professional lives.

Why terminology and not lexicography?

This section reviews the beginnings of terminology as a discipline as well as the most recent literature, and what that means for the methodology of this project.

What is lexicography?

The discipline of lexicography sits within the field of applied linguistics and is preoccupied with observing, recording, and describing words in a given

language, highlighting their most characteristic features and their meaning(s). Thus, the work of lexicographers is considered to be descriptive rather than prescriptive; recording established language use rather than setting standards for correct use.

Moreover, lexicography and terminology also differ in the linguistic object they study.

While specialist dictionaries look at a given language (or languages) as a whole, terminologies or technical dictionaries focus on a specific subfield that is defined by a community of expertise (rather than shared linguistic features).

So a terminological dictionary usually deals with the language of a particular trade, profession, or academic field.

In our case, the language area under consideration is defined by:

a) the institution of NATO in terms of the primary users of the outputs from this project, and

b) the field of Strategic Communications in terms of the area of expert knowledge.

Both the boundaries constituting the NATO linguistic community and the extent of Strategic Communications as a field require further interrogation and definition.

Terminology versus Lexicography in Practice

In its more traditional form, Terminology distinguishes itself from Lexicography in the following respects:

- Lexicography starts with the word and tries to record the most important definitions for that word used in a given language.

  This is also referred to as a semasiological approach (determining the meanings of lexical units). Terminology, on the other hand starts with the concepts that are in need of definition and tries to identify / designate suitable terms (an onomasiological approach).

  Terminology is thus much more prescriptive than lexicography.

- While the objective of the lexicographer is to help readers interpret texts, a terminological project aims to help produce texts.

- Lexicography is more about reflecting or describing established language use. Terminology is guided by principles of clarity and efficiency in specialised communication, so prescribing and potentially wishing to change how language is used.

Lexicographers sometimes compile specialised dictionaries.

However, this project deals with the language used by a specialised language community, which is part of an institution (i.e. NATO). So a terminological approach is more suitable.

Moreover, lexicographers must carefully weigh scientific objectivity against offering authoritative entries.

Yet this balancing act is not of central concern to this terminology project in NATO Strategic Communications.

With Strategic Communications being a relatively new field of research and practice (at least under that name), there have been no comprehensive efforts to standardise the language used by strategic communicators.

This leads us to another reason why this is a terminology rather than a lexicography project: it has grown out of very specific needs in the NATO community to improve communication between different branches and national governments, rather than to describe and record the current use of terms.

What is terminology?

This section offers a brief overview of major developments in the discipline of terminology and how these feed into the approach chosen by this terminology project.

Early developments in Terminology

Terminology is a relatively young field of research. It only became an object of independent study in the 1930s when it was first conceptualised as a discipline with the work of Austrian industrialist (and later, terminologist) Eugen Wüster (1898-1977) and his followers.

His theory of Terminology was based on his experiences as an engineering expert and from compiling The Machine Tool.

An Interlingual Dictionary of Basic Concepts (1968), a project sponsored by the OECD.

Given his background in engineering and entrepreneurship, it is hardly surprising that he developed a theory of Terminology where language was considered to be strictly utilitarian.

Like the parts of a machine, specialised language should live up to standards of precision, efficiency, and economy.

Wüster's theory of Terminology gained currency and legitimacy both in academia and the practical application and study of terminology in international institutions.

The fact that his ideas came to dominate the field of Terminology would be heavily criticised from the 1990s onwards.

But before exploring these critiques further, a closer look at Wüster's theory of Terminology is required.

To read more:
https://www.stratcomcoe.org/clarifying-digital-terms

Number 6

European Insurance Overview 2020
Solo undertakings - Year-end 2019

The Annual European Insurance Overview is an easy-to-use and accessible overview of the European (re)insurance sector. The report is based on annually reported Solvency II information. This ensures that the data has a high coverage in all countries and is reported in a consistent manner across the EEA.

The report is objective, factual and data driven and does not contain analysis or policy messages. All indicators used in the report are calculated from the reported data from undertakings. While the topics and indicators covered is intended to be relatively stable over time, the report will be adapted to respond to changes in micro prudential and supervisory priorities. It will therefore support the supervisory community and industry with highly relevant and easily-accessible data at European level.

The report is published with all charts data available for download in separate excel files.

To learn more:
https://www.eiopa.europa.eu/sites/default/files/financial_stability/european-insurance-overview-report-2020.pdf

https://www.eiopa.europa.eu/sites/default/files/financial_stability/european-insurance-overview-repor-data-2020.xlsx

Number 7

Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm

United States Government Accountability Office (GAO), Report to the Republican Leader, Committee on Education and Labor, House of Representatives

What GAO Found

A cybersecurity incident is an event that actually or potentially jeopardizes a system or the information it holds.

According to GAO's analysis of K-12 Cybersecurity Resource Center (CRC) data from July 2016 to May 2020, thousands of K-12 students were affected by 99 reported data breaches, one type of cybersecurity incident in which data are compromised.

Students' academic records, including assessment scores and special education records, were the most commonly compromised type of information (58 breaches).

Records containing students' personally identifiable information (PII), such as Social Security numbers, were the second most commonly compromised type of information (36 breaches).

Financial and cybersecurity experts say some PII can be sold on the black market and can cause students significant financial harm.

Breaches were either accidental or intentional, although sometimes the intent was unknown, with school staff, students, and cybercriminals among those responsible (see figure).

Staff were responsible for most of the accidental breaches (21 of 25), and students were responsible for most of the intentional breaches (27 of 52), most frequently to change grades.

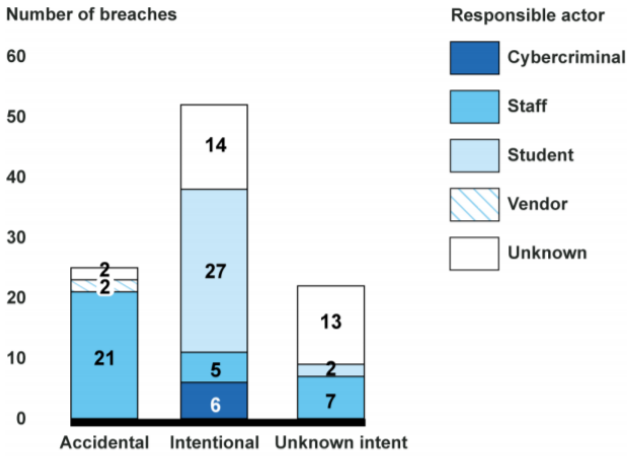
Reports of breaches by cybercriminals were rare but included attempts to steal PII.

Although the number of students affected by a breach was not always available, examples show that thousands of students have had their data compromised in a single breach.

Of the 287 school districts affected by reported student data breaches, larger, wealthier, and suburban school districts were disproportionately represented, according to GAO's analysis.

Cybersecurity experts GAO spoke with said one explanation for this is that some of these districts may use more technology in schools, which could create more opportunities for breaches to occur.

Responsible Actor and Intent of Reported K-12 Student Data Breaches, July 1, 2016-May 5, 2020



Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Notes: The actor or the intent may not be discernible in public reports.

For this analysis, a cybercriminal is defined as an actor external to the school district who breaches a data system for malicious reasons.

To read more: https://www.gao.gov/assets/710/709375.pdf

Number 8

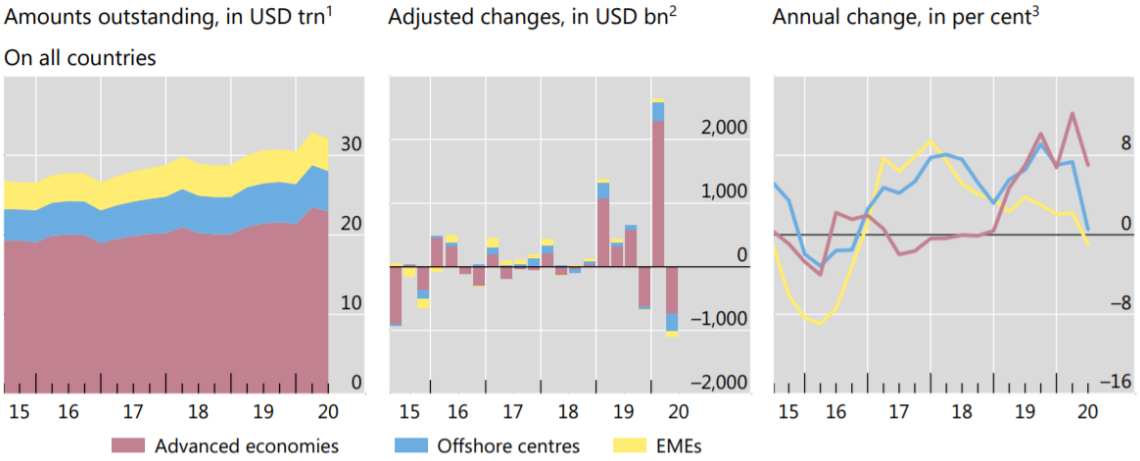
BIS international banking statistics at end-June 2020

• Cross-border claims contracted by $1.1 trillion from Q1 to Q2 2020. The yearon-year growth rate dropped from 10% at end-March to 5% at end-June 2020. Interbank claims, which had surged in the first quarter, fell sharply, driving the overall contraction.

• Cross-border claims on emerging market and developing economies (EMDEs) fell year on year for the first time since 2016, mainly driven by a $43 billion contraction in claims on Latin America and the Caribbean.

• Banks have continued to rebalance their portfolios into government assets. Their consolidated foreign claims on the official sector globally rose to 29% of their total foreign claims in Q2 2020, up from 19% at end-2010.

Cross-border claims by borrowing region — Graph A.2



To read more: https://www.bis.org/statistics/rppb2010.pdf

Number 9

SEC Updates Auditor Independence Rules

Amendments Reflect Staff Experience Applying the Auditor Independence Framework

The Securities and Exchange Commission today announced that it adopted final amendments to certain auditor independence requirements in Rule 2-01 of Regulation S-X.

Informed by decades of staff experience applying the auditor independence framework, the final amendments modernize the rules and more effectively focus the analysis on relationships and services that may pose threats to an auditor's objectivity and impartiality.

The final amendments reflect updates based on recurring fact patterns that the Commission staff has observed over years of consultations in which certain relationships and services triggered technical independence rule violations without necessarily impairing an auditor's objectivity and impartiality.

These relationships either triggered non-substantive rule breaches or required potentially time-consuming audit committee review of non-substantive matters, thereby diverting time, attention, and other resources of audit clients, auditors, and audit committees from other investor protection efforts.

The final amendments result in auditor independence requirements that will be used to evaluate specific relationships and services, with a focus on protecting investors against threats to the objectivity and impartiality of auditors.

"Today's amendments reflect the Commission's long-recognized view that an audit by an objective, impartial, and skilled professional contributes to both investor protection and investor confidence," said Chairman Jay Clayton.

"These modernized auditor independence requirements will increase investor protection by focusing audit clients, audit committees, and auditors on areas that may threaten an auditor's objectivity and

impartiality. They also will improve competition and audit quality by increasing the number of qualified audit firms from which an issuer can choose."

FACT SHEET
Amendments to Rule 2-01, Qualification of Accountants

Since the initial adoption of the current independence requirements in 2000 and amendments adopted in 2003, the Commission and its staff have continued to learn about the application, efficiency, and effectiveness of auditor independence requirements amidst changing capital market conditions. Additionally, in the May 2018 Proposing Release for Auditor Independence with Respect to Certain Loans or Creditor/Debtor Relationships, the Commission solicited suggestions for other revisions to the independence requirements. In December 2019, the Commission issued the Proposing Release for Amendments to Rule 2-01. The final amendments respond to recent changes in capital market conditions, reflect the Commission staff's experience administering the independence requirements, and incorporate both recent and long-term feedback.

Focusing on Risks to Audit Firm Objectivity and Impartiality

The final amendments seek to focus our auditor independence rules on relationships and services that are more likely to jeopardize the objectivity and impartiality of auditors. The following examples, based, in part, on the SEC staff's consultation experience, help to illustrate some of the concerns with the prior rules that today's amendments address.

Example 1 – Student Loans

Audit Firm has an audit partner based in Atlanta who continues to pay her student loans taken to attend college before starting her career at Audit Firm.

A different audit partner in Atlanta audits the lender that provided the student loan, a large student loan company that originates thousands of student loans.

Under the rules prior to today's amendments, the student loan of the audit partner who is not part of the audit would still lead to an independence violation for the audit engagement of the lender.

Under the amended rules, that student loan would no longer result in an independence violation for the audit engagement of the lender.

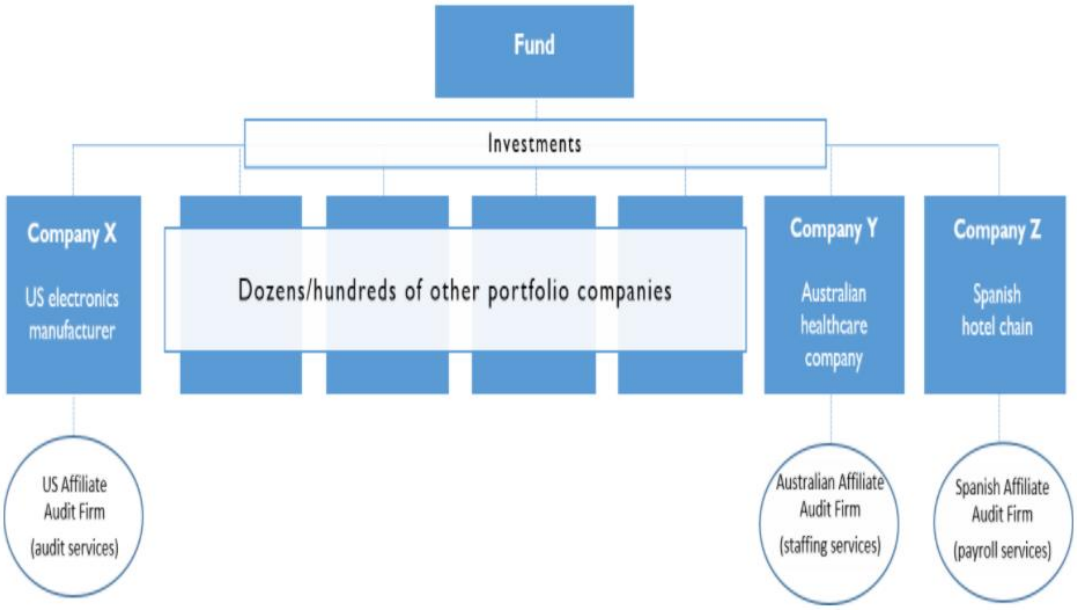
Example 2 – Portfolio Companies

Assume Company X is a U.S.-based portfolio company of Fund F. Fund F invests in various companies around the globe, perhaps dozens or even hundreds, including Company X. Audit Firm A is the auditor of Company X. Also assume that two of Audit Firm A's global network affiliates provide the services discussed below to two separate portfolio companies of Fund F, Company Y and Company Z. Further assume that Company Y and Company Z have no relation to each other or to Company X except for the fact that Fund F is invested in each Company. To add practical context, further assume that:

1. An Australian affiliate of Audit Firm A provides limited staffing services to Company Y –– a healthcare portfolio company based in Australia –– for a short-period of time to meet a resource need.

2. A Spanish affiliate of Audit Firm A provides payroll services to Company Z – a lodging (hotel chain) portfolio company based in Spain – for a short-period of time.

3. Company X has its own separate governance structure that is unrelated to Company Y or Z, and Company Y and Z are not material to Fund F.



Under the auditor independence rules prior to today's amendments, if Company X registers with the SEC (e.g., by conducting an initial public offering), Audit Firm A would not be independent of Company X as a result of the services provided to either Company Y or Z. This is the case regardless of whether, as the SEC staff has observed in similar situations,

these limited services at immaterial portfolio companies (like Companies Y and Z) have no impact on the entity under audit in any way and do not affect the objectivity and impartiality of the auditor in conducting the audit for Company X.

Under the rules prior to today's amendments, Company X would be required: (1) to replace Audit Firm A with another audit firm; (2) to wait to register with the SEC for up to three years after termination of the services provided to Company Y and Company Z; or (3) to make a determination, likely in consultation with Commission staff and/or the audit committee, that the rule violation did not impair the auditor's objectivity and impartiality.

In some situations, the existing audit firm cannot be replaced as a practical matter because all other qualified audit firms have themselves provided services or established other relationships with portfolio companies of Fund F that triggered a breach of our independence rules. The issue of the independence rule set affecting auditor choice is brought home by this example and has increased significantly as the asset management industry has grown, investments have become more global and the global audit services ecosystem has consolidated and become more specialized.

Under the rules as amended, Company X would be able to engage Audit Firm A for audit services. The hypothetical scenario described above is based directly on SEC staff's experience over the past decade. In recent years, the SEC staff conducted a number of consultations in which this fact pattern, or one similar to it, was raised to the SEC staff by the registrant's audit committee and its auditor, and the SEC staff, under such circumstances, did not object to the auditor's and the audit committee's conclusion that the auditor's objectivity and impartiality would not be impaired. SEC staff has provided similar feedback in these types of scenarios over the past decade. The amended rules would mitigate the need for registrants audit committees and their auditors to seek SEC staff guidance in these scenarios.

Highlights

The final amendments will:

1. Amend the definitions of "affiliate of the audit client," in Rule 2-01(f)(4), and "investment company complex," in Rule 2-01(f)(14), to address certain affiliate relationships, including entities under common control;
Amend the definition of "audit and professional engagement period," specifically Rule 2-01(f)(5)(iii), to shorten the look-back period, for

domestic first time filers in assessing compliance with the independence requirements;

2. Amend Rule 2-01(c)(1)(ii)(A)(1) and (E) to add certain student loans and de minimis consumer loans to the categorical exclusions from independence-impairing lending relationships;

3. Amend Rule 2-01(c)(3) to replace the reference to "substantial stockholders" in the business relationships rule with the concept of beneficial owners with significant influence;

4. Replace the outdated transition provision in Rule 2-01(e) with a new Rule 2-01(e) to introduce a transition framework to address inadvertent independence violations that only arise as a result of a merger or acquisition transactions; and

5. Make certain other miscellaneous updates.

What's Next?

The amendments will be effective 180 days after publication in the Federal Register. Voluntary early compliance is permitted after the amendments are published in the Federal Register in advance of the effective date provided that the final amendments are applied in their entirety from the date of early compliance. Auditors are not permitted to retroactively apply the final amendments to relationships and services in existence prior to the effective date or the early compliance date if selected by an audit firm.

To read more: https://www.sec.gov/rules/final/2020/33-10876.pdf

Number 10

Alert (AA20-283A) - APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Summary

Note: the analysis in this joint cybersecurity advisory is ongoing, and the information provided should not be considered comprehensive. The Cybersecurity and Infrastructure Security Agency (CISA) will update this advisory as new information is available.

This joint cybersecurity advisory was written by CISA with contributions from the Federal Bureau of Investigation (FBI).

CISA has recently observed advanced persistent threat (APT) actors exploiting multiple legacy vulnerabilities in combination with a newer privilege escalation vulnerability—CVE-2020-1472—in Windows Netlogon.

The commonly used tactic, known as vulnerability chaining, exploits multiple vulnerabilities in the course of a single intrusion to compromise a network or application.

This recent malicious activity has often, but not exclusively, been directed at federal and state, local, tribal, and territorial (SLTT) government networks.

Although it does not appear these targets are being selected because of their proximity to elections information, there may be some risk to elections information housed on government networks.

CISA is aware of some instances where this activity resulted in unauthorized access to elections support systems; however, CISA has no evidence to date that integrity of elections data has been compromised. There are steps that election officials, their supporting SLTT IT staff, and vendors can take to help defend against this malicious cyber activity.

Some common tactics, techniques, and procedures (TTPs) used by APT actors include leveraging legacy network access and virtual private network (VPN) vulnerabilities in association with the recent critical CVE-2020-1472 Netlogon vulnerability.

CISA is aware of multiple cases where the Fortinet FortiOS Secure Socket Layer (SSL) VPN vulnerability CVE-2018-13379 has been exploited to gain access to networks.

To a lesser extent, CISA has also observed threat actors exploiting the MobileIron vulnerability CVE-2020-15505. While these exploits have been observed recently, this activity is ongoing and still unfolding.

After gaining initial access, the actors exploit CVE-2020-1472 to compromise all Active Directory (AD) identity services. Actors have then been observed using legitimate remote access tools, such as VPN and Remote Desktop Protocol (RDP), to access the environment with the compromised credentials. Observed activity targets multiple sectors and is not limited to SLTT entities.

CISA recommends network staff and administrators review internet-facing infrastructure for these and similar vulnerabilities that have or could be exploited to a similar effect, including Juniper CVE-2020-1631, Pulse Secure CVE-2019-11510, Citrix NetScaler CVE-2019-19781, and Palo Alto Networks CVE-2020-2021 (this list is not considered exhaustive).

To read more:
https://us-cert.cisa.gov/sites/default/files/publications/AA20-283A-APT_Actors_Chaining_Vulnerabilities.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.

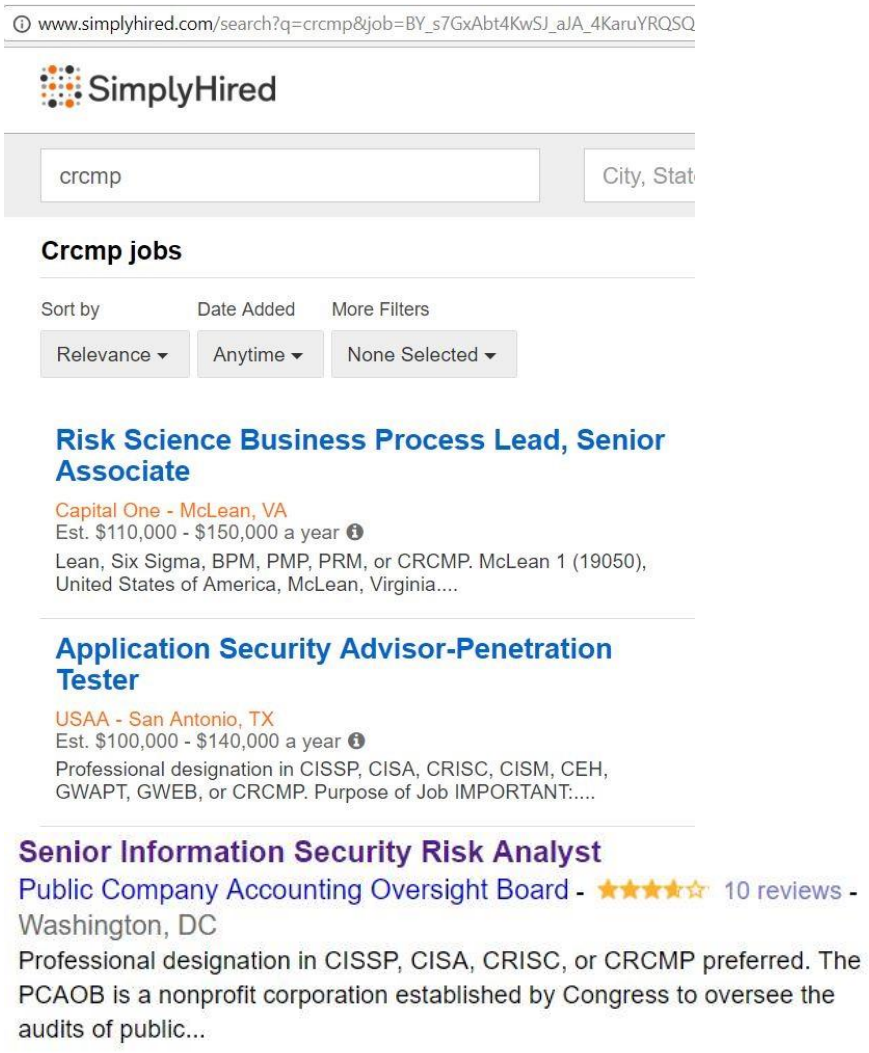
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

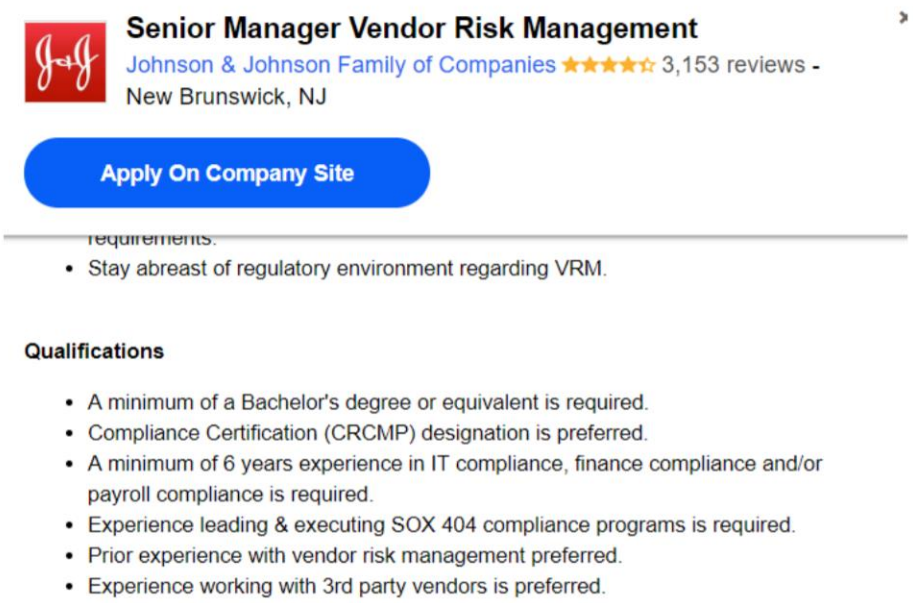
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become a Certified Risk and Compliance Management Professional (CRCMP), a Certified Information Systems Risk and Compliance Professional (CISRCP), a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, and / or a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I.





Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews -
New Brunswick, NJ

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

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

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
https://www.risk-compliance-association.com/IARCP_ACT.html

5. *Approved Training and Certification Centers (IARCP-ATCCs)* - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor led training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
https://www.risk-compliance-association.com/Approved_Centers.html