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, October 9, 2023

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,

In December 2022, Decision (EU) 2022/2481 of the European Parliament and the Council established the "Digital Decade Policy Programme 2030". Risk and compliance professionals must read the program, to understand the challenges and opportunities that come after that, and the recent developments, like the *first State of the Digital Decade* report.

In Article 1 of decision 2022/2481, we read:

"1. This Decision establishes the Digital Decade Policy Programme 2030 and sets out a monitoring and cooperation mechanism for that programme designated to:

(a) creating an environment favourable to innovation and investment by setting a clear direction for the digital transformation of the Union and for

the delivery of digital targets at Union level by 2030, on the basis of measurable indicators;

(b) structuring and stimulating cooperation between the European Parliament, the Council, the Commission and the Member States;

(c) fostering the consistency, comparability, transparency and completeness of monitoring and reporting by the Union.

2. This Decision establishes a framework for multi-country projects."

You can find Decision (EU) 2022/2481 at number 6 of our list below.

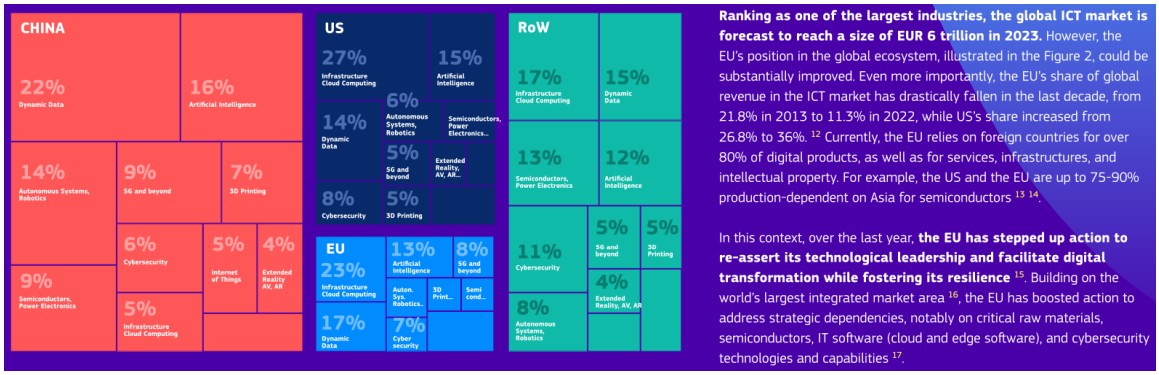
What is new?

27 September 2023 - The first State of the Digital Decade report takes stock of the EU's progress towards a successful digital transformation as set out in the Digital Decade Policy Programme 2030.

This report highlights the need to accelerate and deepen the collective efforts, including through policy measures and investment in digital technologies, skills and infrastructures.

On this basis, the report includes concrete recommendations to Member States ahead of the adoption of their national strategic roadmaps and for their future adjustments.

This report also includes the monitoring of the European Declaration on Digital Rights and Principles for the Digital Decade, which translates the EU's vision of digital transformation into principles and commitments.



Read more at number 7 below. Welcome to the Top 10 list.

Best regards,

George Lekatis

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)

Basel III Monitoring Report, September 2023

Highlights of the Basel III monitoring exercise as of 31 December 2022

Number 2 (Page 8)

Dynamic change in uncertain times, balancing opportunity and risk

Derville Rowland, Deputy Governor of the Central Bank of Ireland, at the Association for Financial Markets in Europe (AFME) 7th Annual European Compliance and Legal Conference, Brussels.

Number 3 (Page 10)

PCAOB Adopts New Standard, Modernizing Requirements for Auditors' Use of Confirmation to Better Protect Investors in Today's World

Number 4 (Page 13)

Project Mariana: BIS and central banks of France, Singapore and Switzerland successfully test cross-border wholesale CBDCs

Number 5 (Page 16)

ESAs specify criticality criteria and oversight fees for critical ICT third-party providers under DORA in response to the European Commission's call for advice

Number 6 (Page 18)

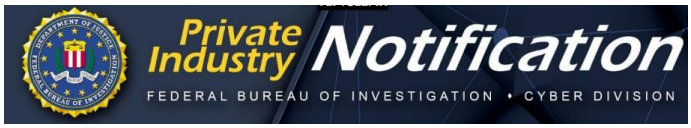
Decision (EU) 2022/2481 of the European Parliament and the Council established the "Digital Decade Policy Programme 2030".

Number 7 (Page 23)

27 September 2023 - The first State of the Digital Decade report

Number 8 (Page 25)

The U.S. Federal Bureau of Investigation (FBI) about dual ransomware attacks targeting the same victims.



Number 9 (Page 27)

BLUE OLEX 2023: Getting Ready for the Next Cybersecurity Crisis in the EU

Number 10 (Page 30)

GEN Nakasone Offers Insight into Future of Cybersecurity and SIGINT

Number 1

Basel III Monitoring Report, September 2023

BIS

Highlights of the Basel III monitoring exercise as of 31 December 2022

After their downturn at end-June 2022, initial Basel III capital ratios increase and rise above pre-pandemic levels.

Liquidity Coverage Ratio declines but remains above pre-pandemic levels

To assess the impact of the Basel III framework on banks, the Basel Committee on Banking Supervision monitors the effects and dynamics of the reforms.

For this purpose, a semiannual monitoring framework has been set up on the risk-based capital ratio, the leverage ratio and the liquidity metrics using data collected by national supervisors on a representative sample of institutions in each country.

Since the end2017 reporting date, the report also captures the effects of the Committee's finalisation of the Basel III reforms.

This report summarises the aggregate results using data as of 31 December 2022. The Committee believes that the information contained in the report will provide relevant stakeholders with a useful benchmark for analysis.

Information considered for this report was obtained by voluntary and confidential data submissions from individual banks and their national supervisors.

At the jurisdictional level, there may be mandatory data collections ongoing, which also feed into this report.

Data were included for 178 banks, including 111 large internationally active ("Group 1") banks, among them 29 G-SIBs, and 67 other ("Group 2") banks.

Members' coverage of their banking sector is very high for Group 1 banks, reaching 100% coverage for some countries, while coverage is lower for Group 2 banks and varies by country.

In general, this report does not consider any transitional arrangements such as grandfathering arrangements.

Rather, the estimates presented generally assume full implementation of the Basel III requirements based on data as of 31 December 2022.

No assumptions have been made about banks' profitability or behavioural responses, such as changes in bank capital or balance sheet composition, either since this date or in the future.

Furthermore, the report does not reflect any additional capital requirements under Pillar 2 of the Basel III framework or any higher loss absorbency requirements for domestic systemically important banks, nor does it reflect any countercyclical capital buffer requirements.

Overview of results (unbalanced data set) Table 1

	30 June 2022[1]			31 December 2022		
	Group 1	Of which: G-SIBs	Group 2	Group 1	Of which: G-SIBs	Group 2
Initial Basel III framework						
CET1 ratio (%)	12.7	12.6	16.8	13.1	13.1	16.8
Target total capital shortfalls (€ bn)[2]	0.0	0.0	0.0	0.0	0.0	0.0
TLAC shortfall 2022 minimum (€ bn)	35.1	35.1		34.4	34.4	
Total accounting assets (€ bn)	81,839.4	59,481.9	2,417.9	80,915.3	55,405.3	4,193.2
Leverage ratio (%)[3]	5.8	5.7	5.8	6.1	5.9	6.3
LCR (%)	138.2	137.5	220.0	132.0	134.2	188.4
NSFR (%)	123.5	125.2	132.3	124.4	126.7	132.2
Fully phased-in final Basel III framework (2028)						
Change in Tier 1 MRC at the target level (%)	2.8	3.2	-2.0	3.0	2.9	6.6
CET1 ratio (%)	12.5	12.5	14.3	12.7	12.8	14.7
Target capital shortfalls (€ bn); of which:	7.8	7.8	0.0	3.2	3.2	1.1
CET1	3.5	3.5	0.0	0.0	0.0	0.1
Additional Tier 1	1.9	1.9	0.0	0.0	0.0	0.4
Tier 2	2.4	2.4	0.0	3.2	3.2	0.6
TLAC shortfall 2022 minimum (€ bn)	29.8	29.8		37.4	37.4	
Leverage ratio (%)[3]	6.0	5.9	5.8	6.1	6.0	6.3

See Table A.4 for the target level capital requirements. [1] The values for the previous period may differ slightly from those published in the end-December 2021 report at the time of its release. This is caused by data resubmissions for previous periods to improve the underlying data quality and enlarge the time series sample. [2] Uses the 2017 definition of the leverage ratio exposure measure. [3] The leverage ratios reflect temporary exclusions from leverage exposures introduced in some jurisdictions.

To read more: https://www.bis.org/bcbs/publ/d554.pdf

Number 2

Dynamic change in uncertain times, balancing opportunity and risk

Derville Rowland, Deputy Governor of the Central Bank of Ireland, at the Association for Financial Markets in Europe (AFME) 7th Annual European Compliance and Legal Conference, Brussels.

It's a pleasure to be with you today and my thanks to AFME for the invitation.

As a barrister by training and a regulator by profession, the theme of this year's conference – "managing legal and regulatory challenges in an ever-changing world" – strikes very close to my heart.

It was the American law professor Grant Gilmore who said: "Law is not static but dynamic. It changes as society changes, both forever in an equilibrium precarious and unstable."

As it is brought into being through law-making, the same can be said for financial regulation. It too evolves - in ways subtle and striking – with the times.

But, it's the latter part of Gilmore's quote – when he speaks of the precarious and unstable equilibrium - that feels especially pertinent right now.

The tectonic plates shifted massively in recent years, and continue to do so. The pandemic, and all that entailed. The Russian invasion of Ukraine, reigniting war on our continent. The acceleration of the devastating effects of climate change. The human suffering, the societal impact, and the economic consequences.

In Jackson Hole last month, Christine Lagarde outlined how we are facing a deepening geopolitical divide and a global economy that is fragmenting into competing blocs. This is being accompanied by rising levels of protectionism as countries align with new strategic goals.

This is coupled with an inflationary shock, the end of quantitative easing and "low for long", and a new era of elevated volatility, higher bank funding

and credit risk, and associated vulnerabilities for markets, businesses and consumers.

For good measure, add the fact that the financial system is changing at pace, both propelled and disrupted by continuing innovation in a tech sector now entering the age of AI.

Our world is increasingly complex, feels increasingly unpredictable, and yet – as regulators and industry professionals alike – it behoves us to respond.

Not just to stay up – but, in so far as possible, to stay ahead.

So how do we manage that?

The answer is by being dynamic ourselves – in evolving our markets, our organisations, our services, our standards. But such dynamism must, necessarily, balance the desire for speed with the need for caution. Seizing the opportunity while mitigating the risk for both the system overall and for consumers and investors within it.

To put it another way, it is about a renewal - without impairing resilience – of the financial system itself, and of the frameworks to protect consumers and investors.

To illustrate, I'll set out the Central Bank's view of how firms should handle such change across a number of related areas – investor protection, governance and accountability, and countering the risk of financial crime.

To read more:
https://www.centralbank.ie/news-media/press-releases/dynamic-change-in-uncertain-times--balancing-opportunity-and-risk--remarks-by-derville-rowland--deputy-governor-consumer-and-investor-protection

Number 3

PCAOB Adopts New Standard, Modernizing Requirements for Auditors' Use of Confirmation to Better Protect Investors in Today's World

New standard replaces outdated interim standard, enhances procedures including strengthening an auditor's approach to identify fraud

The Public Company Accounting Oversight Board (PCAOB) adopted a new standard to strengthen and modernize the requirements for the auditor's use of confirmation – *the process that involves verifying information about one or more financial statement assertions with a third party.*

The new standard reflects changes in technology, communications, and business practices since the interim standard was first adopted by the PCAOB in 2003 after being issued by the AICPA in 1991.

The updated standard will better protect investors by strengthening procedures that enhance an auditor's ability to identify fraud in certain circumstances and improving overall audit quality.

"The new standard will help auditors detect fraud and better protect investors. By replacing a confirmation standard that had not changed significantly since faxes were a regular form of communication, the Board has taken an important step in modernizing our standards to effectively protect investors in today's world," said PCAOB Chair Erica Y. Williams.

"The Board thanks the many commenters whose thoughtful input helped to shape this new standard on the auditor's use of confirmation, and we look forward to monitoring the new standard's implementation and impact."

Key Provisions of the New Standard

Touching nearly every audit, the confirmation process involves an auditor selecting one or more items to be confirmed, sending a confirmation request directly to a confirming party (e.g., a financial institution), evaluating the information received, and addressing nonresponses and incomplete responses to obtain audit evidence about one or more financial statement assertions.

The new standard establishes principles-based requirements designed to stay relevant as technology evolves by applying to all methods of

confirmation, including electronic and paper-based communications. In addition, the new standard better integrates with the PCAOB's risk assessment standards. Among its key provisions, the new standard:

- Includes a new requirement regarding confirming cash and cash equivalents held by third parties or otherwise obtaining relevant and reliable audit evidence by directly accessing information maintained by a knowledgeable external source;

- Carries forward the existing requirement regarding confirming accounts receivable, while addressing situations where it is not feasible for the auditor to perform confirmation procedures or otherwise obtain relevant and reliable audit evidence for accounts receivable by directly accessing information maintained by a knowledgeable external source;

- States that the use of negative confirmation requests alone does not provide sufficient appropriate audit evidence;

- Emphasizes the auditor's responsibility to maintain control over the confirmation process and provides that the auditor is responsible for selecting the items to be confirmed, sending confirmation requests, and receiving confirmation responses; and

- Identifies situations in which alternative procedures should be performed by the auditor.

The adoption of the new confirmation standard was informed by input from an extensive notice-and-comment process, including issuance of a concept release and two proposing releases.

Information on the history of this project, including historical documents and comments received, can be found in Rulemaking Docket 028 and the related Standard-Setting Project page at:

https://pcaobus.org/oversight/standards/standard-setting-research-projects/confirmations

The new standard will apply to all audits conducted under PCAOB standards.

Subject to approval by the Securities and Exchange Commission, the new standard will take effect for audits of financial statements for fiscal years ending on or after **June 15, 2025.**

To read more:
https://assets.pcaobus.org/pcaob-dev/docs/default-source/rulemaking/docket_028/2023-008_confirmation-adopting-release.pdf?sfvrsn=e18cef74_2

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

The Auditor's Use of Confirmation, and Other Amendments to PCAOB Standards

PCAOB Release No. 2023-008
September 28, 2023

PCAOB Rulemaking
Docket Matter No. 028

Number 4

Project Mariana: BIS and central banks of France, Singapore and Switzerland successfully test cross-border wholesale CBDCs

BIS Innovation Hub

Foreign exchange (FX) is the largest financial market in the world, trading about $7.5 trillion a day (BIS (2022b)).

It operates 24 hours a day, five and a half days a week.

Project Mariana looks to the future and envisions a world in which central banks have issued central bank digital currencies (CBDCs) and explores how foreign exchange (FX) trading and settlement might look.

Mariana borrows ideas and concepts from decentralised finance (DeFi) and studies whether so-called automated market-makers (AMMs) can simplify FX trading and settlement with a view to enhancing market efficiency and reducing settlement risk.

Project Mariana is a proof of concept (PoC) for a global interbank market for spot FX featuring both an AMM and wholesale CBDCs (wCBDCs).

In the PoC, wCBDCs circulate on domestic platforms and so-called bridges allow them to be moved on to a transnational network that hosts the AMM.

Project Mariana extends previous experimentation on cross-border settlement using wCBDC arrangements and distributed ledger technology.

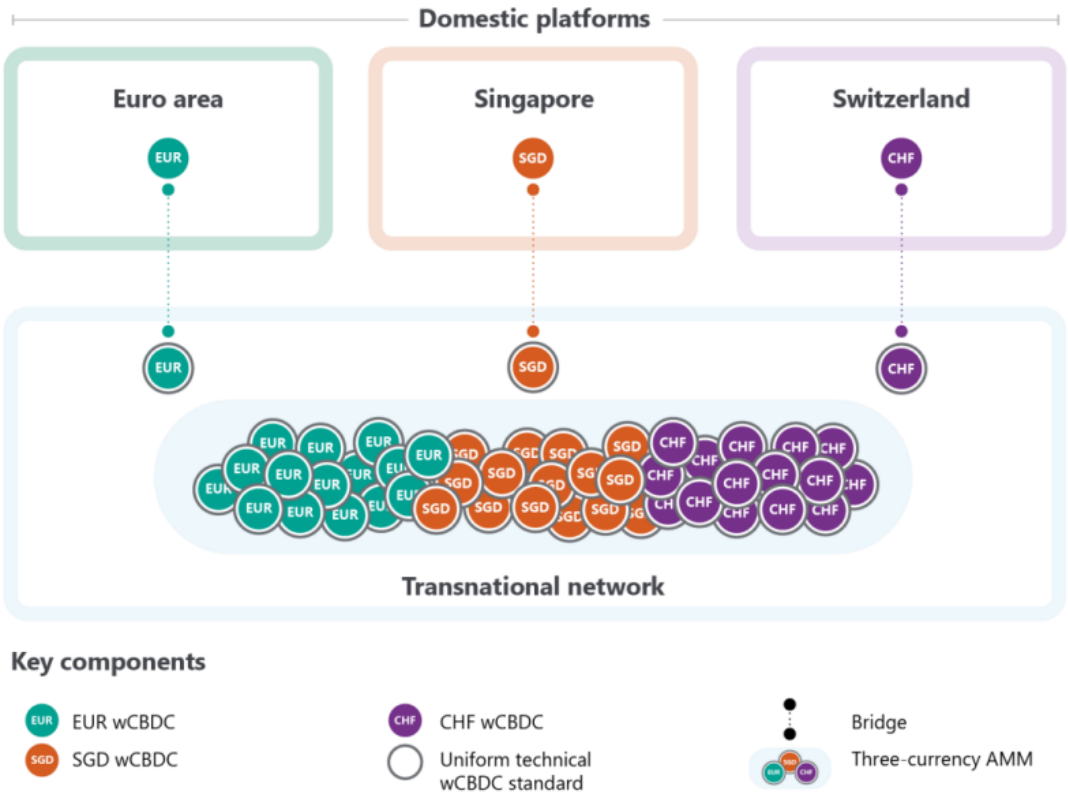
It successfully demonstrates the technical feasibility of the proposed architecture and adds novel insights on the potential of tokenisation in three dimensions.

First, wCBDCs are implemented as smart contracts, enabling central banks to manage their wCBDC without the need to directly operate or control the underlying platform.

Their design followed best practices from the public blockchain space, building on a widely used standard (ie ERC-20), as well as enabling upgradeability.

Second, bridges may serve as a mechanism to enable broader interoperability in an emerging tokenised ecosystem.

Mariana high-level architecture Graph 1



As implemented in the PoC, they may enable the seamless and safe transfer of wCBDC between domestic platforms and the transnational network without manual intervention.

The bridge design features controls and safeguards and ensures resilience through on-chain (ie bridge smart contracts) and off-chain (ie communication between bridge smart contracts) infrastructure managed by central banks.

Third, the AMM, as tested and calibrated in Mariana, fulfilled requirements based on selected FX Global Code (FXGC) principles. It delivers the contours of a possible future tokenised FX market that has a number of potential benefits.

These include supporting simple and automated execution of FX transactions, providing options to broaden the range of currencies, eliminating settlement risk and enabling transparency.

However, the use of AMMs requires the pre-funding of liquidity and their adoption would therefore entail a significant departure from the ex post funding (deferred net settlement) in use in today's FX markets.

To learn more: https://www.bis.org/publ/othp75.pdf

Project Mariana

Cross-border exchange of wholesale CBDCs using automated market-makers

Final report

September 2023

BANQUE DE FRANCE
EUROSYSTÈME

MAS
Monetary Authority of Singapore

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

Number 5

ESAs specify criticality criteria and oversight fees for critical ICT third-party providers under DORA in response to the European Commission's call for advice

The European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) published their joint response to the European Commission's Call for Advice on two EC delegated acts under the Digital Operational Resilience Act (DORA) specifying further criteria for critical ICT third-party service providers (CTPPs) and determining oversight fees levied on such providers.

In relation to the criticality criteria, the ESAs propose 11 quantitative and qualitative indicators along with the necessary information to build up and interpret such indicators following a two-step approach.

The ESAs also put forward minimum relevance thresholds for quantitative indicators, where possible and applicable, to be used as starting points in the assessment process to designate critical third-party providers.

This joint response does not include any details of the designation procedure nor of the related methodology as these are out of the scope of this Call for Advice.

However, the ESAs plan to define these details no later than six months after the adoption of the delegated act by the Commission.

Regarding the oversight fees, the ESAs make proposals for determining the amount of the fees to be levied on CTPPs and the way in which they are to be paid.

The ESAs' proposals cover the types of estimated expenditures (for both the ESAs and the competent authorities) that shall be covered by oversight fees as well as the basis for the expenditures' calculation and the available information for determining the applicable turnover of the CTPPs (the basis of fee calculation) and the method of fee calculation together with other practical issues regarding the collection of fees.

In addition, the advice proposes a financial contribution for voluntary opt-in requests. The ESAs will specify other practical aspects on the estimation of oversight expenditures and operational aspects in the context of the implementation of the oversight framework.

Background

In December 2022, the Commission issued to the ESAs a Call for Advice (CfA) in relation to two delegated acts under DORA to:

1) specify further criteria for critical ICT third-party service providers, and

2) determine the fees levied on such providers.

To inform the responses, the ESAs held a public consultation (May-June 2023). In light of the 41 responses received from various stakeholders, the ESAs have amended the draft advice on the criticality criteria to increase the role of critical or important functions in the assessment and further streamlined the proposed set of indicators.

Regarding the oversight fees, the ESAs have, among others, adapted their advice by proposing to define the scope of the applicable turnover on a narrower basis.

Overall, market participants expressed support to the proposals related to the other aspects of the advice, while requesting clarifications on some other points.

To read more:
https://www.eiopa.europa.eu/esas-specify-criticality-criteria-and-oversight-fees-critical-ict-third-party-providers-under-dora-2023-09-29_en

Number 6

Decision (EU) 2022/2481 of the European Parliament and the Council established the "Digital Decade Policy Programme 2030".

EUR-Lex
Access to European Union law

(1) In its communication of 9 March 2021 entitled '2030 Digital Compass: the European way for the Digital Decade' (the 'Digital Compass Communication') the Commission laid out its vision for 2030 to empower citizens and businesses through digital transformation (the 'Digital Decade').

The Union's path to the digital transformation of the economy and society should encompass digital sovereignty in an open manner, respect for fundamental rights, the rule of law and democracy, inclusion, accessibility, equality, sustainability, resilience, security, improving quality of life, the availability of services and respect for citizens' rights and aspirations. It should contribute to a dynamic, resource-efficient, and fair economy and society in the Union.

(2) The digital transformation is not possible without strong support for science, research, development and the scientific community, which are the driving forces of the technological and digital revolution.

Moreover, since the degree of digitalisation of the economy or society is a critical underpinning of economic and societal resilience as well as a factor in their global influence, it is necessary for the Union's international action to structure the broad range of existing cooperation in line with the pillars of the Digital Decade.

The need for such structuring is also reflected in the joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 1 December 2021 entitled 'The Global Gateway', through which the Union intends to contribute to narrowing the global investment gap, based on a democratic, value-driven approach, fostering high-standards and transparent partnerships in order to meet global infrastructure development needs.

(3) In a statement of 25 March 2021, the members of the European Council considered the Digital Compass Communication to be a step towards charting the Union's digital development for the next decade and confirmed the vision set out in the Digital Compass Communication, including the idea of a policy programme with an efficient governance framework to

facilitate the implementation of multi-country projects that are necessary for the Union's digital transformation in critical areas.

They also invited the Commission to widen the Union's policy toolbox for the digital transformation, at both Union and national level, and to use all available instruments from industrial, trade and competition policy, skills and education, research and innovation policy and long-term funding instruments to facilitate the digital transformation.

Article 3, General objectives of the Digital Decade Policy Programme 2030

1. The European Parliament, the Council, the Commission and the Member States shall cooperate to support and achieve the following general objectives at Union level (the 'general objectives'):

(a) promoting a human-centred, fundamental-rights-based, inclusive, transparent and open digital environment where secure and interoperable digital technologies and services observe and enhance Union principles, rights and values and are accessible to all, everywhere in the Union;

(b) reinforcing Member States' collective resilience and bridging the digital divide, achieving gender and geographic balance by promoting continuous opportunities for all individuals, developing basic and advanced digital skills and competencies, including through vocational and professional training, and lifelong learning, and fostering the development of high-performing digital capacities within horizontal education and training systems;

(c) ensuring the Union's digital sovereignty in an open manner, in particular by secure and accessible digital and data infrastructures capable of efficiently storing, transmitting and processing vast volumes of data that enable other technological developments, supporting the competitiveness and sustainability of the Union's industry and economy, in particular of SMEs, and the resilience of the Union's value chains, as well as fostering the start-up ecosystem and the smooth functioning of the European digital innovation hubs;

(d) promoting the deployment and the use of digital capabilities with a view to reducing the geographical digital divide and granting access to digital technologies and data on open, accessible and fair terms, in order to achieve a high level of digital intensity and innovation in Union enterprises, in particular start-ups and SMEs;

(e) developing a comprehensive and sustainable ecosystem of interoperable digital infrastructures, where high performance, edge, cloud, quantum

computing, artificial intelligence, data management and network connectivity work in convergence, to promote their uptake by businesses in the Union, and to create opportunities for growth and jobs through research, development and innovation, and ensuring that the Union has a competitive, secure and sustainable data cloud infrastructure in place, with high security and privacy standards and complying with the Union data protection rules;

(f) promoting a Union digital regulatory environment to support the ability of Union undertakings, especially that of SMEs, to compete fairly along global value chains;

(g) ensuring that online participation in democratic life is possible for everyone, and that public services, health and care services are also accessible in a trusted and secure online environment for everyone, in particular for disadvantaged groups including persons with disabilities, and in rural and remote areas, offering inclusive, efficient, interoperable and personalised services and tools with high security and privacy standards;

(h) ensuring that digital infrastructure and technologies, including their supply chains, become more sustainable, resilient, and energy- and resource-efficient, with a view to minimising their negative environmental and social impact, and contributing to a sustainable circular and climate-neutral economy and society in line with the European Green Deal, including by promoting research and innovation which contribute to that end and by developing methodologies for measuring the energy and resource efficiency of the digital space;

(i) facilitating fair and non-discriminatory conditions for users during the digital transformation throughout the Union by strengthening the synergies between private and public investments and the use of Union and national funds, and by developing predictable regulatory and supportive approaches that also involve the regional and local levels;

(j) ensuring that all policies and programmes which are relevant to achieving the digital targets set out in Article 4 are taken into account in a coordinated and coherent way to fully contribute to the European green and digital transition, while avoiding overlaps and minimising administrative burdens;

(k) improving resilience to cyberattacks, contributing to increasing risk-awareness and the knowledge of cybersecurity processes, and increasing the efforts of public and private organisations to achieve at least basic levels of cybersecurity.

2. In cooperating to achieve the general objectives set out in this Article, the Member States and the Commission shall take account of the digital principles and rights set out in the European Declaration on Digital Rights and Principles for the Digital Decade.

Article 4, Digital targets

1. The European Parliament, the Council, the Commission and the Member States shall cooperate with a view to achieving the following digital targets in the Union by 2030 (the 'digital targets'):

(1) a digitally skilled population and highly skilled digital professionals, with the aim of achieving gender balance, where:

(a) at least 80 % of those aged 16-74 have at least basic digital skills;

(b) at least 20 million ICT specialists are employed within the Union, while promoting the access of women to this field and increasing the number of ICT graduates;

(2) secure, resilient, performant and sustainable digital infrastructures, where:

(a) all end users at a fixed location are covered by a gigabit network up to the network termination point, and all populated areas are covered by next-generation wireless high-speed networks with performance at least equivalent to that of 5G, in accordance with the principle of technological neutrality;

(b) the production, in accordance with Union law on environmental sustainability, of cutting-edge semiconductors in the Union is at least 20 % of world production in value;

(c) at least 10 000 climate-neutral highly secure edge nodes are deployed in the Union, distributed in a way that guarantees access to data services with low latency (i.e. a few milliseconds) wherever businesses are located;

(d) the Union has, by 2025, its first computer with quantum acceleration, paving the way for the Union to be at the cutting edge of quantum capabilities by 2030.

(3) the digital transformation of businesses, where:

(a) at least 75 % of Union enterprises have taken up one or more of the following, in line with their business operations:

(i) cloud computing services;

(ii) big data;

(iii) artificial intelligence;

(b) more than 90 % of Union SMEs reach at least a basic level of digital intensity;

(c) the Union facilitates the growth of its innovative scale-ups and improves their access to finance, leading to at least doubling the number of unicorns;

(4) the digitalisation of public services, where:

(a) there is 100 % online accessible provision of key public services and, where relevant, it is possible for citizens and businesses in the Union to interact online with public administrations;

(b) 100 % of Union citizens have access to their electronic health records;

(c) 100 % of Union citizens have access to secure electronic identification (eID) means that are recognised throughout the Union, enabling them to have full control over identity transactions and shared personal data.

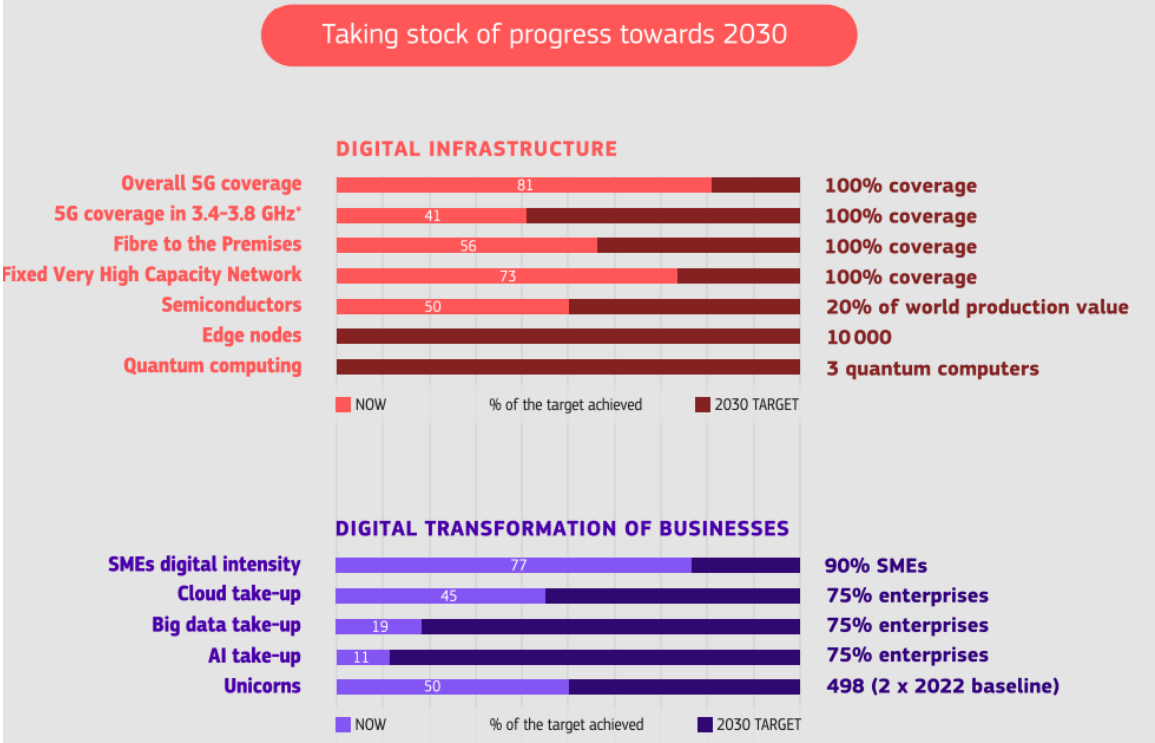
2. The Commission, taking into account in particular the information submitted by Member States in accordance with Article 5(2) and Articles 7, 8 and 9, shall review the digital targets and the relevant definitions by 30 June 2026. The Commission shall submit a report to the European Parliament and to the Council regarding the outcome of the review, and shall submit a legislative proposal to amend the digital targets where it considers it to be necessary to address technical, economic or societal developments in order to achieve a successful digital transformation of the Union.

To read more:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022D2481

Number 7

27 September 2023 - The first State of the Digital Decade report

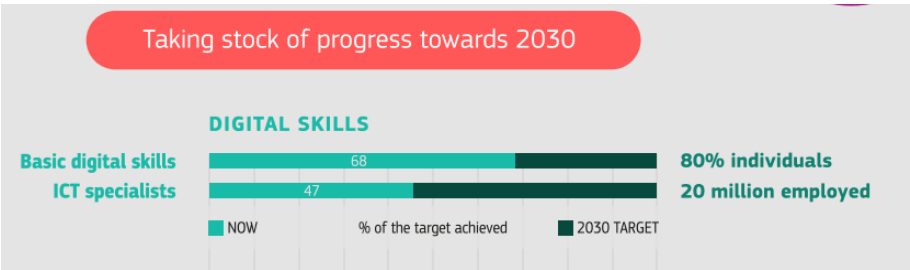
1. Introduction: Delivering the Digital Decade



The first State of the Digital Decade report takes stock of the EU's progress towards a successful digital transformation for people, businesses, and the environment as set out in the Decision establishing the Digital Decade Policy Programme 2030 ("the Digital Decade Decision").

It reviews digital policy developments and describes how the EU is advancing towards the agreed targets and objectives, thus outlining where the EU stands at the outset of the implementation of the Digital Decade Policy Programme.

The overall analysis of the EU's progress against the Digital Decade objectives and targets is shown in Figure 1 and the country reports presented in an annex to this report provide a more detailed picture.



3.3 DIGITAL DECADE OBJECTIVE: CYBERSECURITY

The global cyber threat landscape continues to be volatile, with a rise in cyberthreats of 150% in a year [69], in particular distributed denial of service (DDoS) attacks and an estimated 280 ransomware incidents attacks per month [70]. During 2021, 22.2% of EU enterprises experienced an ICT security-related incident leading to unavailability, destruction or corruption of data, or the disclosure of confidential data [71]. Increased dependencies and the development of new technologies, such as quantum computing and AI, add complexity to the threat landscape and introduce new risks for which further preparedness is needed.

While cybersecurity is not included as a target for 2030, improving resilience to cyberattacks, contributing to increasing risk-awareness and the knowledge of cybersecurity processes, and increasing the efforts of public and private organisations to achieve at least basic levels of cybersecurity is one of the general objectives set out in the Digital Decade Decision [72]. Moreover, the Digital Decade Decision points to the development of a possible specific target as part of its review planned in 2026 [73].

To read more:
https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

Number 8

The U.S. Federal Bureau of Investigation (FBI) about dual ransomware attacks targeting the same victims.

Ransomware attacks against the same victim occurring within 10 days, or less, of each other were considered dual ransomware attacks. The majority of dual ransomware attacks occurred within 48 hours of each other.

Summary

The Federal Bureau of Investigation (FBI) is releasing this Private Industry Notification to highlight emerging ransomware trends and encourage organizations to implement the recommendations in the "Mitigations" section to reduce the likelihood and impact of ransomware incidents.

Threat

As of July 2023, the FBI noted two trends emerging across the ransomware environment and is releasing this notification for industry awareness. These new trends included multiple ransomware attacks on the same victim in close date proximity and new data destruction tactics in ransomware attacks.

The FBI noted a trend of dual ransomware attacks conducted in close proximity to one another.

During these attacks, cyber threat actors deployed two different ransomware variants against victim companies from the following variants: AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum, and Royal. Variants were deployed in various combinations.

This use of dual ransomware variants resulted in a combination of data encryption, exfiltration, and financial losses from ransom payments.

Second ransomware attacks against an already compromised system could significantly harm victim entities.

In early 2022, multiple ransomware groups increased use of custom data theft, wiper tools, and malware to pressure victims to negotiate.
In some cases, new code was added to known data theft tools to prevent detection.

In other cases in 2022, malware containing data wipers remained dormant until a set time, then executed to corrupt data in alternating intervals.

Preparing for Cyber Incidents

1. Maintain offline backups of data, and regularly maintain backup and restoration. By instituting this practice, the organization ensures they will not be severely interrupted, and that backup data will be accessible when it is needed.

2. Ensure all backup data is encrypted, immutable (that is, cannot be altered or deleted), and covers the entire organization's data infrastructure. Ensure your backup data is not already infected.

3. Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.

4. Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established security policy.

5. Document and monitor external remote connections. Organizations should document approved solutions for remote management and maintenance, and immediately investigate if an unapproved solution is installed on a workstation.

6. Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (that is, a hard drive, other storage device, or the cloud).

To read more: https://www.ic3.gov/Media/News/2023/230928.pdf

Number 9

BLUE OLEX 2023: Getting Ready for the Next Cybersecurity Crisis in the EU

Together with the European Commission under the Spanish Presidency of the EU Council, the European Union Agency for Cybersecurity (ENISA) co-organised and co-hosted the Blue Olex table-top cyber exercise in the Hague, Netherlands.

With the upcoming EU elections and cyber threats spreading widely, the EU needs to strengthen its capacities. This was precisely the objective of the Blue Olex exercise to test the preparedness of the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe), the cooperation network for Member States national authorities in charge of cyber crisis management.

Launched in 2020, the EU CyCLONe network was formally established by the NIS 2 directive on 16 January 2023.

Roberto Viola, Director General for Communications Networks, Content and Technology (CNECT): ”Cyber crises have no borders and the EU must continue strengthening its capacities especially when it comes to cyber crisis management. I am pleased that the EU-CyCLONe, combining EU and Member States capabilities is testing its resilience and how to act in the case of cyberattacks and large-scale cyber incidents. A stronger cyber response makes the EU a safer continent.”

Juhan Lepassaar, Executive Director of the European Union Agency for Cybersecurity (ENISA) said: “The EU CyCLONe is an invaluable asset. Only a stronger cyber crisis coordination will allow us to best mitigate future large-scale incidents and cross-border crises in the EU.”

The Chair of the EU-CyCLONe Network (Spain) said: "Crisis management has been a priority for Spain for years. I would like to remember that the origin of CyCLONe was set up in our country, with the celebration of a Seminar in 2019 in Madrid on Large scale cyber incidents and crisis. The first conclusion was the need to set up an Exercise (BlueOlex) to develop the operational layer.

These exercise series allow to test EU preparedness in the event of a cyber-related crisis affecting the EU Member States for strengthening the

cooperation between all relevant actors. Since then, CyCLONe has been maturing in its procedures, tools, mechanisms and capabilities, managing to lay its legal foundations in the NIS 2 Directive. The 2023 BlueOlex edition, has again showed us the strong commitment that all Member States, European Commission and ENISA have against threats and challenges that, for sure, we will face in a near future to guarantee a more cyber secure and resilient Europe."

What is the objective of the EU CyCLONe?

The network collaborates and develops information sharing and situational awareness based on the support and tools provided by ENISA, also acting as the CyCLONe Secretariat. The network is chaired in turns by a representative from the Presidency of the Council of the EU.

Formed by the representatives of Member States' cyber crisis management authorities, the EU CyCLONe intervenes together with the European Commission in case of large-scale cybersecurity incidents likely to have a significant impact on services and activities falling into the scope of the NIS2 Directive.

About Blue Olex '23

BlueOlex '23 tested the EU preparedness in the event of a cyber-related crisis affecting the EU Member States and to strengthen the cooperation between the national cybersecurity authorities, the European Commission and ENISA.

The aim of the exercise is to build a stronger relationship among the cybersecurity community participating in the exercise, increase the situational awareness and share best practices.

Finally, it sets the scene for a high-level political discussion, on strategic cyber policy issues, in particular, shaping a coherent framework for crisis management at EU level.

This edition of the exercise gathered high level executives of the 27 Members States' competent authorities in charge of cyber crisis management and/or cyber policy, the European Commission and the EU Agency for Cybersecurity.

It was the opportunity for them to exercise the interaction between the new network and the EU political level and to strengthen trust and collaboration that is key for joint response.

Cyber Exercises

ENISA also supports the organisation of exercises for EU CyCLONe members, such as CySOPex (played by officers) and as in this case BlueOLEx (played by executives).

These exercises aim to identify improvements and potential gaps in the standardised way of responding to incidents and crises (i.e. Standard Operating Procedures), train on situational awareness and information sharing processes. EU CyCLONe Members also participated in Cyber Europe 2022 and are gearing up for CySOPex 2023 and Cyber Europe 2024.

To read more:
https://www.enisa.europa.eu/news/blue-olex-2023-getting-ready-for-the-next-cybersecurity-crisis-in-the-eu

Number 10

GEN Nakasone Offers Insight into Future of Cybersecurity and SIGINT

GEN Paul M. Nakasone, Commander of U.S. Cyber Command (USCYBERCOM), Director of NSA, and Chief of the Central Security Service (CSS), offered insight into what the future of cybersecurity and signals intelligence may look like during a conference in Washington earlier this month.

Looking to the future, GEN Nakasone focused on what he called "the three P's": the imminent period of intense competition with the People's Republic of China (PRC); the need for persistent engagement with public-private partners; and the critical role that the next generation of people will have in providing the United States with a competitive advantage against its adversaries.

"As we think about the future five years hence, I'm very encouraged. I am very, very optimistic," he said during a fireside chat at the annual Billington Cybersecurity Summit. "I look to the future, and I think that our Nation, obviously the folks that work here in the public and the private sector, will all be the beneficiaries."

When GEN Nakasone took the reins in 2018, he said the leading priority for the Command and Agency was securing the 2018 midterm elections. Since then, the continued rise of the PRC and Russia as global threats and the protection of critical systems and infrastructure from cyber threats have grown to become leading priorities.

"Everything that we've done since, we weren't talking about in 2018," said GEN Nakasone, who explained how cybersecurity has become synonymous with national security during his time atop USCYBERCOM and NSA/CSS.

"Now, if I would have said that in 2018, that probably would have raised a lot of eyebrows. But what have we seen since 2018? We've seen supply chain, we've seen zero days, we've seen ransomware, we've seen a number of different actors that have changed and really provided an inflection point for all of us to say, 'Hey, this is a national security issue, and we've got to treat it differently.'"

The Challenge of Artificial Intelligence

At the Billington Cybersecurity Summit, GEN Nakasone revealed the blueprint for AI and machine learning that the Command and Agency will lean on moving forward.

"Much in the sense that the private sector has been doing artificial intelligence for quite a while, we've been doing it for a long time, as well. It's something that we're familiar with," GEN Nakasone said. "We use artificial intelligence primarily with our signals intelligence mission. Now, how do we look at it for our cybersecurity mission? How do we look at it differently for our cybersecurity mission?"

"As we look at the future, we do see tremendous changes. We see the speed, coupled with the security, and coupled with the safeguards that we will ensure are put in place," he added, pointing to how Congress has also tasked USCYBERCOM with developing a five-year plan for AI. ". This is something that we will continue to work at very, very hard going into the future."

The Importance of FISA Section 702 Reauthorization

Leaning on quantitative and qualitative metrics and bolstered by declassified examples, GEN Nakasone took advantage of his participation in the fireside chat to highlight one of the Intelligence Community's most critical foreign intelligence authorities: Section 702 of the Foreign Intelligence Surveillance Act (FISA).

According to GEN Nakasone, FISA Section 702 is an authority that ensures national security and the protection of civil liberties and privacy.

"Of the things that we look at today, 702 reauthorization is among the most important national security issues I think our Nation faces," GEN Nakasone said at the conference.

Among the metrics the Director shared was that FISA Section 702 contributes to 100% of NSA's reporting on the President's intelligence requirements. He noted that in 2022, 59% of the President's Daily Brief articles contained 702 information reported by NSA, and 20% of all NSA's reporting includes 702 acquired information.

GEN Nakasone also highlighted how FISA Section 702 provided insights into the Chinese origins of precursor chemicals key to the production of fentanyl — a drug responsible for more than 100,000 deaths in the U.S. last year. The authority also enabled the U.S. to recover the majority of the

ransom from the Colonial Pipeline attack in 2021, and played a key role in the 2022 takedown of al-Qa'ida leader Ayman al-Zawahiri, according to GEN Nakasone.

"It's an authority that has saved lives and assured the protection of our homeland," he said.

To read more:
https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3533425/gen-nakasone-offers-insight-into-future-of-cybersecurity-and-sigint/

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

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

International Association of Risk and Compliance Professionals (IARCP)

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,

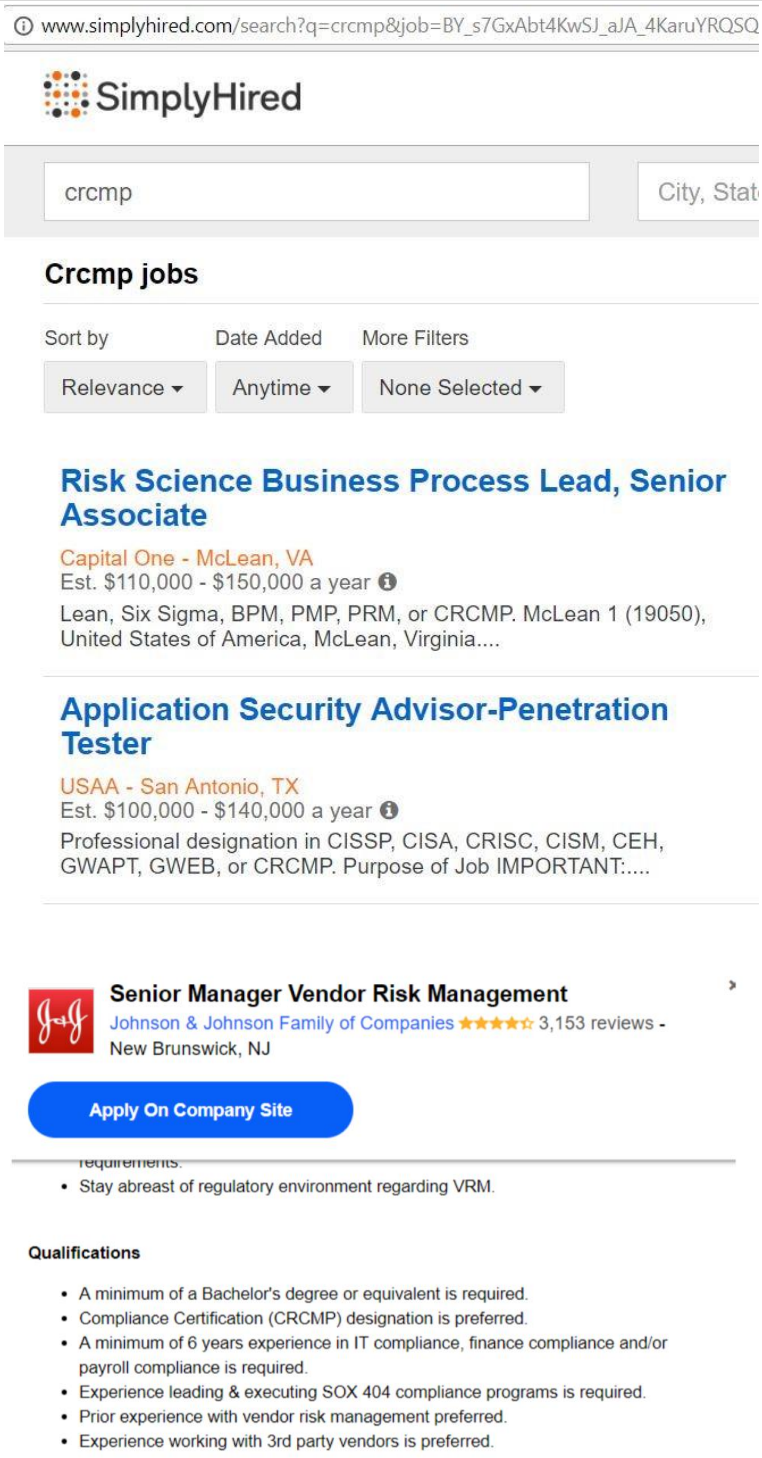
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



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 the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program ($148 instead of $297).

You have a $100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for $297, and then purchase the CISRCP program for $197 (instead of $297), the CC(GRC)P program for $197 (instead of $297), the CRCMP(Re)I program for $197 (instead of $297), and the TSecTPro program for $197 (instead of $297).

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