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, March 21, 2022

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,

I have read again the "Strengthening American Cybersecurity Act of 2022". There are some very important parts, including new offensive cybersecurity tools.

For example, the new *Joint Ransomware Task Force* will prioritize intelligence-driven operations to disrupt specific ransomware actors, and to disrupt ransomware criminal actors, associated infrastructure, and their finances.

SEC. 206. RANSOMWARE THREAT MITIGATION ACTIVITIES.

(a) Joint Ransomware Task Force.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of the Federal Bureau of Investigation,

shall establish and chair the *Joint Ransomware Task Force* to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating Federal agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Joint Ransomware Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of *after-action reports and other lessons learned* from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the Joint Ransomware Task Force to mitigate the threat of ransomware attacks.

The “Strengthening American Cybersecurity Act of 2022” has some interesting definitions:

The term *'ransomware attack'*—

"(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

"(B) does not include any such event where the demand for payment is—

"(i) not genuine; or

"(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.

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

Best regards,

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

Number 1 (Page 6)

S.3600 - Strengthening American Cybersecurity Act of 2022
117th Congress (2021-2022)

CONGRESS.GOV

Number 2 (Page 9)

U.S. Government Accountability Office
Internet Architecture is Considered Resilient, but Federal Agencies Continue to Address Risks

GAO

Number 3 (Page 14)

A global Europe to meet global financial stability challenges
Klaas Knot, Chair, Financial Stability Board and President, De Nederlandsche Bank - The Eurofi High Level Seminar 2022, Paris, France

Number 4 (Page 17)

Recollections on financial stability
Sir Jon Cunliffe, Deputy Governor for Financial Stability of the Bank of England, at The Oxford Union, Oxford

Number 5 (Page 20)

Cross-border regulatory spillovers and macroprudential policy coordination
Pierre-Richard Agénor, Timothy P Jackson and Luiz A Pereira da Silva, Monetary and Economic Department, March 2022

BIS

Number 6 (Page 22)

Data Centre Security: Guidance for owners and users

CPNI
Centre for the Protection of National Infrastructure

Number 7 (Page 27)

Zero trust becoming the default cyber security posture, but it needs to be done correctly

National Cyber Security Centre

Number 8 (Page 29)

Swiss Financial Market Supervisory Authority (FINMA)

FINMA to implement countercyclical capital buffer

finma

Number 9 (Page 31)

NSA Details Network Infrastructure Best Practices

Number 10 (Page 34)

Developing Algorithms that Make Decisions Aligned with Human Experts

New effort seeks to build trusted AI decision-makers for scenarios where ground truth doesn't exist

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

S.3600 - Strengthening American Cybersecurity Act of 2022
117th Congress (2021-2022)

CONGRESS.GOV

117TH CONGRESS
2D SESSION

S. 3600

AN ACT

To improve the cybersecurity of the Federal Government, and for other purposes.

TITLE II—CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

TITLE III—FEDERAL SECURE CLOUD IMPROVEMENT AND JOBS ACT OF 2022

The bill also updates current federal cybersecurity laws to improve coordination between federal agencies, as well as requires all federal civilian agencies to report all substantial cyberattacks to CISA.

In addition, the bill would provide new authorities to CISA and authorize the Federal Risk and Authorization Management Program (FedRAMP) for five years to ensure federal agencies can quickly and securely adopt cloud-based technologies that improve government efficiency and save taxpayer dollars.

An interesting section:

SEC. 114. IMPLEMENTING ZERO TRUST ARCHITECTURE.

(a) Guidance.—Not later than 18 months after the date of enactment of this Act, the Director shall provide an update to the appropriate congressional committees on progress in increasing the internal defenses of agency systems, including—

(1) shifting away from “trusted networks” to implement security controls based on a presumption of compromise;

(2) implementing principles of least privilege in administering information security programs;

(3) limiting the ability of entities that cause incidents to move laterally through or between agency systems;

(4) identifying incidents quickly;

(5) isolating and removing unauthorized entities from agency systems as quickly as practicable, accounting for intelligence or law enforcement purposes;

(6) otherwise increasing the resource costs for entities that cause incidents to be successful; and

(7) a summary of the agency progress reports required under subsection (b).

(b) Agency Progress Reports.—Not later than 270 days after the date of enactment of this Act, the head of each agency shall submit to the Director a progress report on implementing an information security program based on the presumption of compromise and least privilege principles, which shall include—

(1) a description of any steps the agency has completed, including progress toward achieving requirements issued by the Director, including the adoption of any models or reference architecture;

(2) an identification of activities that have not yet been completed and that would have the most immediate security impact; and

(3) a schedule to implement any planned activities.

The Act:
https://www.hsgac.senate.gov/imo/media/doc/BillText_PetersStrengtheningAmericanCybersecurityAct.pdf

Number 2

U.S. Government Accountability Office

Internet Architecture is Considered Resilient, but Federal Agencies Continue to Address Risks

The internet is a vast system of interconnected networks used by billions of people. Its architecture—the backbone of the internet—is owned and governed by organizations around the world. No one organization is responsible for its policy, operation, or security.

Generally, internet architecture is considered resilient, in part because of its decentralized nature. But reports we reviewed and subject matter experts have identified risks to key internet operations.

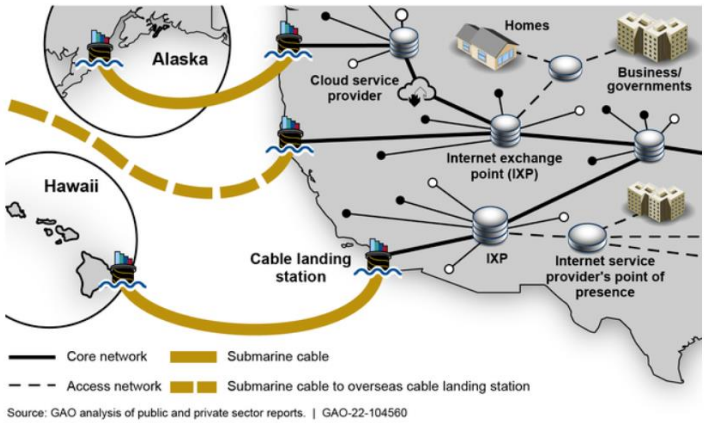
Many federal agencies are involved in addressing these risks, taking actions such as disseminating threat information and participating in global internet governance groups.

What GAO Found

The communications sector operates the multiple, independent networks that form the basis for the internet.

To support the exchange of network traffic, service providers manage and control core infrastructure elements with numerous components, including internet exchange points and submarine cable landing stations that connect to both domestic and international networks (see graphic).

How U.S. Internet Core Networks Connect to Service Providers



Source: GAO analysis of public and private sector reports. | GAO-22-104560

Multiple U.S. service providers operate distinct core networks that traverse the nation and interconnect with each other at several points.

While experts consider the internet architecture to be resilient, it nevertheless faces a variety of cyber and physical risks that can impact its components; such risks can be intentional or unintentional (see table).

Risks to Internet Architecture

Cyber intentional •Denial-of-service attacks •Border gateway protocol (BGP) abuse •Domain name system (DNS) abuse •Supply chain exploitation •Malicious insider(s)	**Cyber unintentional** •BGP failures •DNS failures •Hardware failures •Software failures •Operator error
Physical intentional •Intentional damage to fiber-optic cabling •Attack on an internet architecture facility or related infrastructure	**Physical unintentional** •Accidental damage to fiber-optic cabling •Severe natural event

Source: GAO analysis of federal and nonfederal reports. | GAO-22-104560

In particular, cyber-related risks can impact two sets of protocols needed to ensure the uniqueness of names used in internet-based services and for facilitating the routing of data packets.

Specifically, the domain name system translates names, such as www.gao.gov, to numerical addresses used by computers and other devices to route data.

Additionally, the border gateway protocol is used to exchange network availability and routing information about individual networks (i.e., destinations).

Both of these protocols are threatened by intentional abuse by malicious actors, as well as by unintentional failure.

In addition, the internet architecture can be impacted by physical risks, such as cutting or removing fiber-optic cabling.

Risks, if realized, may result in incidents that disrupt the proper functioning of the internet, including outages, degradation of performance, and interception of traffic.

Panelists serving on two panels convened by GAO also stated that the risk of intentional incidents affecting the internet architecture depends on the capabilities and motives of malicious actors.

GAO and others have reported on the threats posed by criminal groups and nation states, among others, which could potentially use their capabilities to impact components of the internet architecture.

For example, a 2017 Department of Homeland Security information technology-related risk assessment identified organized crime and nation states as threats to operations providing domain name routing services.

As the U.S. government reduced its role regarding internet architecture components, including decommissioning early networks it had developed and relinquishing its oversight role of internet technical functions, those responsibilities passed to the global multistakeholder community.

No one organization is responsible for the entirety of internet policy, operations, and security. However, the federal government fulfills a number of different roles that directly address risks to the internet architecture (see table).

Federal Roles in Infrastructure Architecture Security

Guiding Critical Infrastructure Protection and Performing Private Sector Engagement
Engaging in International Cyber Diplomacy
Supporting Cyber Research and Development
Coordinating Cyber Incident Response
Investigating and Prosecuting Cyber Criminal Activity
Developing Security Standards
Regulating Portions of the U.S. Communication Network
Addressing Supply Chain Concerns Related to Data Routing Hardware and Services
Operating Domain Name System Root Zone Servers
Issuing Licenses to Land and Operate Submarine Cables

Source: GAO analysis of federal law and policy, agency documentation, and prior GAO reports. | GAO-22-104560

To fulfill these roles, agencies have taken actions.

For example, DHS worked with members of the communications and information technology critical infrastructure sectors to, among other things, complete risk assessments on the sectors' ability to provide internet functions.

In addition, the Federal Communications Commission impacts the security of the internet architecture through licensing submarine cables and landing stations, and administering a program to remove and replace equipment determined to pose an unacceptable risk to national security.

Why GAO Did This Study

The internet is a global system of interconnected networks used by billions of people across the world to perform personal, educational, commercial, and governmental tasks.

The U.S. government over time has relinquished its oversight role of the internet. A global, multistakeholder community made up of many organizations shapes internet policy, operations, and security. But the ongoing and increasing reliance on the internet underscores the need to understand the risks to its underlying architecture.

The House Committee on Armed Services Report accompanying the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 included a provision for GAO to examine internet architecture security.

This report (1) identifies security risks related to the internet architecture and (2) determines the extent to which U.S. federal agencies have taken actions to address security risks to the internet architecture.

GAO collected and analyzed publicly available reports from federal and nonfederal organizations to identify risks to internet architecture components (internet exchange points, submarine cabling, the domain name system, and border gateway protocol, among others).

GAO also reviewed federal law and policy and its prior work to identify federal internet architecture security roles and responsible agencies. Based on the agencies' roles, GAO collected and analyzed relevant documents and conducted interviews with officials from the responsible agencies.

In addition, GAO convened two panels with subject matter experts. The panelists have experience in various aspects of the internet architecture, such as owning and operating elements of the infrastructure, participating

in and contributing to standards setting organizations, and studying and participating in various multistakeholder governance entities.

During the panel sessions, GAO presented previously identified cyber and physical risks and requested that the experts identify additional risks or concerns that were not identified. GAO and the experts also discussed federal government involvement in addressing the risks.

To read more: https://www.gao.gov/assets/gao-22-104560.pdf

United States Government Accountability Office

GAO

Report to the Committee on Armed Services, House of Representatives

March 2022

CYBERSECURITY

Internet Architecture Is Considered Resilient, but Federal Agencies Continue to Address Risks

Number 3

A global Europe to meet global financial stability challenges

Klaas Knot, Chair, Financial Stability Board and President, De Nederlandsche Bank - The Eurofi High Level Seminar 2022, Paris, France

Thank you Didier, it is great to be back. As you indicated in your kind introduction, this time I am speaking here in my capacity as Chair of the Financial Stability Board, although with a nod to my other hat, as President of De Nederlandsche Bank.

But whether you stand on top of the BIS tower in Basel - where the FSB is housed -, the Eurotower in Frankfurt, or the Toorop building in Amsterdam, the view is not fundamentally different.

In fact, many financial stability risks we face today are not only common across Europe, but are global in nature. And these global issues require global cooperation, which is why they are at the top of the FSB's agenda.

Today I want to talk about these global issues, what the FSB is doing, and how Europe can play its part.

I will be discussing these issues against the backdrop triggered by the Russian invasion of Ukraine. Developments keep evolving as I am speaking, and I do not want to engage in any speculation about what might happen.

But we need to be alert that the dramatic shift in the geopolitical landscape may also affect the functioning and resilience of the global financial system. One of the first priorities for policy makers worldwide is to navigate their economies out of the Covid pandemic.

The economic fall-out of the pandemic seems to be subsiding, and the extraordinary fiscal and monetary support measures that kept economies afloat are being gradually unwound.

But, as the economic recovery is proceeding at an uneven pace across regions, this unwinding process is increasingly likely to be asynchronous. This creates the potential for cross-border spillovers.

Moreover, since the onset of the pandemic, both public and private sector debt have increased, while asset valuations have grown amid a continued search for yield.

This has made the global financial system more vulnerable to a disorderly tightening of financial conditions. A concern that has been accentuated lately by the return of high inflation.

The job of the FSB here is to monitor and analyse developments closely and facilitate global coordination of policies, where necessary, to minimize the risk of a disorderly exit.

At the same time as we need to chart a course out of the pandemic, we need to strengthen resilience in the non-bank financial intermediation, or NBFI, sector. A sector that now represents almost half of global financial assets and is evolving rapidly.

Enhancing NBFI resilience offers significant benefits, not least during the transition to a post-Covid world.

First and foremost, it will contribute to a more stable provision of financing to the economy.

Second, it will enhance the ability of the financial system to absorb different types of shocks.

And a resilient NBFI sector reduces the need for the types of extraordinary central bank interventions we witnessed in March 2020.

The FSB is therefore working on vulnerabilities in specific NBFI areas. This includes money market funds, where we have developed policy proposals to enhance their resilience.

And it includes open-ended funds, where we are working with IOSCO to assess whether recommendations to address structural vulnerabilities are effective.

We will use the insights to develop a systemic approach to NBFI risks and policies to address them. We also need to remain vigilant to new threats to the financial system, particularly those that will have a transformational impact on our economies such as digitalisation and climate change.

Digital innovation offers opportunities for more efficient and inclusive finance, for example in global payments, but it also creates potential new risks. In particular, markets for crypto-assets are fast evolving and could

reach a point where they represent a threat to global financial stability. It is critical that we address risks in crypto-asset markets holistically and avoid fragmented policy approaches that could give rise to regulatory gaps and arbitrage.

The FSB is stepping up to the plate to deliver effective and risk-based regulatory approaches for all types of crypto-assets. We are doing so in close cooperation with standard setting bodies and national authorities.

These approaches include reviewing the High-level Recommendations for the regulation, supervision and oversight of stablecoins, undertaking further work on so-called unbacked crypto assets, and analysing the financial stability implications of the rapidly evolving decentralized finance.

Another feature of digital innovation is the ever-greater use by financial institutions of outsourcing to third-party service providers.

While this may have provided additional resilience during the pandemic, it has also reinforced the importance of effective policies for the oversight of financial institutions' reliance on critical service providers. To this can be added the greater exposure to cyber risk.

Greater interconnections in the financial system increase the surface for cyber attacks, which have escalated during the Covid pandemic. Enhancing operational and cyber resilience will therefore remain an important item on the FSB agenda.

To read more: https://www.fsb.org/wp-content/uploads/S250222.pdf

Number 4

Recollections on financial stability

Sir Jon Cunliffe, Deputy Governor for Financial Stability of the Bank of England, at The Oxford Union, Oxford

Almost exactly 25 years ago, on the day after a general election, I was handed the incoming government's surprise, detailed plan for giving the Bank of England operational independence in monetary policy making.

I was a Treasury official at the time. I was allowed to tell only a couple of colleagues and together we worked through that night and over the subsequent Bank Holiday weekend so that, three days after taking office, the new Chancellor could announce not just that he was giving the Bank monetary policy independence from that day but the key details of how the new system would work.

Over subsequent months, we prepared the necessary legislation, redrawing the functions of the Bank of England, and managed its passage through Parliament until the Bank of England Act 1998 was on the statute book.

The Act did not mention financial stability, even though the legislation transferred the Bank's responsibility for the supervision and surveillance of banks to a new authority, the Financial Services Authority.

The reforms to the Bank were focussed on the pressing issue of the time – the UK's high and volatile record on inflation.

There was, it is true, some consideration at the time of how the Bank, the Financial Services Authority and the Treasury should work together on financial stability issues.

This was codified in a memorandum of understanding between the three authorities later that year, clarifying the roles of each and setting up the so called 'Tripartite Committee' to pursue "the common objective of financial stability in the UK".

But there was no statutory backing for this objective – nor was the Bank or the Financial Services Authority given any specific powers to secure it.

The Bank did not get a financial stability objective until 2009. I should emphasise at this point that this was not some idiosyncratic UK blind-spot.

As the Global Financial Crisis was to reveal brutally, some 10 years later, the increasing integration and liberalisation of the global financial system that had been in train since the last decades of the 20th century had not been accompanied by anything like a commensurate attention to financial stability.

Warning signs were not recognised. And when the crisis struck, institutional arrangements were found sorely lacking in all of the key jurisdictions.

The depth and duration of the economic damage done by the near death of the global financial system over 10 years ago, led to a general realisation of the cost of losing financial stability and the need for greatly reinforced mechanisms to prevent it happening again.

In the UK, following the model of the monetary policy reforms ten years before, an independent committee of the Bank of England – the Financial Policy Committee (the FPC) – was established, armed with serious powers and charged with the responsibility of ensuring financial stability. And, shortly after its formal establishment, in 2013, I was appointed Deputy Governor for Financial Stability.

I have often, by the way, wondered whether this twist of fate was poetic justice for the failure of my younger self to understand the fundamental importance of financial stability back in 1997.

I have, in any event, spent the last 8 years, trying to embed and develop the domestic and international machinery to ensure we can have a vibrant and innovative financial system – but without periodic financial stability crises.

I want this evening to set out some of the key lessons over that period I have learned about financial stability – about the FPC's objectives and its scope and also to talk a little about some of the challenges it currently faces.

The objective: what are we trying to achieve?

I'll start with a question that I have been asked many times over the last 8 years: "what exactly are you trying to achieve?" It is a very reasonable and a rather awkward question.

While there are many indicators of financial activity, there is no single metric, no quantified objective for financial stability.

My answer is rooted in the human characteristic that makes financial activity – and indeed, economic growth – possible: our ability to envisage the future.

Human beings are probably unique in being able to imagine the future. I say 'probably' because there may be evidence that suggests that some animals may share, to a limited degree, our ability to engage in what has been termed 'mental time travel' – the ability we have in our minds not only to recall the past but to use past experience to form expectations of the future.

Mental time travel no doubt evolved because it gave us advantages as a species. It is fundamental to the development of economic life which is inextricably bound up with our ability to form expectations about the future and to make claims upon it.

However, though we can envisage the future, we cannot know it. Whether we form our expectations by extrapolating our memory of the past or whether they are rationally formed on the basis of all available evidence, they are expectations, no more. And when, for whatever reason, the future does not match those expectations there has to be a correction.

To read more:
https://www.bankofengland.co.uk/-/media/boe/files/speech/2022/the-state-of-financial-stability-speech-by-jon-cunliffe.pdf?la=en&hash=10A3B7B12901EAA7CDD3B2F4970FA27F97477BFB

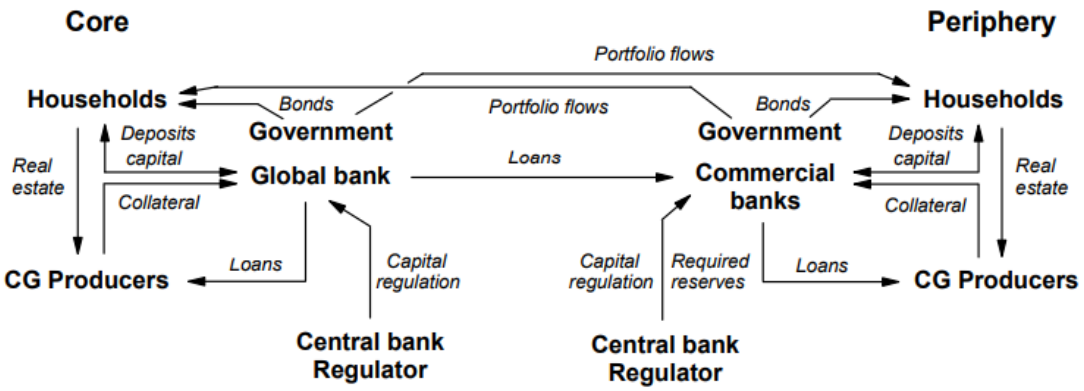
Number 5

Cross-border regulatory spillovers and macroprudential policy coordination

Pierre-Richard Agénor, Timothy P Jackson and Luiz A Pereira da Silva,
Monetary and Economic Department, March 2022

BIS

Figure 1
Core-Periphery Model with Capital Regulation



Abstract

A core-periphery model with financial frictions, imperfect financial integration, and cross-border banking is used to assess the magnitude of regulatory spillovers and the gains from international macroprudential policy coordination.

A core global bank lends to its affiliates in the periphery and banks in both regions are subject to risk-sensitive capital regulation.

Following an expansionary monetary policy in the core, a countercyclical response in capital requirements induces the global bank to engage in regulatory arbitrage.

The magnitude of the resulting cross-border capital flows depends on the degree of economies of scope in lending.

Welfare gains associated with countercyclical capital buffers are calculated for three policy regimes: independent policies (Nash), coordination, and reciprocity–a regime in which capital ratios set in the core are imposed on branches operating in the periphery.

If regulators set policies on the basis of a narrow financial stability mandate, and these policies are evaluated in terms of household welfare, reciprocity may perform better than Nash, and as well as coordination for all parties, when regulatory leakages are strong.

To read more: https://www.bis.org/publ/work1007.pdf

Number 6

Data Centre Security: Guidance for owners and users

CPNI
Centre for the Protection of National Infrastructure

This guidance has been broken up into audiences. To get started on the CPNI and the NCSC data centre guidance, decide whether you are a data centre user or a data centre owner and click on the appropriate button below.

Owners:
https://www.cpni.gov.uk/system/files/documents/a4/8d/cpnidata-centre-owners-considerations.pdf

https://www.cpni.gov.uk/data-centre-security-owners

Users:
https://www.cpni.gov.uk/system/files/documents/4b/34/cpnidata-centre-users-considerations.pdf

https://www.cpni.gov.uk/data-centre-security-users

The data hall

No matter how secure the data centre, as a customer, it is your responsibility to ensure sufficient controls are in place at the data hall to limit who might be able to access your networking equipment. If you have your own suite or hall, you need to conduct your own risk assessment and identify the security measures you need.

Meet-me rooms

Access should be strictly controlled to meet-me rooms. Meet-me room security details and assurances should be provided by data centres during tendering. As well as access control, data centre users should consider access screening processes, intrusion detection such as CCTV, rack security, and asset destruction.

People

People can become force multipliers to improve security. They can help detect, deter and disrupt hostile actors planning attacks and a good security culture can also reduce the risk of the insider threat. The data centre you select should be able to demonstrate the policies and procedures it has place to deliver good people and personnel security.

Supply chain

Securing the supply chain can be hard because vulnerabilities are inherent or introduced and exploited at any point in the chain. As a data centre user, it's important you understand the impact outsourcing can have on your data centre requirements and the risks a supplier poses to assets.

Cyber

Data centres as targets

Data centres and the data they hold are attractive targets. One of the UK's most valuable assets is its data. Together with the data centres that hold and process it, they underpin almost all facets of modern life. This makes data centres an attractive target for threat actors, due to the large and diverse amount of information that supports our national infrastructure and businesses.

The opportunities for attack are diverse. Threat actors will target vulnerabilities in data centres' ownership, geography, physical perimeter, data halls, Meet Me Rooms (MMRs), supply chains, staff, and cyber security in a concerted effort to breach data centres' defences or tamper with sensitive information or disrupt critical services.

The risks of breaches and disruption

The security and resilience of your data and the infrastructure beneath it are therefore critical. High-profile data breaches and disruption to services are frequently reported with each incident, causing operators and data owners potentially huge financial losses in regulatory fines, loss of sensitive IP, downtime, post-incident recovery, security improvements, and perhaps most valuably of all, reputation.

Cyber intrusion methodology evolves constantly, and sophisticated attackers have a strong incentive to defeat the defences you put in place. It should be assumed that at some point your defences will be breached and therefore it is also important to be able respond proactively by detecting attacks and having measures in place to minimise the impact of any cyber security incidents.

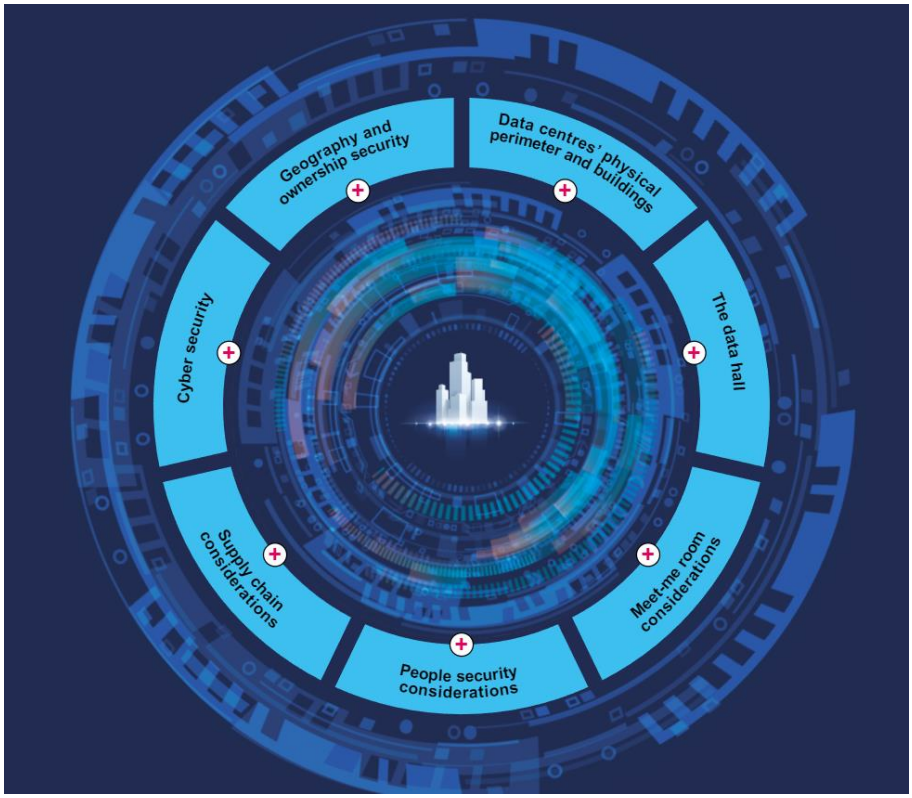
Holistic approach

To combat theses diversified threats, we need to approach data centre security holistically. By bringing together the physical, personnel and cyber security of data centres into a singular single strategy you can better withstand the diversified methods state threat actors, cyber criminals and others may use to attack them.

There is no one-size-fits-all approach to holistic data centre security. Every data centre operator and user will need to consider this guidance based on their own risk assessments. This guidance contains the security considerations you need to be aware of to make sure your data stays protected.

Guidance structure

This guidance is laid out by key areas of risk. Each of these areas should be considered when developing a risk management strategy that encourages a holistic security approach in data centres – moving from where the data centre is located, and who manages and operates it, to protecting against cyber threats. You should use this guidance to inform your own risk management strategy that is unique to your organisation's needs.



Key Types of Data Centre

There are several options for the type of data centre you may choose as a data owner.

They offer different levels of service which can impact the control you have over security arrangements.

It is important to remember that as a data owner, whichever option you choose to go with, the responsibility for managing the risks to your own information remains with you.

You should therefore understand the benefits and disadvantages of each option and use this to inform your risk management strategy.

Enterprise or 'wholly-owned' data centres

These are data centres that an organisation solely owns and operate for their own use. This gives you complete oversight of your security and operational arrangements, which often incurs higher costs.

Co-located data centres

These are centres where your organisation's data system is housed within a shared facility, along with other organisations' data.

This is often more cost effective due to the lack of upfront costs of building and running a data centre.

Whilst allowing flexibility and the ability to scale at speed, you don't have sole access to the data centre and may have fewer, or sometimes no customisable options for its security.

Managed-hosting data centres

The hybrid model – a customised data-hosting package provided by a third-party in a data centre.

The servers you use can be dedicated or shared with other customers.

This option removes the need to hire staff and places responsibility for security on the third party.

Whilst attractive from a convenience point of view, this is balanced with the fact that you have less oversight or control of your security arrangements.

Cloud-hosting data centres

Your data is stored in a network of servers across different data centres, in different locations, which increases your flexibility to scale at speed and may also improve your resilience in the case of an outage due to the distributed nature of your data.

However, you will need to be clear on how your data is stored and managed; for example, where and how your data will be moved, stored, or split while in the cloud.

Cloud service administration systems are often also highly privileged; if they are compromised, they could have a significant impact on your data.

The NCSC provides comprehensive guidance on the use of cloud services and their security.

The below table summarises the degree of control you may have over areas of risk for data centres, depending on the option you choose:

Control of aspects of a data centre	Enterprise	Co-located	Managed hosting	Cloud
Ownership	High	Medium	Medium	No
Location	High	High	Medium	Low
Data hall occupancy	High	No	No	No
Data hall operations	High	Medium	No	No
Building services operation	High	No	No	No
Facilities management	High	No	No	No
Security requirements	High	Medium	Low	Medium
Access to data centre	High	Medium	No	No
Access to your equipment	High	Medium	No	No
Staffing	High	Low	No	No
Supply chain	High	Medium	No	No
Security procedures (physical/personnel)	High	Low	No	No
Cyber security	High	Medium	No	No

To read more: https://www.cpni.gov.uk/data-centre-security

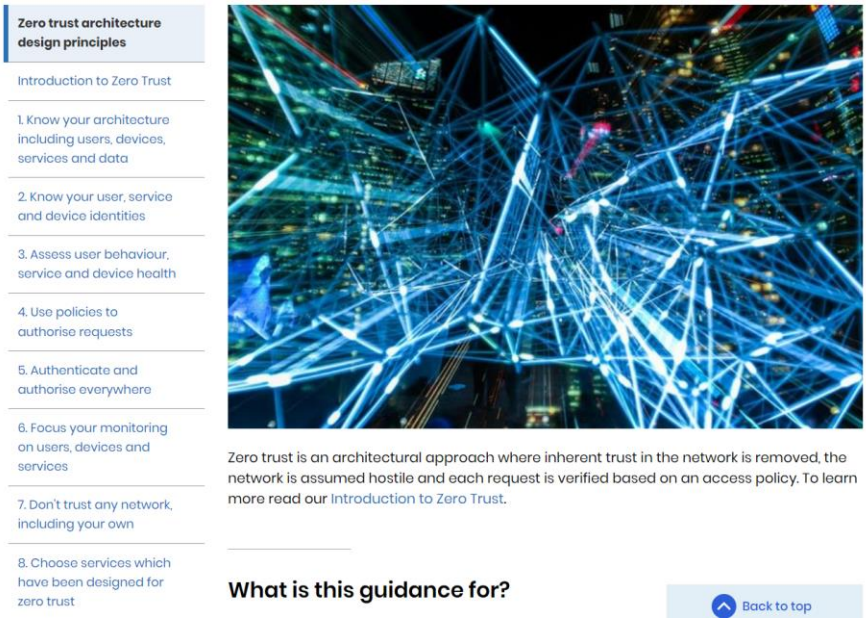
Number 7

Zero trust becoming the default cyber security posture, but it needs to be done correctly

National Cyber Security Centre

During the panel discussion at this year's Cloud and Cyber Security Expo in London, Tim Holman CEO of 2|SEC Consulting, asked the question "Given the sheer scale of attacks in businesses with zero trust, why are businesses getting zero trust wrong?".
You may visit: https://www.cloudsecurityexpo.com/

The answer, unsurprisingly, wasn't a simple one but ultimately came down to companies choosing zero trust out of necessity, often as a result of an attack. If not implemented correctly, it can often mean threats continue to occur.



The NCSC has published guidance for zero trust architecture for organisations and it's a good place to start if you're unsure whether it's the right option for you. The eight principles can help you to implement your own zero trust network architecture in an enterprise environment.
You may visit: https://www.ncsc.gov.uk/collection/zero-trust-architecture

The network is hostile

The network should be treated as compromised and therefore hostile, This means you need to remove trust from the network.

In a zero trust architecture, inherent trust is removed from the network. Just because you're connected to a network, doesn't mean you should be able to access everything on that network. Each request to access data or a service should be authenticated and authorised against an access policy. If a connection does not satisfy the access policy, the connection is dropped.

It is common in breaches to see an attacker gain a foothold on a network and then move laterally. This is possible because everything and everyone already on the network is trusted with access to the rest of the network. In a zero trust architecture, the network is treated as hostile, so every request for data or service access is continually verified against an access policy. This will also improve monitoring and detection of attempts at lateral movement by an attacker, compared to a traditional wall garden, but zero trust won't completely remove the threat.

Number 8

Swiss Financial Market Supervisory Authority (FINMA)

FINMA to implement countercyclical capital buffer

finma

The Federal Council decided on 26 January 2022 to reactivate the countercyclical capital buffer at a level of 2.5% on loans secured against residential properties in Switzerland.

The press release:
https://www.admin.ch/gov/en/start/documentation/media-releases/media-releases-federal-council.msg-id-86922.html

The banks will be given until 30 September 2022 to meet the increased capital requirements. FINMA is responsible for overseeing the implementation of the countercyclical capital buffer.

It will therefore review in the course of its ongoing supervision how the Swiss banks integrate the higher capital requirements in particular into their capital planning.

In its statement to the Swiss National Bank (SNB), FINMA recommended that the countercyclical capital buffer be reactivated and that the **maximum level of 2.5%** be applied.

This was also the SNB's view. The real estate and mortgage markets are showing clear signs of overheating for residential properties. Various factors point towards such properties being overvalued.

For example, real estate prices have risen much more sharply in the last 20 years than consumer prices or GDP. This trend has accentuated even more since the outbreak of the coronavirus pandemic, thereby further increasing the vulnerabilities on the mortgage and real estate markets in the event of a correction.

In addition, analyses carried out by FINMA show that some of the banks and also some of the insurance companies would fall far below the threshold of the capital requirements in force in the event of a severe real estate crisis and would have to be recapitalised as a result.

Jan Blöchliger, Head of the Banks division, says: "The volume of mortgages is continuing to grow. And it is even accelerating – despite the coronavirus pandemic. The institutions are taking increasingly higher risks in mortgage lending. FINMA sees risks in particular in the residential buy-to-let market.

With a volume of over CHF 1,100 billion, the Swiss mortgage market is larger than the balance sheet of a systemically important large bank. It is therefore de facto “too big to fail”. The reactivation of the countercyclical capital buffer at the level of 2.5% will increase the banks’ resilience. It is a step in the right direction for greater safety and stability of the financial system.”

Countercyclical capital buffer suspended in the context of the coronavirus crisis

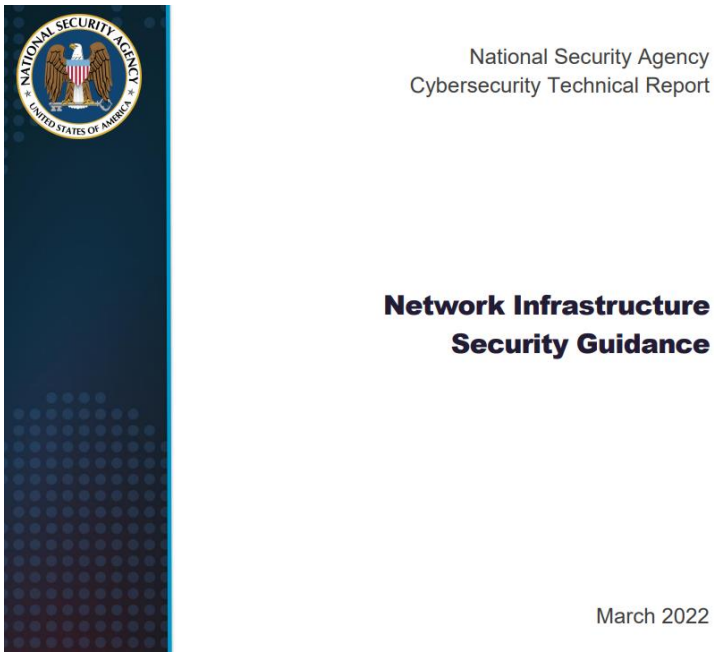
The countercyclical capital buffer was deactivated in March 2020 in light of the unfolding coronavirus crisis (see link). This took place as part of the package of measures rolled out by the Federal Council, the National Bank and FINMA. The aim was to give banks more flexibility in granting credits to companies, thus preventing a possible credit crunch.

You may visit:
https://www.finma.ch/en/news/2022/01/20220126-mm-azp/

Number 9

NSA Details Network Infrastructure Best Practices

The National Security Agency (NSA) released the "Network Infrastructure Security Guidance" Cybersecurity Technical Report. The report captures best practices based on the depth and breadth of experience in supporting customers and responding to threats.



Network environments are dynamic and evolve as new technologies, exploits, and defenses affect them. While compromise occurs and is a risk to all networks, network administrators can greatly reduce the risk of incidents as well as reduce the potential impact in the event of a compromise. This guidance focuses on the design and configurations that protect against common vulnerabilities and weaknesses on existing networks.

Recommendations include perimeter and internal network defenses to improve monitoring and access controls throughout the network.

Existing networks likely have some or most of the recommended configurations and devices noted, so administrators can use the report to help prioritize next steps in continuing to harden their network against cyber threats.

Regarding Zero Trust

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries.

The National Security Agency (NSA) fully supports the Zero Trust security model, and much of the guidance in this report can be applied at different boundaries as recommended in Zero Trust guidance.

However, this report is focused on providing guidance to mitigate common vulnerabilities and weaknesses on existing networks.

As system owners introduce new network designs intended to achieve more mature Zero Trust principles, this guidance may need to be modified.

The guidance:
https://media.defense.gov/2022/Mar/01/2002947139/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220301.PDF

Number 10

Developing Algorithms that Make Decisions Aligned with Human Experts

New effort seeks to build trusted AI decision-makers for scenarios where ground truth doesn't exist

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Military operations – from combat, to medical triage, to disaster relief – require complex and rapid decision-making in dynamic situations where there is often no single right answer.

Two seasoned military leaders facing the same scenario on the battlefield, for example, may make different tactical decisions when faced with difficult options.

As AI systems become more advanced in teaming with humans, building appropriate human trust in the AI's abilities to make sound decisions is vital.

Capturing the key characteristics underlying expert human decision - making in dynamic settings and computationally representing that data in algorithmic decision-makers may be an essential element to ensure algorithms would make trustworthy choices under difficult circumstances.

DARPA announced the In the Moment (ITM) program, which seeks to quantify the alignment of algorithms with trusted human decision-makers in difficult domains where there is no agreed upon right answer. ITM aims to evaluate and build trusted algorithmic decision-makers for mission-critical Department of Defense (DoD) operations.

"ITM is different from typical AI development approaches that require human agreement on the right outcomes," said Matt Turek, ITM program manager. "The lack of a right answer in difficult scenarios prevents us from using conventional AI evaluation techniques, which implicitly requires human agreement to create ground-truth data."

To illustrate, self-driving car algorithms can be based on ground truth for right and wrong driving responses based on traffic signs and rules of the road that don't change. One feasible approach in those scenarios is hard-coding risk values into the simulation environment used to train self-driving car algorithms.

"Baking in one-size-fits-all risk values won't work from a DoD perspective because combat situations evolve rapidly, and commander's intent changes from scenario to scenario," Turek said.

"The DoD needs rigorous, quantifiable, and scalable approaches to evaluating and building algorithmic systems for difficult decision-making where objective ground truth is unavailable. Difficult decisions are those where trusted decision-makers disagree, no right answer exists, and uncertainty, time-pressure, and conflicting values create significant decision-making challenges."

ITM is taking inspiration from the medical imaging analysis field, where techniques have been developed for evaluating systems even when skilled experts may disagree on ground truth.

For example, the boundaries of organs or pathologies can be unclear or disputed among radiologists. To overcome the lack of a true boundary, an algorithmically drawn boundary is compared to the distribution of boundaries drawn by human experts.

If the algorithm's boundary lies within the distribution of boundaries drawn by human experts over many trials, the algorithm is said to be comparable to human performance.

"Building on the medical imaging insight, ITM will develop a quantitative framework to evaluate decision-making by algorithms in very difficult domains," Turek said.

"We will create realistic, challenging decision-making scenarios that elicit responses from trusted humans to capture a distribution of key decision-maker attributes. Then we'll subject a decision-making algorithm to the same challenging scenarios and map its responses into the reference distribution to compare it to the trusted human decision-makers."

The program has four technical areas.

The first is developing decision-maker characterization techniques that identify and quantify key decision-maker attributes in difficult domains.

The second technical area is creating a quantitative alignment score between a human decision-maker and an algorithm in ways that are predictive of end-user trust.

A third technical area is responsible for designing and executing the program evaluation.

The final technical area is responsible for policy and practice integration; providing legal, moral, and ethical expertise to the program; supporting the development of future DoD policy and concepts of operations (CONOPS); overseeing development of an ethical operations process (DevEthOps); and conducting outreach events to the broader policy community.

ITM is a 3.5-year program encompassing two phases with potential for a third phase devoted to maturing the technology with a transition partner.

The first phase is 24-months long and focuses on small-unit triage as the decision-making scenario.

Phase 2 is 18-months long and increases decision-making complexity by focusing on mass-casualty events.

To evaluate the whole ITM process, multiple human and algorithmic decision-makers will be presented scenarios from the medical triage (Phase 1) or mass casualty (Phase 2) domains.

Algorithmic decision-makers will include an aligned algorithmic decision-maker with knowledge of key human decision-making attributes and a baseline algorithmic decision-maker with no knowledge of those key human attributes. A human triage professional will also be included as an experimental control.

“We’re going to collect the decisions, the responses from each of those decision-makers, and present those in a blinded fashion to multiple triage professionals,” Turek said.

“Those triage professionals won’t know whether the response comes from an aligned algorithm or a baseline algorithm or from a human. And the question that we might pose to those triage professionals is which decision-maker would they delegate to, providing us a measure of their willingness to trust those particular decision-makers.”

A virtual Proposers Day for potential proposers is scheduled for March 18, 2022. For more information and registration details, visit: https://go.usa.gov/xzjc2 A Broad Agency Announcement (BAA) solicitation is expected to available on SAM.gov in the coming weeks.

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.

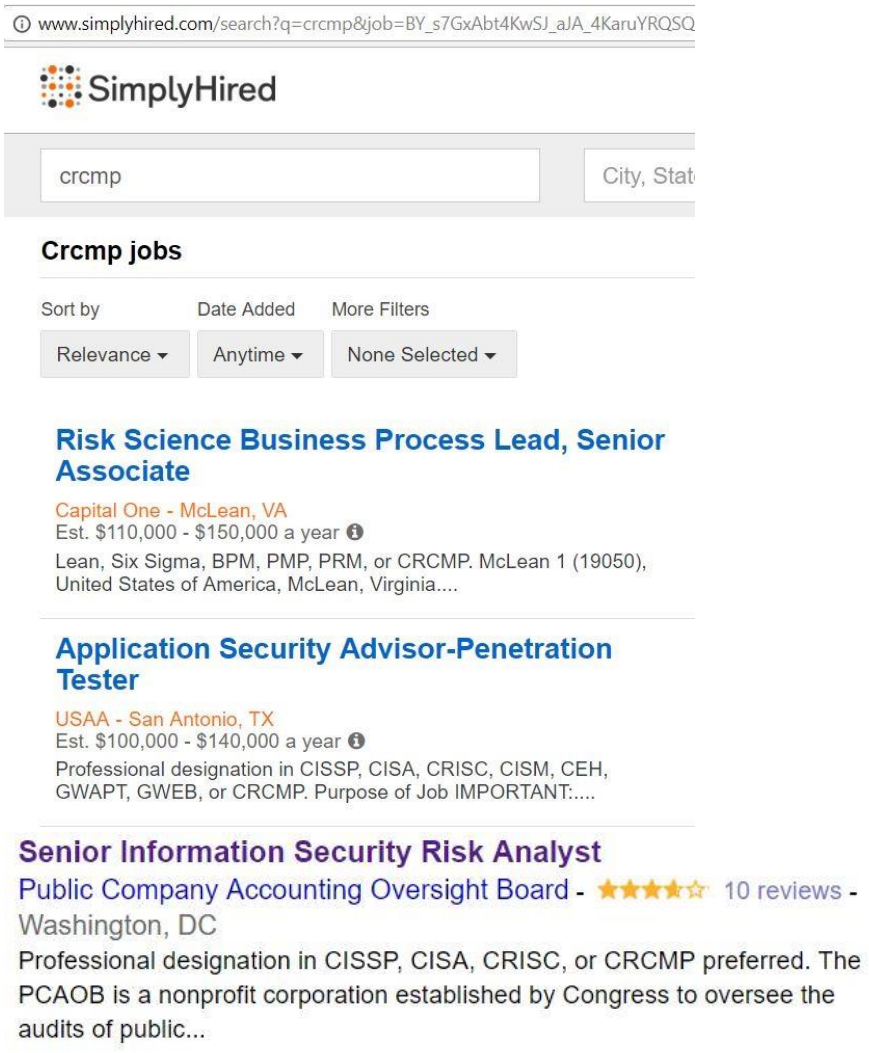
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

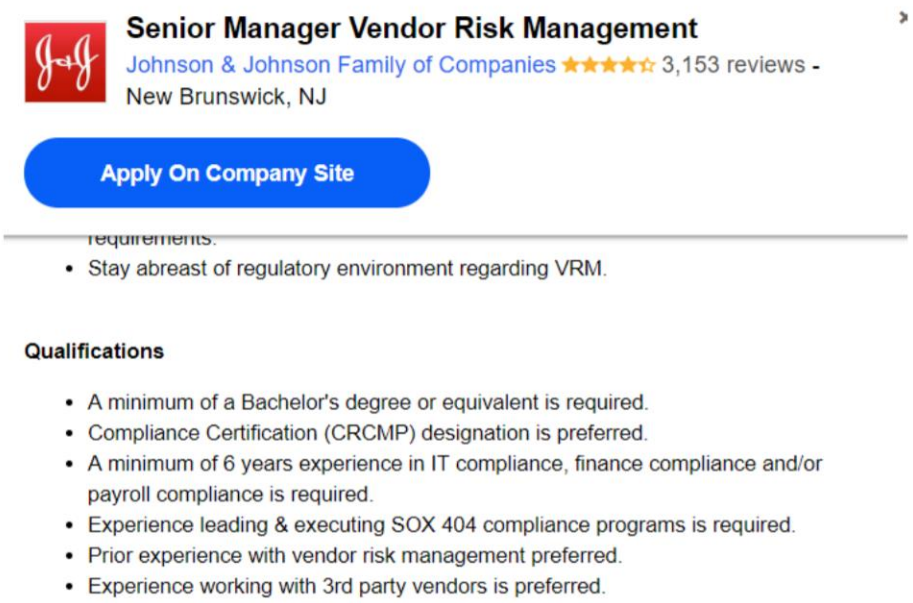
You can explore what we offer to our members:

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.

Our Reading Room:
https://www.risk-compliance-association.com/Reading_Room.htm