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

Monday, November 1, 2021

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 Anatole France, *to accomplish great things, we must not only act, but also dream; not only plan, but also believe.*

I have just read the "*Fiscal Year 2022, Bank Supervision Operating Plan*", from the Office of the Comptroller of the Currency (OCC), Committee on Bank Supervision. It is an interesting paper that gives a good understanding of the supervisory expectations, priorities and objectives.

The agency's fiscal year (FY) for 2022 begins October 1, 2021, and ends September 30, 2022.

Operational risk, resilience, incident response, data recovery and business resumption are supervisory focal points. Examinations should assess the bank's capabilities to *recover from destructive malware attacks*. Examinations should emphasize threat vulnerability and detection,

authentication and access controls, network management, data management, and managing *third-party access*.

Examiners should perform assessments of internal controls and operational processes that *changed* during the pandemic.

We read about *Fintech and Cryptocurrencies,* that examiners should identify banks that are implementing significant changes in their operations using new technological innovations and evaluate implementation, including use of cloud computing, artificial intelligence, and digitalization in the risk management processes.

Examiners should evaluate the appropriateness of governance processes when banks undertake significant changes.

We read about *Climate* that the OCC is working to *better understand* how the financial risks associated with climate change may affect the safety and soundness of institutions including their ability to serve all parts of their communities.

During FY2022, the OCC will continue information gathering efforts and plan on conducting additional industry outreach.

At the largest banks, examiners should focus on establishing a *baseline understanding* of the effects of physical and transition risks including the development of climate risk management frameworks and governance processes.

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

Best regards,

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

Number 8 (Page 29)

Updated from the Threat Analysis Group (TAG)

Ajax Bash, Threat Analysis Group

Number 9 (Page 32)

SEC Awards $40 Million to Two Whistleblowers

Number 10 (Page 35)

Ongoing Cyber Threats to U.S. Water and Wastewater Systems

Number 1

Fiscal Year 2022, Bank Supervision Operating Plan

Office of the Comptroller of the Currency, Committee on Bank Supervision

The Office of the Comptroller of the Currency's (OCC) Committee on Bank Supervision (CBS) strategy planning guidance sets forth the agency's supervision priorities and objectives.

The agency's fiscal year (FY) for 2022 begins October 1, 2021, and ends September 30, 2022.

The FY 2022 Bank Supervision Strategy Planning Guidance outlines the OCC's supervision priorities and aligns with "The OCC's Strategic Plan, Fiscal Years 2019–2023" and the National Risk Committee's (NRC) priorities.

The strategy planning guidance facilitates the development of supervisory strategies for individual national banks, federal savings associations, federal branches, and agencies of foreign banking organizations (collectively, banks), as well as identified service providers.

CBS managers and staff will use this plan to guide their supervisory priorities, planning, and resource allocations for FY 2022.

Priority Objectives for CBS Operating Units

The FY 2022 strategy planning guidance and the FY 2022 Bank Supervision Operating Plan establish priority objectives across the CBS operating units.

CBS operating units and managers should use this guidance to develop and execute individual operating unit plans and risk-focused bank supervisory strategies.

While the objectives are similar for the Large Bank Supervision and Midsize and Community Bank Supervision, CBS managers will differentiate bank size, complexity, and risk profile when developing individual bank supervisory strategies.

CBS operating plans include resources and support for risk-focused examinations of technology and significant service providers that provide critical processing and services to banks.

The OCC will adjust supervisory strategies, as appropriate, during the fiscal year in response to emerging risks and supervisory priorities.

For FY 2022, supervision will focus on the impacts of the pandemic and resulting economic, financial, operational, and compliance implications.

In addition to the baseline supervision to assign ratings, examiners will focus on the safety and soundness of strategic and operational planning, including:

• **Guarding against complacency:** Examiners should focus on strategic and operational planning to ensure banks maintain stable financial positions, especially regarding capital, the allowances for credit losses, management of net interest margins, and earnings.

Examiners should ensure banks remain vigilant when considering growth and new profit opportunities and will assess management's and the board's understanding of the impact of new activities on the bank's financial performance, strategic planning process, and risk profile.

• **Credit:** Examiners should evaluate banks' actions to manage credit risk given changes in market condition, termination of pandemic-related forbearance, uncertainties in the economy, and the lasting impacts of the COVID-19 pandemic.

Supervisory focus should ensure that risk management functions are providing an appropriate credible challenge. Examiners will evaluate underwriting practices on new or renewed loans for easing in structure and terms. Reviews will focus on new products, areas of highest growth, or portfolios that represent concentrations.

Supervisory focus should include those portfolios hard hit by the pandemic that may experience amplified impacts from changes in market conditions.

• **Allowance for loan and lease losses (ALLL)/allowance for credit losses (ACL):** For all banks, examiners should focus on ALLL and ACL adequacy considering any stress on credit portfolios.

U.S. Securities and Exchange Commission (SEC) filers, except small reporting companies as defined by the SEC, were required to adopt the current expected credit losses (CECL) accounting standard in 2020 but could delay adoption until 2022.

All other banks are required to implement CECL by 2023. For banks that have not yet adopted CECL, examiners should evaluate preparedness,

including bank implementation plans and use of third parties to assist in the development of the loss estimation methodology, modeling techniques, and management information systems.

Additional impacts may include post-hardship performance of borrowers assisted with streamlined deferral and loan modifications.

For banks that have adopted CECL, examiners should evaluate the effectiveness of the methodology at estimating lifetime expected credit losses.

• **Cybersecurity:** Operational risk, resilience, incident response, and data recovery and business resumption should be supervisory focal points. Examinations should assess the bank's capabilities to recover from destructive malware attacks.

Examinations should emphasize threat vulnerability and detection, authentication and access controls, network management, data management, and managing third-party access.

Examiners should perform assessments of internal controls and operational processes that changed during the pandemic.

• **Third parties and related concentrations:** Examiners should determine whether banks are providing proper oversight of their significant third-party relationships, including partnerships.

Examiners should identify where those relationships are critical to bank operations and understand whether they represent significant concentrations or impact resiliency.

Examiners should also be aware of the cyber-related risks emanating from third parties and evaluate the bank assessments of the third party's cybersecurity risk management and resilience capabilities.

• **Bank Secrecy Act, consumer compliance, and fair lending:**

- **BSA/AML and Office of Foreign Assets Control:** Strategies should continue to focus on BSA/AML compliance, with emphasis on evaluating the effectiveness of BSA/AML risk management systems relative to the complexity of business models, products and services offered, and customers and geographies served; evaluating technology and modeling solutions to perform or enhance BSA/AML oversight functions; and determining the adequacy of suspicious activity

monitoring and reporting systems and processes in providing meaningful information to law enforcement.

Examiners should also begin to assess bank change management plans for implementing changes to existing BSA/AML compliance programs that will be required regulatory changes to implement the Anti-Money Laundering Act of 2020.

- **Consumer compliance:** Examiners should focus on compliance management systems, including third-party risk management and higher risk products and services such as overdraft protection programs, particularly focusing on how the programs are implemented and how terms of the programs are disclosed.

  Examiners should consider the effect that earnings pressure has had on banks, monitoring the effect that may have had on the compliance risk management functions, if any, through cutting personnel or waiving audits.

- **Fair lending:** Examiners should focus on assessing fair lending risk, considering changes to the bank's products, services, and operating environments.

  These should be based upon the bank's fair lending risk profile and the annual Home Mortgage Disclosure Act data screening process. Fair lending supervision activities should consider the full lifecycle of credit products (e.g., mortgages).

- **CRA:** OCC Bulletin 2020-99, "Community Reinvestment Act: Key Provisions of the June 2020 CRA Rule and Frequently Asked Questions," provides updated guidance following issuance of the OCC's June 2020 rule.

  Examiners should be familiar with this set of policies and procedures and plan accordingly for examinations that cover calendar years before and during the time that the 2020 rule is in effect.

  In addition, the OCC has proposed to rescind the June 2020 rule and replace it with rules largely like the 1995 CRA rules. Examiners should plan on additional training on these rule changes and to incorporate new CRA policy or process guidance issued during FY2022.

• **Interest rate risk:** Examiners should assess the impact of a low-rate environment on banks' business models, strategies, asset and liability risk exposures, net interest margin, funding stability, and modeling capabilities.

• **London Interbank Offered Rate (LIBOR):** Examiners should evaluate each bank's implementation and execution of alternative reference rates given the December 30, 2021, cessation of LIBOR.

Banks should fully understand all their exposures and be nearly complete with remediation efforts. Examiners should evaluate operational, reputation, and consumer impact assessments and change management related to an alternative index for pricing loans, deposits, and other products and services.

• **Payments:** Examiners should evaluate payment systems products and services that banks offer or plan to offer, with a focus on new or novel products, services, or channels for wholesale and retail customer relationships.

Examiners should consider potential risks including operational, compliance, strategic, credit, and reputation and how these risks are incorporated into institution-wide risk assessments and new product review processes, if applicable.

• **Fintech/Cryptocurrency:** Examiners should identify banks that are implementing significant changes in their operations using new technological innovations and evaluate implementation, including use of cloud computing, artificial intelligence, and digitalization in the risk management processes.

Examiners should evaluate the appropriateness of governance processes when banks undertake significant changes.

• **Climate:** The OCC is working to better understand how the financial risks associated with climate change may affect the safety and soundness of institutions including their ability to serve all parts of their communities.

During FY2022, the agency will continue information gathering efforts and plan on conducting additional industry outreach.

At the largest banks, examiners should focus on establishing a baseline understanding of the effects of physical and transition risks including the development of climate risk management frameworks and governance processes.

Resources should focus on significant risks in FY2022 while considering appropriate coverage of other areas. Strategies should focus on control functions and leverage the institutions' audit, loan review, and risk management processes when the OCC has validated reliability.

To facilitate an agency-wide view of risk on selected topics, the CBS operating units will prioritize and coordinate resources and conduct horizontal risk assessments during the fiscal year. The CBS may direct horizontal assessments during the supervisory cycle.

The OCC will provide periodic updates about supervisory priorities, emerging risks, and horizontal risk assessments in the Semiannual Risk Perspective report.

Number 2

Cyber risks: what is the impact on the insurance industry?

October is the European cyber security month. As cyber attacks are a continuing risk for insurers, in this article we are discussing their incidence in the financial industry as a whole and among insurers in particular, why insurers are on the radar and what are the consequences for insurers and for policyholders.

The pandemic has accelerated the digital transformation. Financial institutions have increased their use of information technology. They are now more heavily relying on digital and remote solutions to perform their daily operations and to deliver their services to customers.

While this has brought along benefits, the increasing reliance on digital solutions has also expanded the risk for cyber attacks.

Cyber risks are considered as a top global risk for the financial sector and the economy as a whole. The type of ICT risks to which the undertakings are exposed have not changed in the past years, however the frequency of incidents and the magnitude of their impact on financial entities has increased.

A recent study on Covid-19 and cyber risk in the financial sector revealed that the financial sector has experienced the largest number of Covid-19-related cyber events after the health sector. Payment institutions, insurers and credit unions are the most affected.

Insurers in some jurisdictions are reporting an increasing number of malware and other cyber attempts.

Insurance supervisors consider cyber security risks as the main trigger of other risks, as highlighted by the European Supervisory Authorities (EIOPA, ESMA and EBA) in their report on the risks and vulnerabilities in the financial sector.

Some of these risks include:

- digitalisation risks (for 73% of insurance supervisors)
- cyber underwriting risks (19%)
- InsurTech competition (8%)

Why insurers are on the radar of cyber attacks ?

Insurance groups are a natural target for cyber attacks because they possess substantial amounts of confidential policyholder data. Products, policies and pricing are all powered by data.

This is what makes it so valuable: with data an insurance company is able to offer the consumer just what they need and hopefully at just the right price. More choice and lower costs are what makes consumers so ready to share their data.

In contrast to other sectors, which hold mainly sensitive financial data, insurers typically also collect a large amount of protected personal sensitive information.

What are the consequences?

The main consequences suffered by insurers following these cyber incidents are business interruption and material costs for the undertaking, for policyholders and for third parties.

Data obtained can be used for different criminal purposes such as identity theft to obtain financial gains.

Besides the direct financial consequences, cyber incidents can also result in severe and long-lasting operational issues for the targeted insurance groups. The reputational damage may also be substantial or even irreversible.

If malicious cyber incidents cause business interruptions, this has a direct impact on all policyholders.

At the same time, as a direct consequence of the increase of ICT incidents as described above the cyber-underwriting market is expanding. According to Statista, the European cyber insurance market is expected to grow exponentially between 2020 and 2030, doubling in size between 2020 and 2025. Insurers have their role to play in this area. A sound cyber insurance market is an important measure. The challenge is how to insure and help prevent cyber risk.

In conclusion, insurers and pension funds need not only to manage cyber and IT risk within the company and the value chain, but they also need to keep pace with new threats and developments. Here operational resilience testing and cooperation can help and as such EIOPA welcomes the Digital

Operational Resilience Act, or DORA and other initiatives in this field and stands ready to contribute.

The Digital Operational Resilience Act (DORA): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

Brussels, 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

EIOPA will continue to monitor and motivate innovation, while keeping a close eye on new risks that are emerging, as well as on how consumers are served.

Number 3

Progress report on adoption of the Basel regulatory framework

BIS

The Basel Committee on Banking Supervision (BCBS) and its oversight body, the Group of Central Bank Governors and Heads of Supervision (GHOS) have set as high priority the full, timely and consistent implementation of all aspects of the Basel III framework.

This includes the finalised Basel III post-crisis reforms published by the Committee in December 2017 and set to go into effect on 1 January 2023 with a five-year phase-in.

Continuing the periodic monitoring initiated a decade ago, this report sets out the adoption status of Basel III standards for each of the BCBS member jurisdictions as of end-September 2021.

It is part of the broader Committee's Regulatory Consistency Assessment Programme (RCAP) established to monitor progress in introducing corresponding domestic regulations, assessing their consistency and analysing regulatory outcomes.

Despite the disruptions resulting from Covid-19 and the required shift in regulatory and supervisory priorities, further progress has been made in the implementation of the Basel III standards especially those with deadlines that have already passed.

In fact, many jurisdictions used the existing flexibilities in the Basel framework to provide regulatory relief during the pandemic.

All jurisdictions now have final rules in force for the countercyclical capital buffer (CCyB). Overall, in respect of the outstanding capital standards there have been 11 new adoptions.

This includes three additional jurisdictions which have adopted final rules with regard to total loss-absorbing capacity (TLAC), and two additional jurisdictions which have adopted final rules with regard to the standardised approach for measuring counterparty credit risk exposure (SA-CCR) and capital requirements for equity investments in funds.

An additional four jurisdictions have adopted the Net Stable Funding Ratio (NSFR) standard. Further, across the disclosure parts of the framework there have been seven additions. In respect of the Basel III standards which have a deadline in the future, there have been new adopters of the revised

operational risk framework and revised standardised approach for credit risk.

The report excludes standards that had previously been implemented by all jurisdictions such as the Liquidity Coverage Ratio (LCR) and capital conservation buffers (CCoB) and is based on Basel adoption status updates submitted by jurisdictions as of end-September 2021.

A complete view by standard and jurisdiction is provided in the Overview section followed by summary information about the implementation status and adoption plans for each of the 27 jurisdictions and the EU.

Table 1: Member jurisdictions that have issued final rules

Standard		Number of jurisdictions as of end-May 2020	Number of jurisdictions as of end-September 2021	Increase in adoption
Capital	Countercyclical capital buffer	26	27	1
	Margin requirements for non-centrally cleared derivatives	19	20	1
	Capital requirements for CCPs	21	22	1
	Capital requirements for equity investments in funds	19	21	2
	SA-CCR	23	25	2
	Securitisation framework	21	22	1
	TLAC holdings	18	20	3*
	Revised standardised approach for credit risk	1	2	1
	Revised operational risk framework	2	5	3
Liquidity	Net Stable Funding Ratio (NSFR)	22	26	4
Disclosure	CCyB, Liquidity, Remuneration, Leverage ratio (revised)	20	21	1
	Key metrics, IRRBB, NSFR	15	18	3
	Composition of capital, RWA overview, Prudential valuation adjustments, G-SIB indicators	19	20	1
	TLAC Disclosure	15	17	2

* The increase in adoption is actually three in 2021 rather than two. This is because one jurisdiction revised its TLAC status from fully adopted (4) to not applicable (na) during this period.

Table 1 highlights the progress made since the last report published in July 2020 by listing the standards with an increase in the number of jurisdictions with final rules in place.

The shaded area indicates the standards with deadlines in the future. Further evaluation of the consistency of jurisdictional implementation is

addressed through the RCAP assessments. The outstanding RCAP on NSFR and large exposures framework (LEX) are expected to resume soon after they were suspended last year in response to Covid-19.

Overview of implementation

	Basel standards	Deadline	AR	AU	BR	CA	CN	HK	IN	ID	JP	KR	MX	RU	SA	SG	ZA	CH	TR	UK	US	EU
Capital	Countercyclical capital buffer	Jan 2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	Margin requirements for non-centrally cleared derivatives	Sep 2016	1	4	4	4	1	4	2	2	4	3	2	2	4	4	4	4	1	4	4	4
	Capital requirements for CCPs	Jan 2017	4	4	4	4	1	4	3	2	4	4	1	2	4	4	4	4	2	3	3	4
	Capital requirements for equity investments in funds	Jan 2017	4	4	4	4	1	2	na	na	4	4	*	4	4	4	4	4	4	3	1	4
	SA-CCR	Jan 2017	4	4	4	4	4	4	3	4	4	4	1	4	4	4	4	4	2	3	3	4
	Securitisation framework	Jan 2018	4	4	4	4	1	4	4	4	4	4	1	4	4	4	2	4	1	4	1	4
	TLAC holdings	Jan 2019	na	4	4	4	2	4	1	na	4	1	4	4	4	4	2	4	1	4	4	4
	Revised standardised approach for credit risk	Jan 2023	1	2	2	2	1	1	1	2	2	3	4	2	1	2	1	1	1	1	1	1
	Revised IRB approach for credit risk	Jan 2023	na	2	1	2	1	1	1	na	2	3	1	4	1	2	1	1	1	1	1	1
	Revised CVA framework	Jan 2023	1	1	1	2	1	1	1	2	2	1	1	1	1	2	1	1	1	1	1	1
	Revised minimum requirements for market risk	Jan 2023	1	1	*	2	1	1	1	2	2	1	1	1	2	2	1	1	1	1	1	*
	Revised operational risk framework	Jan 2023	1	3	1	2	1	1	1	3	2	3	4	4	2	2	1	1	1	1	1	1

Status classification code (numerical code):

4=Final rule in force: the domestic legal or regulatory framework has been published and is implemented by banks;

3=Final rule published: the domestic legal or regulatory framework has been published but is not implemented by banks;

2=Draft regulation published: a draft law, regulation or other official document has been made public and is specific enough to be implemented;

1=Draft regulation not published: no draft law, regulation or other official document has been made public to detail the planned content of the domestic regulatory rules.

This status includes cases where a jurisdiction has communicated high-level information about its implementation plans, but not detailed rules.

* = Cases where the implementation status for the full standard is partial are indicated with an asterisk;

na = not applicable.

Applicable standards for which the agreed implementation deadline has passed receive a colour code to reflect the status (colour code):

green = adoption completed;

yellow = adoption in process (at least some draft regulation published);

red = adoption not started (no draft regulation published yet).

A standard is deemed to be adopted and implemented when the numerical code is 4 and the colour code is green.

To read more: https://www.bis.org/bcbs/publ/d525.pdf

Number 4

BaFin amends its BAIT

In the current amendment to the BAIT, BaFin clarifies its expectations for IT and information security at banks.
Thorsten Sämisch, BaFin IT Supervision Group

BaFin Federal Financial Supervisory Authority

On 16 August 2021, BaFin published the new version of its BAIT, the Supervisory Requirements for IT in Financial Institutions. The amendment came into force on the same date.

BaFin is using this amendment to set out the overall conditions it now expects for secure information processing and information technology.

There are no transitional periods because BaFin is not imposing any fundamental new requirements, but has clarified existing requirements.

Background to the amendment

Guidelines issued by the European Banking Authority (EBA) in November 2019 form part of the backdrop to the BAIT amendment. You may visit: https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

In its Guidelines on ICT and security risk management (EBA/GL/2019/04), the EBA had previously responded to the European Commission's FinTech action plan and introduced standardised requirements for the entire single market: for credit institutions, investment firms and payment service providers.

The EBA thus established the corresponding framework for the supervisory practice of the national competent authorities.

Together with the Deutsche Bundesbank, BaFin then examined whether, and to what extent, the BAIT would have to be supplemented and adapted. Experience gained from supervisory practice was also expected to be incorporated into the work.

The IT expert committee, whose members are representatives of the trade associations of the banking sector, smaller and larger institutions, as well as BaFin and Bundesbank staff, was also closely involved in the amendment. The Federal Ministry of Finance also participated.

A public consultation on the BAIT amendment was launched in autumn 2020.

Because the content of the BAIT builds on the Minimum Requirements for Risk Management (MaRisk) , the BAIT amendment was developed in parallel with the sixth amendment to MaRisk, and both circulars were published at the same time.

Significant amendments

Even though there were no fundamental changes, some parts of the BAIT were expanded and adapted.

In the new "Operational information security" chapter, for example, BaFin sets out requirements for the design of effectiveness controls of information security measures that have already been implemented in the shape of tests and exercises.

Such effectiveness controls, for example gap analysis, vulnerability scans, penetration tests and simulated attacks, are a key element of any effective, sustainable information security management system.

The institutions must verify the security of the IT systems regularly and on an event-driven basis. They must avoid conflicts of interest when they do so: for example, anybody involved in planning and implementing security measures cannot subsequently test them.

The institutions have to analyse the results of such effectiveness controls, identify any need for improvement and manage risks appropriately.

The institutions are expected to document the new requirements in an internal policy that BaFin now calls for in the "Information security management" chapter.

This chapter also contains requirements relating to logging and monitoring, in other words recording results and real-time monitoring, as well as the identification and analysis of security-related events.

For example, potentially security-related information must be evaluated suitably promptly, using a rule-based approach, and must be held available for an appropriate period for subsequent evaluation.

To do this, a portfolio of rules for identifying security-related events must be defined and updated.

The expanded AT 7.3 “Contingency management” in the new MaRisk forms the basis for the new BAIT chapter “IT contingency management”.

It stipulates the establishment of restart, emergency operation and recovery plans for time-critical processes and activities.

According to the BAIT, the institutions must verify annually that these three types of IT contingency plan are effective – based on an IT testing concept.

The new third chapter in the BAIT is called “Managing relationships with payment service users”.

It is taken from the new circular “Supervisory Requirements for IT in Payment Services and Electronic Money Institutions” (ZAIT). Its content is also relevant for large parts of the BAIT target group.

Information security instead of IT security

It was also important for BaFin and the Deutsche Bundesbank to follow the objective of “information security” in the BAIT and not the – narrower – objective of “IT security”.

Traditional IT security is limited to the field of information technology, whereas information security aims to protect relevant information, regardless of the form it takes. The area of information security therefore encompasses everything related to information processing.

In the context of information security and information risk management (ISM/IRM), it is now spelled out more clearly that the business processes concerned must take effect across the entire organisation, and that it is not enough to provide adequate resources to IT operations and application development alone.

The BAIT requirements now clarify, for example, that the institutions must develop a comprehensive training and awareness programme for their staff on the topic of information security.

The BAIT reflect the requirement in the EBA guidelines referred to earlier for a clear allocation of responsibilities by designating additional roles and tasks of information security and information risk management and differentiating them from responsibilities for business processes.

Among other things, the organisational units that are responsible for the individual business processes are responsible for determining and

documenting the protection requirements of the relevant processes. By contrast, information risk management is responsible for verifying this determination and documentation.

In light of the complexity of cyber threats, the BAIT now expressly emphasise how important it is for institutions to keep themselves informed about current external and internal threats and vulnerabilities, and to notify the management board about the risk analysis and changes in the risk situation.

The BAIT chapter “Information risk management” now clarifies that threats and vulnerabilities must also be taken into account by information risk management if they could pose risks to the organisation.

Several BAIT chapters address requirements for physical security, as described in the EBA guidelines.

For example, the institutions must develop a physical security policy, implement physical access controls and establish an adequate perimeter protection using state-of-the-art technology. Perimeter protection means protecting the area between the building and the property boundary.

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2021/fa_bj_2108_BAIT_en.html

Number 5

Transforming risk culture: observations from APRA's pilot survey

- APRA's risk culture survey is internationally leading regulatory practice that expands its supervisory toolkit to transform risk culture.

- Survey results provide a unique employee view of the risk management practices and behaviours in an entity.

- APRA will benchmark up to 60 more entities in the next 12 months, and will share additional insights with industry.

A strong risk culture is essential for effective risk management outcomes that support an organisation's financial and operational resilience.

Ultimately, organisations with a strong risk culture that supports sound risk management practices and behaviours are better placed in terms of financial performance and fair, quality outcomes for their customers.

Under Prudential Standard CPS 220 Risk Management, the boards of APRA-regulated entities are required to form a view of the risk culture in the institution that they govern, and identify any desirable changes to the risk culture necessary to ensure that culture supports the ability of the institution to operate consistently within its risk appetite.

APRA aims to reinforce, support and assess the work regulated entities are doing to build and maintain an effective risk culture. To this end, APRA has introduced an industry-wide risk culture survey recently piloted with 10 general insurance entities.

The survey is a key initiative that supports APRA's expanded supervisory toolkit designed to transform governance, risk culture, remuneration and accountability (GCRA) practices across regulated entities.

APRA's pilot risk culture survey, conducted between March and April 2021, provides insights from employees on perceived risk behaviours and the effectiveness of the risk management structures within their entities.

The responses, over time, will determine the extent to which positive changes to risk culture are (or are not) taking place within individual entities, and correspondingly, will identify areas where an entity's risk culture can be improved.

The survey also provides the opportunity to benchmark results across a number of regulated entities within an industry sector (for example, insurance), providing an opportunity for entity leaders and APRA supervisors to understand how the entity's results compare to others in its peer group.

APRA is one of the only regulatory bodies worldwide that directly collects survey data at an industry level, so APRA's risk culture survey represents internationally leading regulatory practice.

What is risk culture?

Risk culture refers to an entity's attitudes and behaviours towards risk management. Specifically, it is the behavioural norms and practices of individuals and groups that shape an entity's ability to identify, understand, openly discuss, escalate and act on its current and emerging risks.

A strong risk culture creates an environment where employees are comfortable speaking up and voicing concerns with their leaders. It produces better decisions by ensuring a broader range of views are considered, and allows ideas that present heightened risks to be appropriately challenged during decision-making.

It incentivises boards and senior executives to prioritise effective risk management. In doing these things, a strong risk culture helps to deliver better business and customer outcomes for organisations. APRA is committed to enhancing and reinforcing a strong risk culture across all regulated entities.

In particular, an entity's risk culture is influenced and shaped by two key aspects:

- *Risk behaviours:* the observable actions and behaviours of individuals and groups (for example, role modelling, operating practices and symbols, such as discussion of risk management as a standing agenda item in team meetings), and

- *Risk architecture:* the formal structures and arrangements that support the management of risks (for example, systems, policies, procedures and governance structures).

APRA's Risk Culture 10 Dimensions

APRA has developed a framework called the Risk Culture 10 Dimensions to assess the risk culture of regulated entities. The Risk Culture 10 Dimensions

articulate the key aspects of an entity's risk behaviours and risk architecture that contribute to its risk culture. Each of the survey questions in the pilot (approximately 40) aligned with one of APRA's Risk Culture 10 Dimensions.

The Risk Culture 10 Dimensions – coupled with the survey results – allow APRA to access comparable data in a consistent way across regulated entities in order to assess and benchmark risk culture.

Figure 1: APRA's Risk Culture 10 Dimensions

APRA's Risk Culture 10 Dimensions is not a prescriptive framework, and APRA does not expect entities to adopt it. While the 10 Dimensions framework provides insights into how APRA assesses risk culture, an entity should have a risk culture framework that fits its own particular circumstances (such as its size and complexity).

This framework should allow an entity to measure, monitor and report on its risk culture in a consistent and meaningful way.

To read more:
https://www.apra.gov.au/transforming-risk-culture-observations-from-apra%E2%80%99s-pilot-survey

Number 6

Approval of first Swiss crypto fund

finma

The Swiss Financial Market Supervisory Authority FINMA has approved the first crypto fund according to Swiss law. The fund, which is restricted to qualified investors, invests primarily in so-called cryptoassets. For the first time, FINMA has approved a Swiss fund that invests primarily in cryptoassets, that is to say in assets based on the blockchain or distributed ledger technology.

The fund concerned goes by the name of the “Crypto Market Index Fund”, an investment fund according to Swiss law belonging to the category "other funds for alternative investments" with particular risks. Distribution of this fund is restricted to qualified investors.

Consideration of the particular risks

In order to facilitate serious innovation, FINMA applies the existing provisions of financial market laws in a consistently technology-neutral way, i.e. in keeping with the “same risks, same rules” principle.

In doing so, it makes sure that new technologies are not being used to circumvent the existing rules and that the protective goals of financial market legislation are preserved.

Since cryptoassets involve particular risks, FINMA also tied the approval to specific requirements in the present case. For instance, the fund may only invest in established cryptoassets with a sufficiently large trading volume.

Furthermore, the investments must be made through established counterparties and platforms that are based in a member country of the Financial Action Task Force (FATF) and are subject to corresponding anti-money laundering regulations.

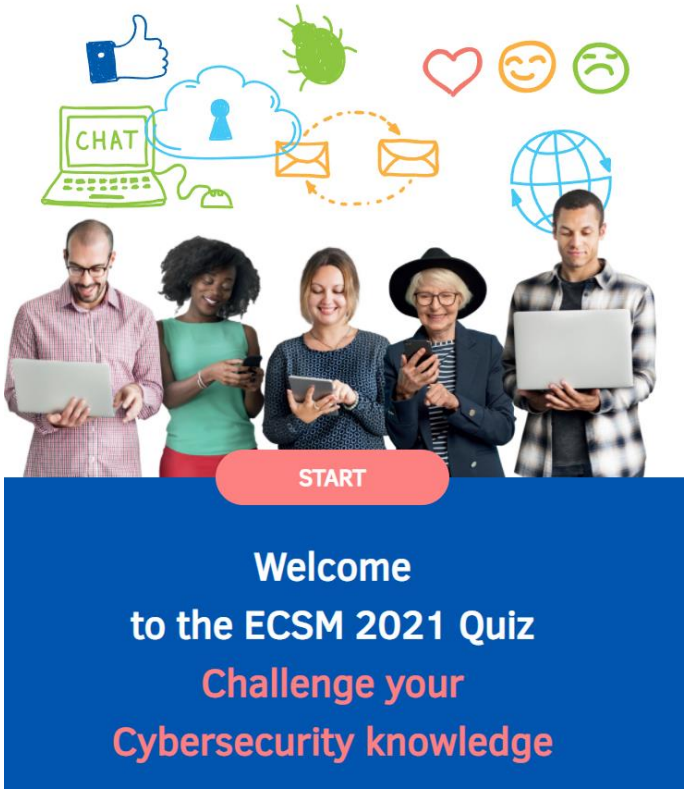
Finally, there are specific requirements with regard to risk management and reporting for the institutions involved in the management and custody.

To read more:
https://www.finma.ch/en/news/2021/09/20210929-mm-genehmigung-schweizer-kryptofonds/

Number 7

European Cybersecurity Month: Test your Skills with a Quiz

The new ECSM Quiz goes live. The game will guide players through mock adventures with IT, testing their skills on everyday online actions, such as replying to an email, which could have hidden traps.



Everyone is welcome to play. After each quiz, players will learn about the risks and the traps to avoid. The aim of the quiz is to increase cyber hygiene among players, encouraging them to stay vigilant and #ThinkB4UClick.

For the ECSM Quiz you may visit: https://cybersecuritymonth.eu/quiz

The 'Cyber First Aid' theme running until 31 October, will introduce guidelines on how to deal with a cyberattack. Citizens will be able to access an interactive EU map to find local services they can contact and get advice from in case they fall victim of online shopping frauds, identity theft or social media hacks. In addition, they will also be able to register to interactive events on the ECSM platform and access videos and tips.

Covering topics such as online shopping fraud and social media hacks, organisers will showcase first aid resources for the most common cyber threats. 'Cyber First Aid' will kick off with a video on the real life story of a small business owner who experienced a ransomware attack and came out on top.

'Cyber First Aid' includes key advice for online users:

- #ThinkB4UClick: When receiving a message that appears to be from a social media provider, check the source of the email address first;

- Secure online accounts with a multi-factor authentication (MFA) and with strong, unique passwords;

- In the case of a cyberattack, immediately inform the social media provider(s) and report it to the relevant local authorities, find local resources using the interactive map;

- Never pay ransom to cyber criminals, as there is no guarantee they will give in and paying ransom only encourages them to continue their criminal activity towards others.

To read more:
https://www.enisa.europa.eu/news/enisa-news/cybersecurity-month-test-your-skills-with-a-quiz

Number 8

Updated from the Threat Analysis Group (TAG)

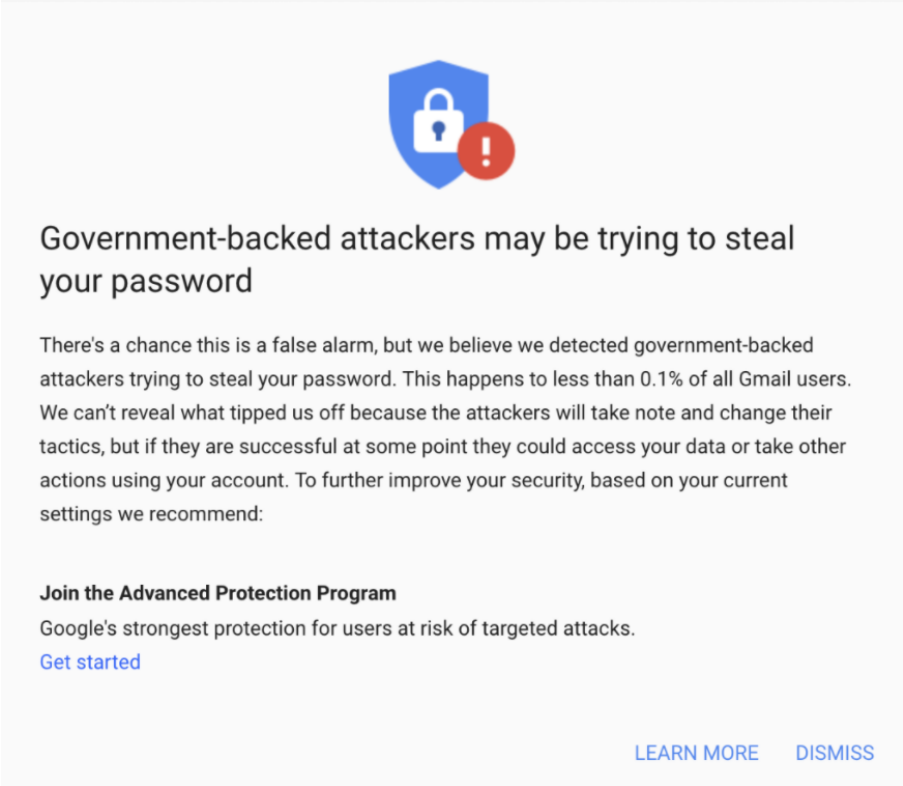
Ajax Bash, Threat Analysis Group

Google

Google's Threat Analysis Group tracks actors involved in disinformation campaigns, government backed hacking, and financially motivated abuse.

We have a long-standing policy to send you a **warning** if we detect that your account is a target of government-backed phishing or malware attempts.

Google



So far in 2021, we've sent over 50,000 warnings, a nearly 33% increase from this time in 2020. This spike is largely due to blocking an unusually large campaign from a Russian actor known as APT28 or Fancy Bear.

We intentionally send these warnings in batches to all users who may be at risk, rather than at the moment we detect the threat itself, so that attackers cannot track our defense strategies. On any given day, TAG is tracking more than 270 targeted or government-backed attacker groups from more than

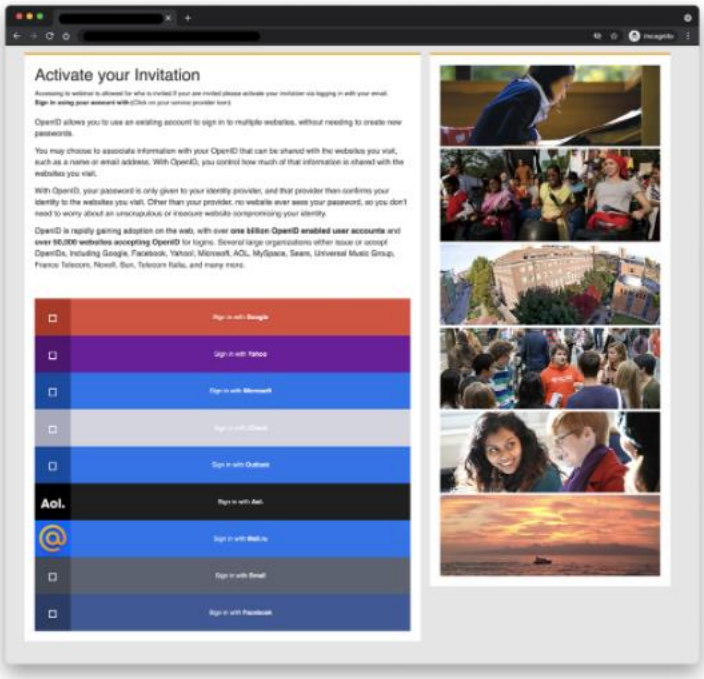
50 countries. This means that there is typically more than one threat actor behind the warnings.

In this blog, we explore some of the most notable campaigns we've disrupted this year from a different government-backed attacker: APT35, an Iranian group, which regularly conducts phishing campaigns targeting high risk users.

This is the one of the groups we disrupted during the 2020 US election cycle for its targeting of campaign staffers. For years, this group has hijacked accounts, deployed malware, and used novel techniques to conduct espionage aligned with the interests of the Iranian government.

Hijacked websites used for credential phishing attacks

In early 2021, APT35 compromised a website affiliated with a UK university to host a phishing kit. Attackers sent email messages with links to this website to harvest credentials for platforms such as Gmail, Hotmail, and Yahoo. Users were instructed to activate an invitation to a (fake) webinar by logging in. The phishing kit will also ask for second-factor authentication codes sent to devices.



Phishing page hosted on a compromised website

APT35 has relied on this technique since 2017 — targeting high-value accounts in government, academia, journalism, NGOs, foreign policy, and national security. Credential phishing through a compromised website

demonstrates these attackers will go to great lengths to appear legitimate – as they know it's difficult for users to detect this kind of attack.

Utilization of Spyware Apps

In May 2020, we discovered that APT35 attempted to upload spyware to the Google Play Store.

The app was disguised as VPN software that, if installed, could steal sensitive information such as call logs, text messages, contacts, and location data from devices.

Google detected the app quickly and removed it from the Play Store before any users had a chance to install it.

Although Play Store users were protected, we are highlighting the app here as TAG has seen APT35 attempt to distribute this spyware on other platforms as recently as July 2021.

Conference-themed phishing emails

One of the most notable characteristics of APT35 is their impersonation of conference officials to conduct phishing attacks.

Attackers used the Munich Security and the Think-20 (T20) Italy conferences as lures in non-malicious first contact email messages to get users to respond.

When they did, attackers sent them phishing links in follow-on correspondence. Targets typically had to navigate through at least one redirect before landing on a phishing domain.

Link shorteners and click trackers are heavily used for this purpose, and are oftentimes embedded within PDF files. We've disrupted attacks using Google Drive, App Scripts, and Sites pages in these campaigns as APT35 tries to get around our defenses. Services from Dropbox and Microsoft are also abused.

To read more:
https://blog.google/threat-analysis-group/countering-threats-iran/

Number 9

SEC Awards $40 Million to Two Whistleblowers

U.S. SECURITIES AND EXCHANGE COMMISSION

The Securities and Exchange Commission today announced awards of approximately $40 million to two whistleblowers whose information and assistance contributed to the success of an SEC enforcement action.

The first whistleblower, whose information caused the opening of the investigation and exposed difficult-to-detect violations, will receive an award of approximately $32 million.

The first whistleblower also provided substantial assistance to the staff, including identifying witnesses and helping the staff to understand complex fact patterns.

The second whistleblower, who submitted important new information during the course of the investigation but waited several years to report to the Commission, will receive an award of approximately $8 million.

"Today's whistleblowers underscore the importance of the SEC's whistleblower program to the agency's enforcement efforts," said Emily Pasquinelli, Acting Chief of the SEC's Office of the Whistleblower. "These whistleblowers reported critical information that aided the Commission's investigation and provided extensive, ongoing cooperation that helped the Commission to stop the wrongdoing and protect the capital markets."

The SEC has awarded approximately **$1.1 billion** to 218 individuals since issuing its first award in 2012. All payments are made out of an investor protection fund established by Congress that is financed entirely through monetary sanctions paid to the SEC by securities law violators.

No money has been taken or withheld from harmed investors to pay whistleblower awards. Whistleblowers may be eligible for an award when they voluntarily provide the SEC with original, timely, and credible information that leads to a successful enforcement action.

Whistleblower awards can range from 10-30% of the money collected when the monetary sanctions exceed $1 million.
As set forth in the Dodd-Frank Act, the SEC protects the confidentiality of whistleblowers and does not disclose information that could reveal a whistleblower's identity.
For more information about the whistleblower program and how to report a tip, visit www.sec.gov/whistleblower

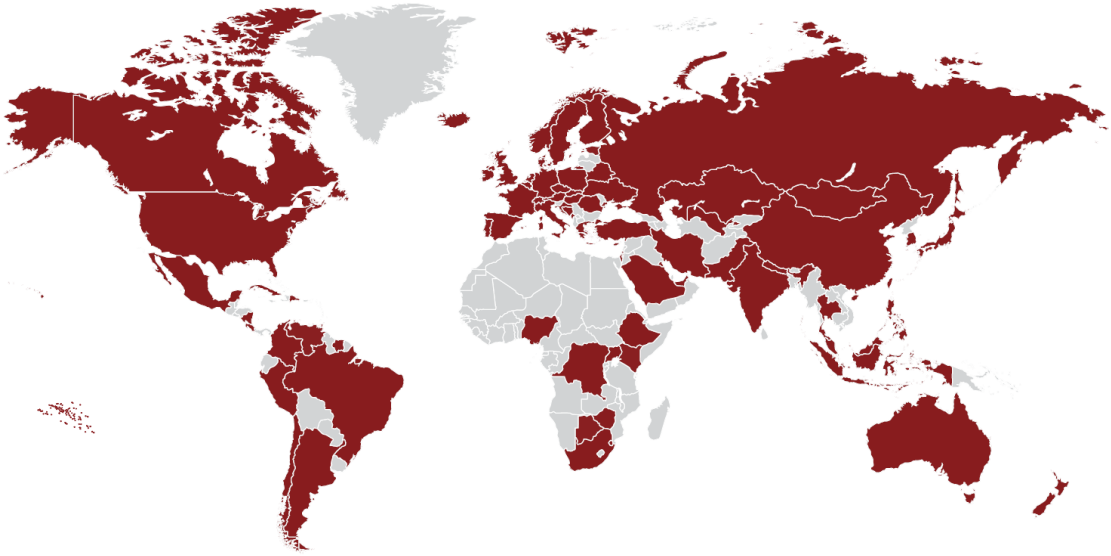
U.S. SECURITIES AND EXCHANGE COMMISSION

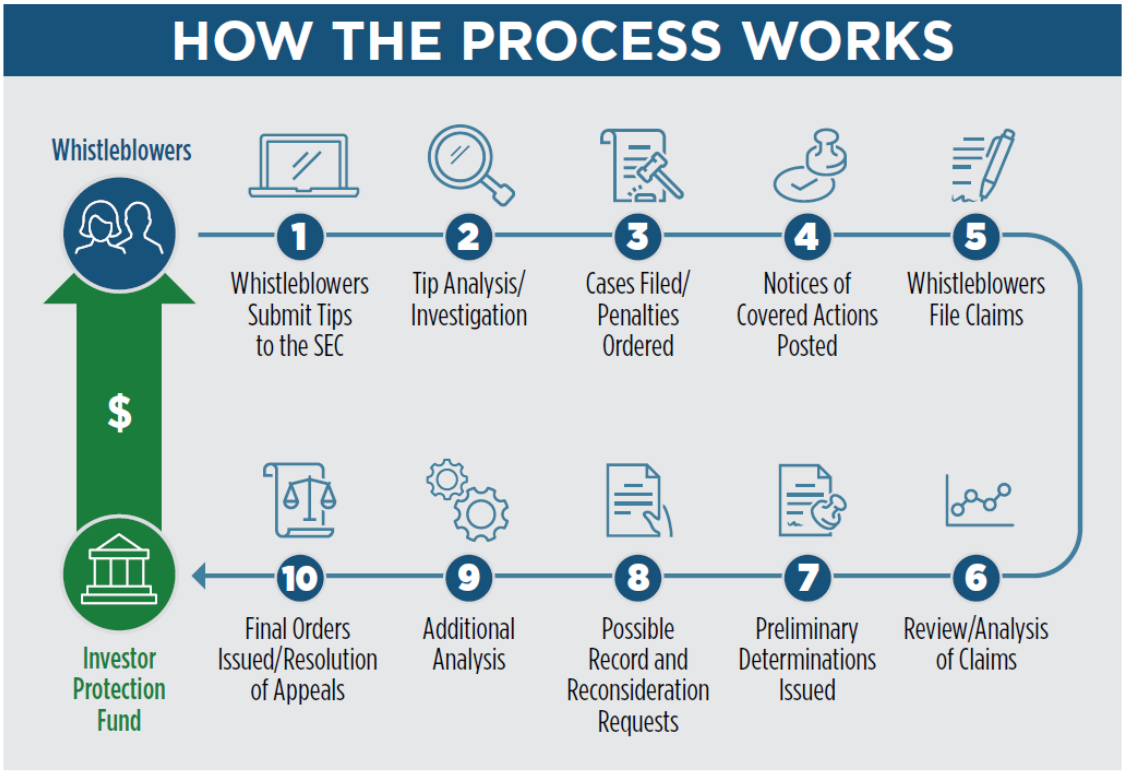
ABOUT | DIVISIONS & OFFICES | ENFORCEMENT | REGULATION

Office of the Whistleblower

Office of the Whistleblower

The map below reflects the countries in which whistleblower tips originated during FY 2020.




HOW THE PROCESS WORKS
Whistleblowers
$
Investor Protection Fund
1
Whistleblowers Submit Tips to the SEC
2
Tip Analysis/ Investigation
3
Cases Filed/ Penalties Ordered
4
Notices of Covered Actions Posted
5
Whistleblowers File Claims
6
Review/Analysis of Claims
7
Preliminary Determinations Issued
8
Possible Record and Reconsideration Requests
9
Additional Analysis
10
Final Orders Issued/Resolution of Appeals

Number 10

Ongoing Cyber Threats to U.S. Water and Wastewater Systems

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems, and devices of U.S. Water and Wastewater Systems (WWS) Sector facilities. You may visit: https://www.cisa.gov/water-and-wastewater-systems-sector

This activity—which includes attempts to compromise system integrity via unauthorized access—threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities.

Note: although cyber threats across critical infrastructure sectors are increasing, this advisory does not intend to indicate greater targeting of the WWS Sector versus others. To secure WWS facilities—including Department of Defense (DoD) water treatment facilities in the United States and abroad—against the TTPs listed below, CISA, FBI, EPA, and NSA strongly urge organizations to implement the measures described in the Recommended Mitigations section of this advisory.

THREAT OVERVIEW
Tactics, Techniques, and Procedures

WWS facilities may be vulnerable to the following common tactics, techniques, and procedures (TTPs) used by threat actors to compromise IT and OT networks, systems, and devices.

• *Spearphishing personnel to deliver malicious payloads, including ransomware.*

o Spearphishing is one of the most prevalent techniques used for initial access to IT networks. Personnel and their potential lack of cyber awareness are a vulnerability within an organization. Personnel may open malicious attachments or links to execute malicious payloads contained in emails from threat actors that have successfully bypassed email filtering controls.

o When organizations integrate IT with OT systems, attackers can gain access—either purposefully or inadvertently—to OT assets after the IT network has been compromised through spearphishing and other techniques.

o Exploitation of internet-connected services and applications that enable remote access to WWS networks.

o For example, threat actors can exploit a Remote Desktop Protocol (RDP) that is insecurely connected to the internet to infect a network with ransomware. If the RDP is used for process control equipment, the attacker could also compromise WWS operations. Note: the increased use of remote operations due to the COVID-19 pandemic has likely increased the prevalence of weaknesses associated with remote access.

• *Exploitation of unsupported or outdated operating systems and software.*

o Threat actors likely seek to take advantage of perceived weaknesses among organizations that either do not have—or choose not to prioritize—resources for IT/OT infrastructure modernization. WWS facilities tend to allocate resources to physical infrastructure in need of replacement or repair (e.g., pipes) rather than IT/OT infrastructure.

o The fact that WWS facilities are inconsistently resourced municipal systems—not all of which have the resources to employ consistently high cybersecurity standards—may contribute to the use of unsupported or outdated operating systems and software.

• *Exploitation of control system devices with vulnerable firmware versions.*

o WWS systems commonly use outdated control system devices or firmware versions, which expose WWS networks to publicly accessible and remotely executable vulnerabilities. Successful compromise of these devices may lead to loss of system control, denial of service, or loss of sensitive data.

WWS Sector Cyber Intrusions

Cyber intrusions targeting U.S. WWS facilities highlight vulnerabilities associated with the following threats:

• Insider threats from current or former employees who maintain improperly active credentials

• Ransomware attacks

WWS Sector cyber intrusions from 2019 to early 2021 include:

• In August 2021, malicious cyber actors used Ghost variant ransomware against a Californiabased WWS facility. The ransomware variant had been in the system for about a month and was discovered when three supervisory control and data acquisition (SCADA) servers displayed a ransomware message.

• In July 2021, cyber actors used remote access to introduce ZuCaNo ransomware onto a Maine-based WWS facility's wastewater SCADA computer. The treatment system was run manually until the SCADA computer was restored using local control and more frequent operator rounds.

• In March 2021, cyber actors used an unknown ransomware variant against a Nevada-based WWS facility. The ransomware affected the victim's SCADA system and backup systems. The SCADA system provides visibility and monitoring but is not a full industrial control system (ICS).

• In September 2020, personnel at a New Jersey-based WWS facility discovered potential Makop ransomware had compromised files within their system.

• In March 2019, a former employee at Kansas-based WWS facility unsuccessfully attempted to threaten drinking water safety by using his user credentials, which had not been revoked at the time of his resignation, to remotely access a facility computer.

To read more:
https://us-cert.cisa.gov/sites/default/files/publications/AA21-287A-Ongoing_Cyber_Threats_to_U.S._Water_and_Wastewater_Systems.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.

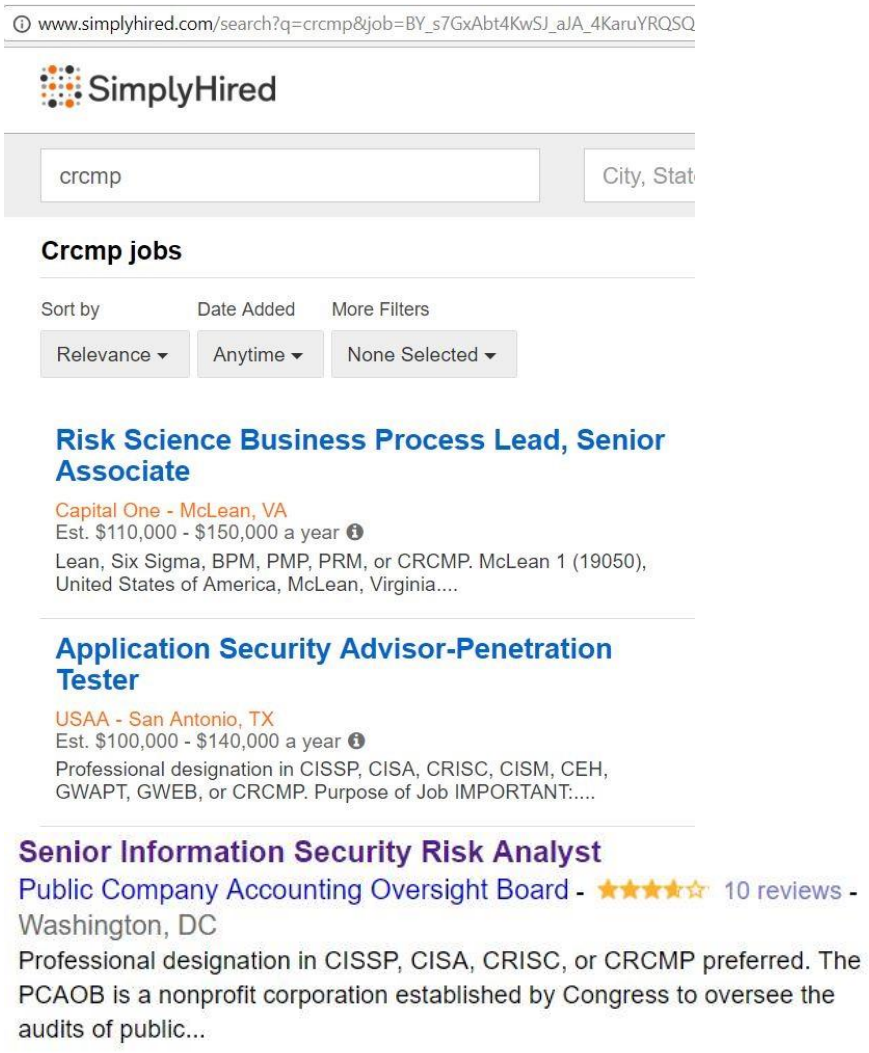
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

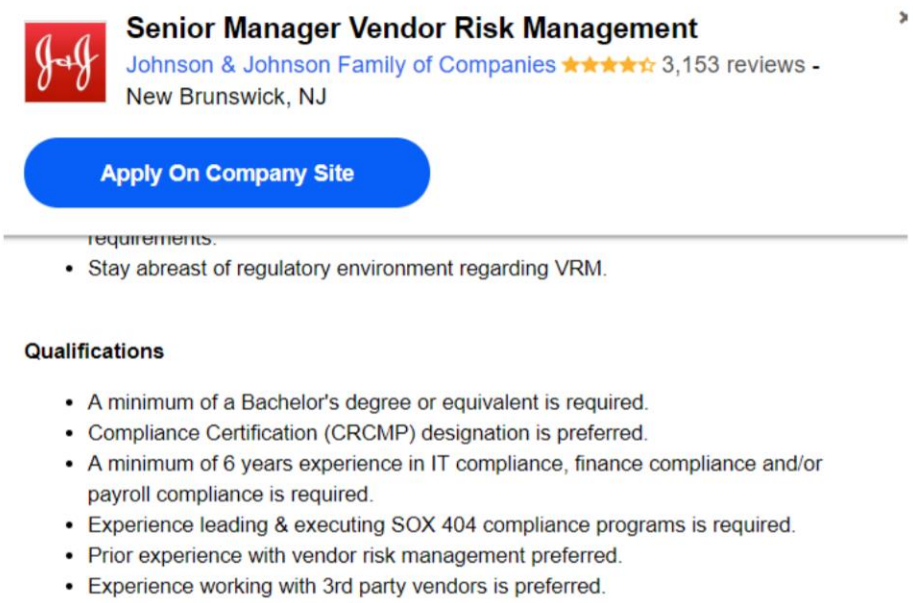
You can explore what we offer to our members:

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.