Review and comparison of US, EU, and UK regulations on cyber risk/security of the current Blockchain Technologies - viewpoint from 2023

Dr Petar Radanliev

Oxford e-Research Centre, Department of Engineering Sciences, University of Oxford, UK, petar.radanliev@oerc.ox.ac.uk

Abstract

The first cryptocurrency was invested in 2008/09, but the Blockchain-Web3 concept is still in its infancy, and the cyber risk is constantly changing. Our cybersecurity should also be adapting to these changes to ensure security of personal data and continuation of business for organisations. This review paper starts with a comparison of existing cybersecurity standards and regulations from the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) - ISO27001, followed by a discussion on more specific and recent standards and regulations, such as the Markets in Crypto-Assets Regulation (MiCA), Committee on Payments and Market Infrastructures and the International Organisation of Securities Commissions (CPMI-IOSCO), and more general cryptography and post-quantum cryptography, in the context of cybersecurity. These topics are followed up by a review of recent technical reports on cyber risk/security and a discussion on cloud security questions. Comparison of Blockchain cyber risk is also performed on the recent EU standards on cyber security, including European Cybersecurity Certification Scheme (EUCS) – cloud, and additional US standards – The National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS). The study includes a review of Blockchain endpoint security, and new technologies e.g., IoT. The research methodology applied is a review and case study analysing secondary data on cybersecurity. The research significance is the integration of knowledge from the United States (US), the European Union (EU), the United Kingdom (UK), and international standards and frameworks on cybersecurity that can be alighted to new Blockchain projects. The results show that cybersecurity standards are not designed in close cooperation between the two major western blocks - US and EU. In addition, while the US is still leading in this area, the security standards for cryptocurrencies, internet-of-things, and blockchain technologies have not evolved as fast as the technologies have. The key finding from this study is that although the crypto market has grown into a multi-trillion industry, the crypto market has also lost over 70% since its peak, causing significant financial loss for individuals and cooperation's. Despite this significant impact to individuals and society, cybersecurity standards and financial governance regulations are still in their infancy.

Key words: Cyber Risk Assessment; Cloud Cybersecurity Standards; Financial Governance, DeFi, NIST; ISO27001; IoT; Blockchain Technologies, Metaverse, Cryptocurrencies.

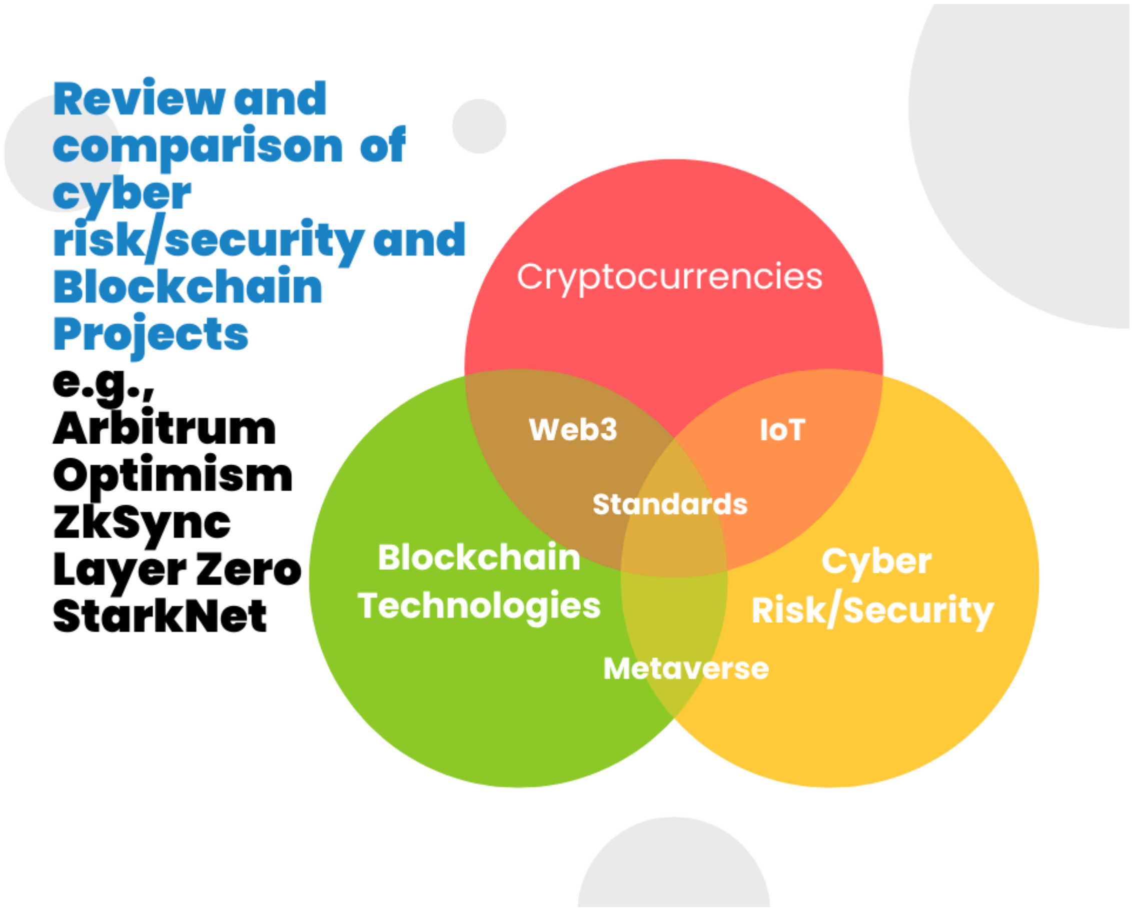


Figure 1: Graphical abstract

1. Introduction to Cybersecurity, Regulations, and Standards for new and emerging Blockchain Technologies

This article reviews the cybersecurity regulations and standards that are in existence in 2023, and derives conclusions on gaps in standards and regulations, and how these gaps can impact individuals and companies in terms of financial impact and socio-economic impact. With the emergence of new layer-2 Blockchains such as Arbitrum and Optimism, and many new layer-2 solutions expected to emerge as leaders in Blockchain projects in 2023 (e.g., ZKSync, StarkNet, Sui and Layer Zero), we can expect this technology to predominate the Web3 development. The collapse of many well-known Blockchain projects in 2022 (e.g., Terra Luna, FTX) and the recent depegging of the USD Coin (USDC) has exposed some major risk in Blockchain Technologies, even Stablecoins.

Another major concern in the increasing number of Blockchain projects, and the increased investment in these projects, despite the financial risks, is the cyber risk. In the past year, we have witnessed numerous cyber-attacks to Blockchain projects, some examples of cyber-attack breaches include:

- Ronin Network — $625 million.
- Wormhole Bridge — $325 million.
- Nomad Bridge — $190 Million.
- Beanstalk Farms — $182 million.
- Wintermute — $162 million.

The review includes aspects related to technical attacks and non-technical attacks (e.g.., social engineering, insider threats). Some of the biggest cyber threats in Blockchain Technologies in 2023 are insider threats, ransomware, and phishing/social engineering attacks. These threats can take different forms and insider threats are not always malicious. Non-malicious examples include the use of default passwords, poor data hygiene, server misconfigurations, etc. For this king of cyber threats, even the most secure cryptographic algorithm would not be very helpful, because the risk is not placed in the communication, or in the device, the risk is in the implementation of cybersecurity for the blockchain system that is secured with cryptography.

1.1. Types of cyber attacks

Even the most secure Blockchain systems, with the strongest cryptography, are vulnerable to malicious attacks when cybersecurity is badly implemented. The implementation exposes organisations to phishing attacks [1] and social engineering attacks [2]. These are also very effective tools for hackers, especially if privileged user gets phished and a hacker gets administrative access to critical systems.

Ransomware is another example of cyber threats [3], for Blockchain Technologies, and has proven very effective for cyber attackers. We can expect ransomware to continue to be heavily favourite tool for hackers, especially state sponsored hackers like the Lazarus Group.

Such attacks are extremely difficult to detect, unless the attacker trips the suspicious activity monitoring systems, or the phished user reports the event. While continuous training and cyber education is considered as the best preventative measure [4], it is easy to fall for extremely well disguised social engineering attacks [5]–[8]. Hence, cybersecurity focus needs to be placed on the TCP/IP network, and on ‘employee education, training, and awareness’ [9]. While staff training and network security can help with avoiding some of the common vulnerabilities, organisations should develop and maintain plans for delivering critical services with business resilience system integrated with artificial intelligence systems [10], [11] and anticipate that at some point, cyber-attack will create a system wide disruption, as we have witnessed in Ukraine [12].

The article is statured with an introduction, literature review, technical review, comparison, lesson learned, discussion, and a conclusion sections.

2. Review

2.1. Literature review

According to one recent study, Blockchain-based systems expose five major attack vectors, categorised as: *‘blockchain infrastructure, subsuming the P2P network, consensus mechanism, VM, and blockchain applications, including the application logic and wallets’* [13]. Another recent study found that *‘that malleability attacks, 51% attacks, and wallet security attacks are the most common attacks’* on Blockchain projects [14]. Existing standards are used to attempt to assess the risk from these new technologies, including the ‘ISO 27001 and the General Data Protection Regulations’ [15].

Although Blockchain-based systems open new attack vectors, Blockchain Technologies are also considered for cybersecurity management, some examples include to *‘to examine if a network has been compromised and to what extent’* [16], to secure the Internet-of-Things (IoT) [17], including the Industrial Internet of Things (IIoT) [18]. One emerging study presents a *'blockchain-based solutions for the cybersecurity of the main smart city applications, namely smart healthcare, smart transportation, smart agriculture, supply chain management, smart grid, and smart homes'* [19]. Multiple research studies have been published recently conducing a systematic literature review and classification of blockchain for cybersecurity [20], or a comprehensive survey of blockchain enabled cyber security [21]. However, major concerns remain on 'several vulnerabilities associated with blockchain technology' [22], with the same study reporting that some of the most frequent and common vulnerabilities on blockchain networks include:

- 51% or Majority Attack (in PoW-based blockchains like Bitcoin),
- Routine attack (double coin spent),
- BC Endpoint Vulnerabilities,
- Attacks due to vulnerability in smart-contracts and their deployment,
- Transaction Privacy Leakage, and,
- Phishing Attacks.

This study is focused on identifying solutions from existing cybersecurity standards and regulations. The next section reviews technical reports on cybersecurity that can provide insights into the Blockchain security problem.

2.2. Review of technical reports on new Cybersecurity, Regulations, and Standards for new and emerging Blockchain Technologies

To ensure coverage of the numerous technical publications on the topic of cyber risk, and to keep the volume of this review within a reasonable length, while eliminating potential bias, this section outlines how the technical papers are selected in this reviewed.

- First, Google scholar was used.
- Second, the Web of Science Core Collection was searched.
- Third, Scopus was used.
- Finally, multiple reciprocities were researched for the inclusion of missing technical papers.

To ensure state-of-the-art is presented in the review, the search for literature includes only the most prominent records (selected by number of citations and quality of journals published) and most recent studies (records from 2021 onwards). Hence, the review and the results are influenced by the most cited records - published in top technical journals. The reputation of the journal publisher was strongly considered - only reputable publishers, e.g., Springer, IEEE, Elsevier.

2.3. The MiCA Crypto-Assets Regulation

The Markets in Crypto-Assets Regulation (MiCA) [23] is a new European Union (EU) legislation designed to regulate crypto-asset-related activities carried on in the EU. The EU Parliament Committee on Economic and Monetary Affairs (ECON) endorsed the approved text for the Markets in Crypto-assets regulation (MiCA) on the 10th of October 2022. In 2022, the collapse of multiple crypto projects (e.g., FTX, Alameda Research, Terra Luna) triggered the debate on regulating the crypto markets and how we can ensure a more diligent risk management, including the management of counter-party risk between crypto market participants and projects.

MiCA divides cryptocurrencies into four categories:

1. Crypto assets that are rewarded for maintaining distributed ledger technology or validations of transactions (e.g., Bitcoin) seem like they will be exempted from MiCA, because layer one assets are seen as commodities of their systems.
2. Utility tokens that are used for exchange of goods and services seem like will also be exempted from MiCA,
3. Asset-reference tokens (ART), are money market accounts known as stable coins and although they include real government issued money (fiat money), they might also include treasury and other debt,
   and
4. Electronic money tokens (e-money or EMT), are real government issued money, pegged by the value of one type of fiat currency and used for payment processing (e.g., Wise, Revolut, Alipay, WeChat Pay)

MiCA provides:

- important rules for the crypto industry,
- market guidelines for crypto companies, requiring them to provide detailed information about their projects (e.g., if a crypto company is paying 10% yield, where are they getting that yield from),
- it mandates stable coins issues to maintain sufficient liquidity in the form of deposits to prevent crashes like Terra UST.

Regulations like MiCA might encourage big companies to get involved into crypto. The challenge for traders is that MiCA introduces a transaction value cap of 200m euros per day, for non-euro stable coins and most crypto traders trade USD not Euro. In fact, nobody trades Euros on the crypto markets. The provisional MiCA bill has caused Circle (USDC) to create the Euro Coin (EUROC). In other words, EUROC is a coin designed in collaboration with the EU regulators and USDT seems to be doing the same.

It also restricts stable coin issues on how many tokens they can issue if they are not denominated in Euros or other EU currencies.

2.4. Review of the NIST approach to cyber risk assessment

The National Institute of Standards and Technology (NIST) Cybersecurity Framework - version 1.1 [24] is considered as the most wide-ranging approach for identity management that contains description of how to manage supply chain cybersecurity (e.g., it includes third party risk, Blockchain technologies, digital currencies, and other risk categories which are not covered by ENISA and/or ISO). Version 1.1 was created in close discussion with 1,200 participants. This included annual workshops, open reviews, and the Framework remains as a *'living document'*, with regular updates constantly integrated and published – often as 'Special Publications' (SP). Since Version 1.1 was created in 2018, there has been numerous SP documents.

According to NIST, some of the **most common questions** asked by practitioners are: *'what is wrong with the way we have been doing'*, and *'why is the additional expense necessary'* [25]. **The answer** is that NIST Cybersecurity Framework *'provides a common language, regardless of if you are a CEO, or you just walked into a company as a new employee, it's something that you can feasibly grasp'*. It offers the *'ease of understanding, simplicity, in a* *very complex topic'*. It helps *'communicate risk in the way that everyone understands, from the server room to the board room'* [25].

NIST Cybersecurity Framework is organized in five categories: (1) **identify**, (2) **protect**, (3) **detect**, (4) **respond**, (5) **recover** [25]. Version 1.1 includes provisions on supply chain cybersecurity (e.g., **third party and/or participants**). The framework provides 108 subcategories, and informative references. Subcategories are **outcome oriented**, and often close ended – you can answer yes/no, and special attention has been placed on the verbs used: e.g., suppliers and third-party partners/participants of information systems, components, and services, are *identified, prioritised, and assessed, using the cyber supply chain risk assessment process'* [25]. The NIST Cybersecurity Framework is used by non-cyber experts to **translate** the meaning of documents like **ISO/IEC27001** into understandable information, like from the function **respond**, into a **category**, then **subcategory**, and finally into a technical objective. This transformative structure enables almost anyone to engage in the topic of cybersecurity. The NIST Cybersecurity Framework consists of **seven step process** – which can also be described as a gap analysis using the framework profiles:

- Step 1: **Prioritise and scope** – implementation tiers can be used to express varying risk tolerances,
- Step 2: **Orient**,
- Step 3: **Create a current profile,**
- Step 4: **Conduct a risk assessment**,
- Step 5: **Create a target profile** – used in conjunction with the implementation tiers, where the characteristic of the tier level should be reflected in the desired cybersecurity outcomes.
- Step 6: **Determine, analyse and prioritise gaps**,
- Step 7: **Implementation action plan**.

3. Comparison of existing cybersecurity standards and their relevance to Blockchain projects.

This section includes a review and comparison of existing cybersecurity standards (including NIST, ENISA, and ISO271001) with Blockchain standards (MiCA and CPMI-IOSCO) and derives new findings on the relevance of existing cybersecurity standards to Blockchain projects. The review starts with ISO, but focuses more on the NIST standards, as the NIST guidance is more comprehensive and most frequently updated – in relation to Blockchain technologies and cybersecurity.

3.1. ISO cybersecurity standards

The ISO standards are on the other hand used by many organisations that seek compliance, and the main concern with ISO 27001 standards (according to Advisera [26]) is that:

1. *ISO 27001 is it a management standard framework, not a security specific standard.*
2. *ISO 27001 provides a framework for the management of security within an organisation's but does not provide a 'how to' guide for implementing the security.*

3. *Compliance or external certification to ISO 27001 does not mean you are secure. It means that you are managing security in line with the standard, and to the risk level you think is appropriate to the organisation’s.*
4. *In conjunction with ISO 27002, it provides some guidance on the controls that we should consider. However, it does not provide detailed guidance for the organisation’s, the information that we handle, and the systems that we use.*
5. *Security expertise is required both to implement an information security risk assessment and to define the required security controls.*

While ISO standards are reviewed in this article, the value of ISO for Blockchain projects is currently limited, because Blockchain technologies are adapting and evolving at a pace that ISO cannot catch up with. ISO standards are well established and extremely detailed in areas of risk where the risk is not changing from day to day. If we consider that during the writing of this article, the Blockchain risks have already changed multiple times, it is hard to see how any standard that is based on a consensus of the entire international community, would be able to catch up with the constantly evolving Blockchain risks. In this article, we review ISO, in combination with NIST, and we also consider various less known standards, e.g., MiCA, NVD, EUCS, ENISA.

3.2. NIST 800-53 and NIST CSF

NIST 800-53 [27] is a more comprehensive and more frequently updated cybersecurity standard than the ISO 27001 [28], but NIST Cybersecurity Framework (NIST CSF) [25] is commonly confused with the NIST 800-53. NIST 800-53 is a globally recognised security standard, while NIST CSF is the most used cybersecurity framework [29]. The NIST 800-53 and NIST CSF are used in the developed and developing countries e.g., Argentina, Brazil, Chile, Colombia, and Uruguay [30]. The NIST 800-53 and NIST CSF are adopted by some of the most critical sectors, such as oil and gas [31] and medical systems [32].

3.3. NIST special publications on endpoint security

The NIST Special Publication 800-128 [33] provides a guide concentrated on implementation of the information system security aspects of configuration management, referred as: security-focused configuration management (SecCM). This standard is directly relevant to Blockchain projects, because the cryptographic security is not the main security concern for Blockchain projects in 2023, but the implementation of endpoint cybersecurity is a big concern.

3.4. NIST special publications on cryptography

The NIST Cryptographic Standards and Guidelines Development Process: (NISTiR 7977) describes the principles, processes and procedures that drive cryptographic standards and guidelines development efforts at the National Institute of Standards and Technology (NIST). Cryptography involves techniques for exchanging secure messages even in the presence of adversaries. NIST continues to lead public collaborations for developing modern cryptography, including:

Block ciphers [34], which encrypt data in block-sized chunks (rather than one bit at a time) and are useful in encrypting large amounts of data.

Cryptographic hash algorithms [35], which create short digests, or hashes, of the information being protected. These digests find use in many security applications including digital signatures, the development of which NIST also leads.

Key establishment [36], employed in public-key cryptography to establish the data protection keys used by the communicating parties.

Post-quantum cryptography [37], intended to be secure against both quantum and classical computers and deployable without drastic changes to existing communication protocols and networks.

Lightweight cryptography [38], which could be used in small devices such as Internet of Things devices and other resource-limited platforms that would be overtaxed by current cryptographic algorithms.

Privacy-enhancing cryptography [39], intended to allow research on private data without revealing aspects of the data that could be used to identify its owner.

Given the detail of these special publications, we can conclude that individual and isolated issues to cryptography – have been addressed in terms of cybersecurity in 2023. Questions remain on how the new solutions of lightweight cryptography (cryptography for low memory IoT devices), is compliant with the guidance on post-quantum cryptography. This needs to be considered by Blockchain projects operating on IoT devices (e.g., IoTA).

3.5. Cyber risk in Blockchain projects – example of Lazarus and suggestions on how to protect Blockchain projects from cyber campaigns from groups like Lazarus.

Short discussion on the North Korea-based threat actor widely known as **Lazarus**. One of their recent campaigns infected networks with a malicious implant designed to hack mobile telecommunications infrastructure (known as: 'MESSAGETAP' [40]).

For a Blockchain organisation's to be secure, we need to consider disabling unnecessary ports and services. Organisation's need to implement strong Network Detection System (NDS) and Network Prevention Systems (NPS), and have in place account use policies, multi factor authentication and password policies. Important note here is that cyber-attacks based on internal abuse of system features cannot be easily mitigated [41], [42].

Second point is detection, originations need to trace system and network events, with strong Network Intrusion Detection System that can a). monitor for process use of the network; b) monitor authentication logs for systems and applications; c) monitor for many failed authentication attempts across various accounts.

Third point is on organisation's personal preference, but as a minimum, organisation's need to create and monitor a honeypot service in a common port that the organisation's doesn't use, for example. Blockchain organisations (e.g., Arbitrum, Optimism, ZKSync, StarkNet) should create honeypot accounts. User training is also important personal preference, along with limiting credential overlap across accounts. Next generation firewalls can detect indicators in RAM, perform real-time monitoring of incoming and outgoing network traffic, and detect unwanted tasks in operations e.g., The Cisco Firepower™ Next-Generation Firewall (NGFW) [43].

Main cybersecurity problems derived from the review – root risk causes:
○ Legacy systems,

○ Default users and passwords
○ Reused accounts,
○ No password policy
○ No monitoring of privileged accounts.
Main recommendations derived from the review - to avoid cyber risk:
○ An organisation’s patch policy and enforcement of this in critical assets
○ Isolate the legacy systems
○ An organisation’s password and user policy that includes no default surnames, good password rotation, and not allow users to reuse passwords in different environments.
○ Use PAM, PUM or both to manage administrate and user accounts
○ Enforce active monitoring in critical assets

3.6. National Blockchain Cybersecurity Strategies

National efforts are placed by governments around the world to increase national capacity to *‘..withstand threats to the security of their citizens and their digital resources.’*, and such ‘cybersecurity capacity-building initiatives entail a multidimensional range of actions to address problems, ranging from awareness-raising to technological innovations.’ [44]. Cybersecurity capacity-building needs to be prioritised by national policymakers to address the global cybersecurity gaps, because ‘there are incremental differences in capacity that are tied to the wealth of nations’ [44]. This requires understanding cybersecurity behavioural habits, because *‘cybersecurity behaviours do not necessarily come naturally, and people need support and encouragement to develop and adopt them’* [45]. Habits are important factors in cybersecurity behaviours, and *‘efficacy and behavioural comprehensiveness predict cybersecurity behavioural habits’*, ‘*efficacy has a positively impact on behavioural comprehensiveness’* and *‘situational support has a positive influence on efficacy’* [45]. This means that cybersecurity behavioural habits can be formed by promoting the diversity of cybersecurity measures practiced and efficacy [45].

In the most recent EU cybersecurity strategy published in open access (from the Republic of Poland), the national cybersecurity system includes entities which cannot be subject to the provisions of the Strategy e.g., under Article 4 of the NCSA, the national cybersecurity system consists of: operators of essential services—digital service providers; CSIRT MON; CSIRT NASK; CSIRT GOV. Given such status of the ‘strategy’, it can have a direct impact on government administration authorities, but, given its legal status in relation to generally applicable law, its impact on other public authorities, entrepreneurs, and citizens is only indirect [46]. Building upon the argument from the previous paragraph, the strategy includes provisions for educational, informational, and training programmes in cybersecurity.

Bringing this into banking perspective, one of the recent technical papers reviewed is related to applying the Framework for Improving Critical Infrastructure Cybersecurity, created by NIST to a case study of a large Brazilian bank in Brazil [47]. The technical paper concluded that the category of Security Continuous Monitoring controls is more important than other cybersecurity categories. It also shows the importance of ‘applying the constructivist method for the management of cyber risks by unravelling a problem and providing a basis for decision making’. This is compliant with a recent Master thesis on ‘Banking and Cybersecurity Governance’. The Master thesis argues that *‘while the various cybersecurity frameworks are present for financial organizations to choose from, NIST is the* *current cybersecurity framework recommended.'* and that *'The research also found that there is no single cybersecurity framework that encompasses all the requirements needed for the technical infrastructure of financial service providers.'* [48].

3.7. International Blockchain Cybersecurity Strategies

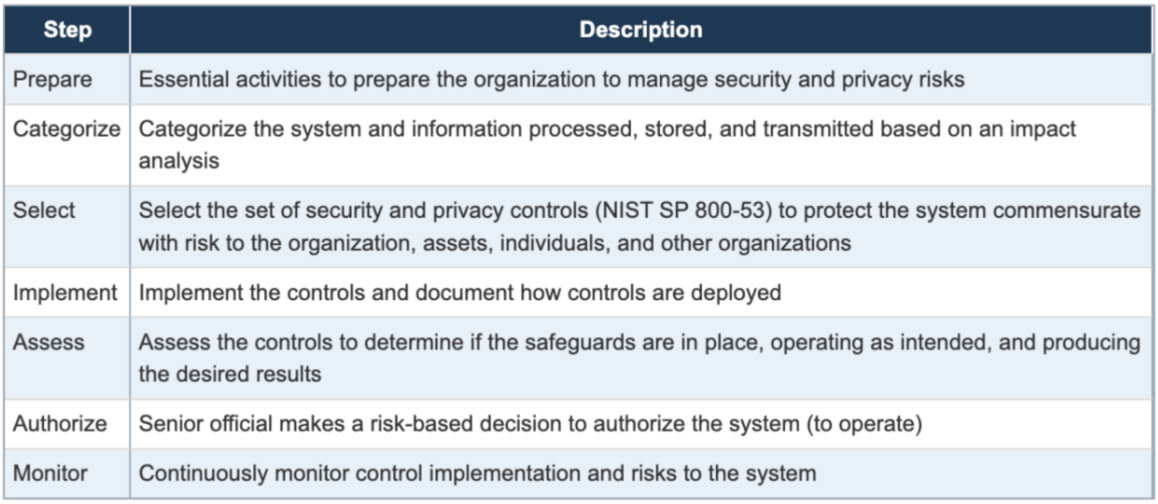
While some central banks still perceive cyber risk as financial risk, IMF has conducted a review of nine central bank cases and presented an argument that cyber risk is a non-financial risk [49]. Cyber risk is categorised as 'fintech' risk and its related to technological innovation. This view is supported by a review paper on the designs, problems, and prospects of the Central Bank Digital Currency (CBDC) in China [50]. Although most CBDC projects are still in research and development stage, there are some projects that are in advanced stages e.g., Digital renminbi (e-CNY), mobile phone-based money transfer service (M-Pesa).

The Federal Reserve recently published a report [51] on the 'Security Considerations for a Central Bank Digital Currency', in which they present four key points:

- Supporting a Resilient Payment System,
- Building Trust in a Payment Instrument,
- Protecting End User Asset and Sensitive Personal Information, and
- Preventing Reputational Harm to a Central Bank.

The report proposes a new framework for 'General Risk Management Guidance' called NIST Risk Management Framework (NIST RMF). In Table 1, we can see the basic characteristics of the new framework.

Table 1: NIST Risk Management Framework (NIST RMF)

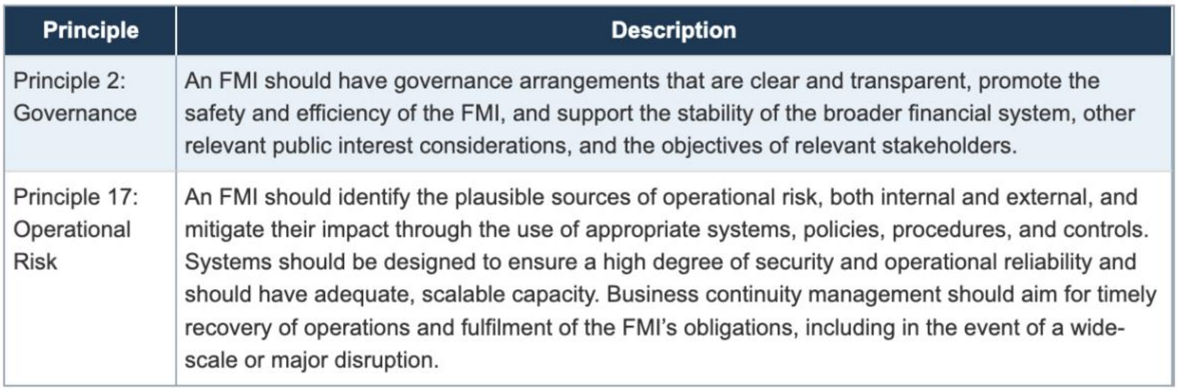


Step	Description
Prepare	Essential activities to prepare the organization to manage security and privacy risks
Categorize	Categorize the system and information processed, stored, and transmitted based on an impact analysis
Select	Select the set of security and privacy controls (NIST SP 800-53) to protect the system commensurate with risk to the organization, assets, individuals, and other organizations
Implement	Implement the controls and document how controls are deployed
Assess	Assess the controls to determine if the safeguards are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to authorize the system (to operate)
Monitor	Continuously monitor control implementation and risks to the system

As with previous NIST frameworks, the approach is built upon existing standards that include the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 Series, the Committee on Payments and Market Infrastructures and the International Organisation of Securities Commissions (IOSCO), the NIST developed the Cybersecurity Framework (NIST CSF), among other standards.

In Table 2, we can see examples of how CPMI-IOSCO principles are used.

Table 2: CPMI-IOSCO Principles 2 and 17



Principle	Description
Principle 2: Governance	An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.
Principle 17: Operational Risk	An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.

While using the NIST approach was expected, the lack of detail in this report also confirms that US is lagging behind some countries in terms of developing its own CBDC. It is possible that at the time of writing this report, the IOSCO considered the US banking systems as sufficiently advanced to integrate in the Industry 4.0 and Web3, because the payment systems are already distributed and digitalised. Maybe the IOSCO considered that the US banking systems simply do not need a digital currency given the strength of their actual currencies.

However, the Federal Reserve is still considering the potential of CBDC and although they haven't made any official decision at present, the Federal Reserve states on their main webpage that *'a CBDC would be the safest digital asset available to the general public, with no associated credit or liquidity risk'* [52]. The point made here is that the Federal Reserve is currently considering CBDC and has funded and published in open access numerous reports on a USA CBDC [53]. If this was not the case, and if a USA CBDC was not a desired approach, this point would have been rather superficial, but since they are, and there is no working USA CBDC at present, then it becomes obvious that China – with its e-CNY, is leading the innovation in the field of CBDC research and development.

3.1. ENISA Cloud security for Blockchain projects

The ENISA Cloud security risk assessments discussed in previous section, seem focused on the simplified version of the NIST CSF, and do not cover the cryptography algorithms that NIST was originally designed to develop. Since Cloud security is predominately about security of data in transit or data in storage, ENISA should focus on advancing their risk assessment with a deeper understanding of the cryptography algorithms. In the next section, we describe the most important algorithms that NIST includes in their guidance documents but are not present in the ENISA guidance documents. These special publications need to be considered by ENISA when designing the new standards and regulations for Blockchain projects.

4. Lessons for Blockchain projects from existing EU standards and regulations on cyber risk and risk assessment.

The new and emerging Blockchain projects are also addressing the cloud risk, moistly by developing decentralised blockchain based cloud solutions, but the innovation in the Blockchain cloud space is continuous and evolving. In current cloud solutions, Private cloud is frequently used in centralised financial transactions for making resources available on-demand, without moving to the public cloud. However, Private cloud still requires third party services (e.g., encryption protocols, firewalls), but theoretically, adds additional security because access is limited. However, encryption and firewalls can still be exploited by adversaries, and this risk increases with adding third party services to managed private clouds (e.g., infrastructure-as-a-service or platform-as-a-service) which can be used as a gateway for cyber-attack. In short summary, the current clous solutions can be categorised as:

- Private cloud – More system control but less scalability
- Public cloud – Less system control greater scalability
- Hybrid cloud – Deployed on private, scaled on public on demand.

While Blockchain cloud solutions offer various alternatives to centralised clouds, existing cloud providers can still benefit from the incorporation of blockchain in cloud computing. Some examples include better data security, easy traceability, improved system interoperability, decentralisation, faster system discovery. AWS and many other cloud providers are already building Blockchain technologies in their cloud solutions.

However, in terms of cloud security, according to The European Union Agency for Cybersecurity (ENISA), organisations' need ask specific questions to the supply chain participant in a cloud infrastructure, and most of these are also relevant to Blockchain projects. In other words, Blockchain projects can learn from existing cyber risk assessment standards and regulations, even if not all aspects are directly relevant, some if not most, will still be relevant. Here we include a list of questions taken from existing EU standards and regulations on cloud cyber risk and risk assessment, that can be used for risk assessing new and emerging Blockchain projects. Although the list of questions is too long to conclude in this paper, some of these questions are included below as examples:

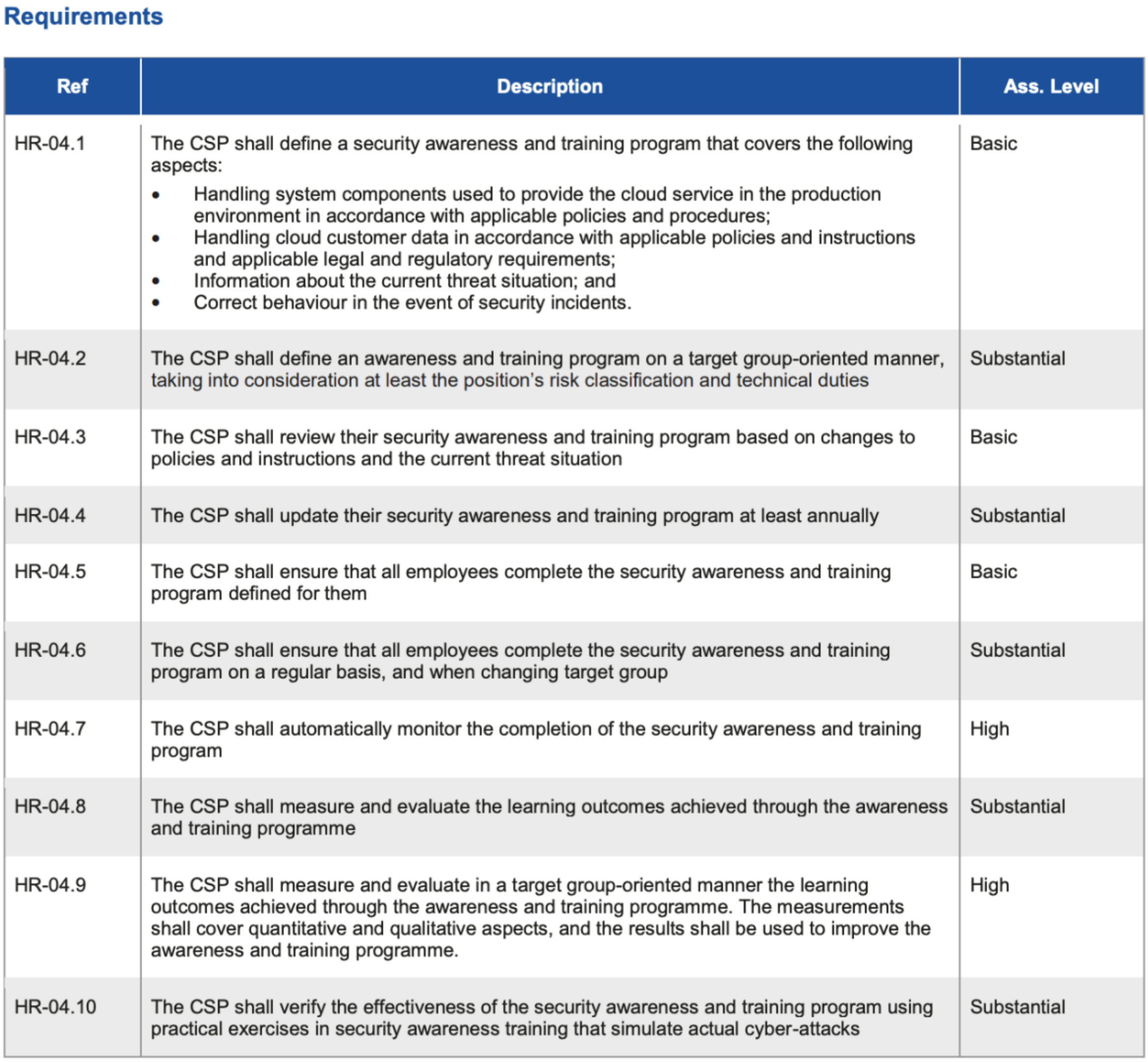
- *'Question 1: How do you check (and do they) for third party obligations already set out under the PRA SS and the EBA Guidelines on Outsourcing?'*
- *'Question 2: Do you have any cloud exposure?* If so, which cloud solution for financial transactions:
    - *platform-as-a-service;*
    - *infrastructure-as-a-service;*
    - *software-as-a-service;*
    - *multi-cloud?'*
- *'Question 3: What cloud solutions would be most beneficial for our future supply chains?*
    - *Storage*
    - *Data management*
    - *Reporting and analytics*
    - *Risk and regulatory: risk calculation, transaction surveillance, regulatory reporting: (e.g., Solvency 2)*
- *'Question 4: Do you expect any changes in operations as a result of the new Digital Operational Resilience Act (DORA)?'*

The conclusions we can draw from the format of these questions is that ENISA has worded the questions as open-ended, seeking information, not giving authorities statements on how to review cyber risk from cloud computing. Although the attempt of ENISA is to provide guidance on Cloud security for companies operating in European Union (EU), this version of the document doesn't seem to provide guidance but seek information that is needed to develop the guidance.

4.1. EU standards: EUCS – Cloud Services Scheme and Blockchain Techologies

In December 2020, the European Union agency for cybersecurity published a draft version of the EUCS candidate scheme [54] (European Cybersecurity Certification Scheme for Cloud Services), which investigates the certification of the cybersecurity of cloud services. This is a draft version to be used as basis for an external review. The objective of the review is to validate the principles and general organisations of the proposed scheme, and to gather feedback on the proposed wording of the sections and annexes. In *Table 3* we can see one of the many requirements listed in the emerging EU standard on cloud security. The *Table 3* presents a sample of the most recent framework from ENISA, and it is shown the similarities in how risk categories are structured in accordance with NIST.

Table 3: One example of EU requirements – ENISA/EUCS

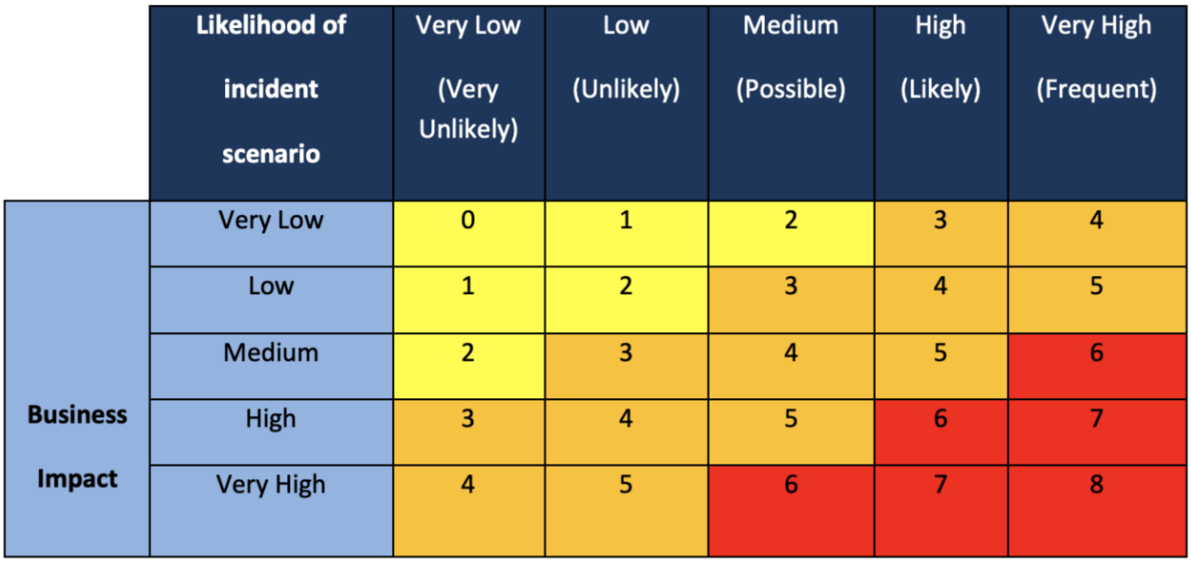


Requirements

Ref	Description	Ass. Level
HR-04.1	The CSP shall define a security awareness and training program that covers the following aspects: • Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures; • Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; • Information about the current threat situation; and • Correct behaviour in the event of security incidents.	Basic
HR-04.2	The CSP shall define an awareness and training program on a target group-oriented manner, taking into consideration at least the position's risk classification and technical duties	Substantial
HR-04.3	The CSP shall review their security awareness and training program based on changes to policies and instructions and the current threat situation	Basic
HR-04.4	The CSP shall update their security awareness and training program at least annually	Substantial
HR-04.5	The CSP shall ensure that all employees complete the security awareness and training program defined for them	Basic
HR-04.6	The CSP shall ensure that all employees complete the security awareness and training program on a regular basis, and when changing target group	Substantial
HR-04.7	The CSP shall automatically monitor the completion of the security awareness and training program	High
HR-04.8	The CSP shall measure and evaluate the learning outcomes achieved through the awareness and training programme	Substantial
HR-04.9	The CSP shall measure and evaluate in a target group-oriented manner the learning outcomes achieved through the awareness and training programme. The measurements shall cover quantitative and qualitative aspects, and the results shall be used to improve the awareness and training programme.	High
HR-04.10	The CSP shall verify the effectiveness of the security awareness and training program using practical exercises in security awareness training that simulate actual cyber-attacks	Substantial

Earlier versions of the ENISA Cloud Computing Risk Assessment (from 2009) [55] can be seen in Table 4 and Table 5.

Table 4: ENISA Cloud Computing Risk Assessment - Estimation of risk levels based on ISO/IEC 27005:2008



	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

This is an in-depth and independent analysis that outlines some of the information security benefits and key security risks of cloud computing. The report provides a set of practical recommendations. Certain organisation's migrating to the cloud have made considerable investments in achieving certification either for competitive advantage or to meet industry standards or regulatory requirements (e.g., PCI DSS).

One example of how ENISA recommends for cloud risk assessment [55] is set of 35 questions based on vulnerabilities assessment – see Table 5. ENISA builds on the work of NIST, but it has a different approach for quantifying Cloud risk – we show this in the example presented in Table 5.

Table 5: Example of the ENISA 35 questions on cloud risk - loss of governance and control

R.2 LOSS OF GOVERNANCE

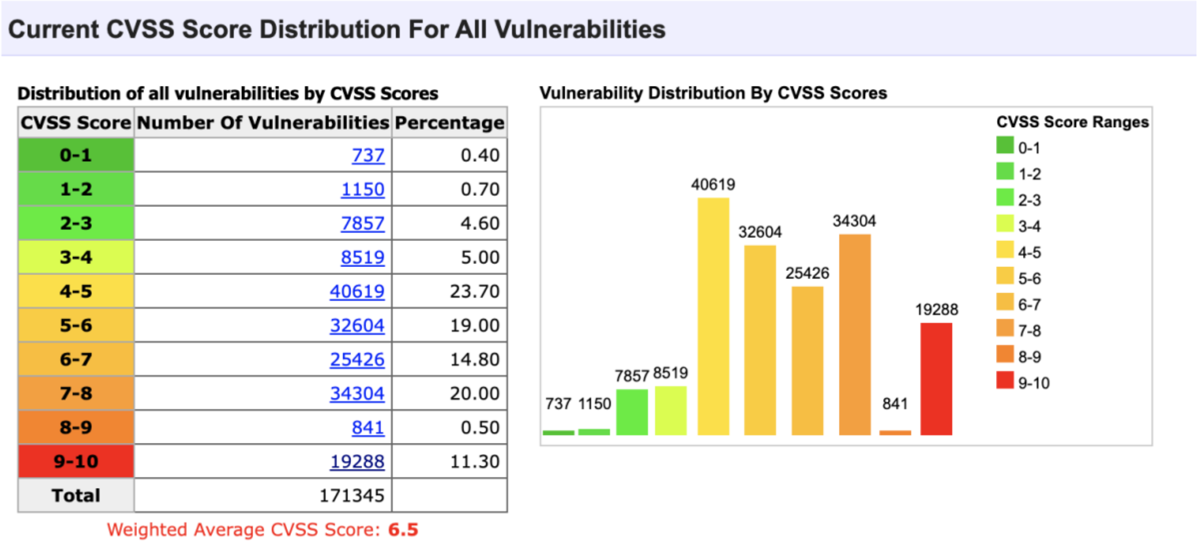
Probability	VERY HIGH	Comparative: Higher
Impact	VERY HIGH (depends on organization) (IaaS VERY HIGH, SaaS Low)	Comparative: Equal
Vulnerabilities	V34. Unclear roles and responsibilities V35. Poor enforcement of role definitions V21. Synchronizing responsibilities or contractual obligations external to cloud V23. SLA clauses with conflicting promises to different stakeholders V25. Audit or certification not available to customers V22. Cross-cloud applications creating hidden dependency V13. Lack of standard technologies and solutions V29. Storage of data in multiple jurisdictions and lack of transparency about THIS V14. No source escrow agreement V16. No control on vulnerability assessment process V26. Certification schemes not adapted to cloud infrastructures V30. Lack of information on jurisdictions V31. Lack of completeness and transparency in terms of use V44. Unclear asset ownership	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

A more comprehensive and up-to-date version for cyber risk assessment is by using the NIST vulnerability metrics, based on the national vulnerability database – see section: Product

4.2. USA standards: NVD CVSS / CVE vulnerability database

Integration using NVD CVSS Calculators [56]. Although this can be seen as a daunting task for a novice cybersecurity practitioner, the security community has created a ‘Current CVSS Score Distribution for All Vulnerabilities’ - see CVE [57] visualised in Table 6.

Table 6: Current CVSS Score Distribution for All Vulnerabilities



Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

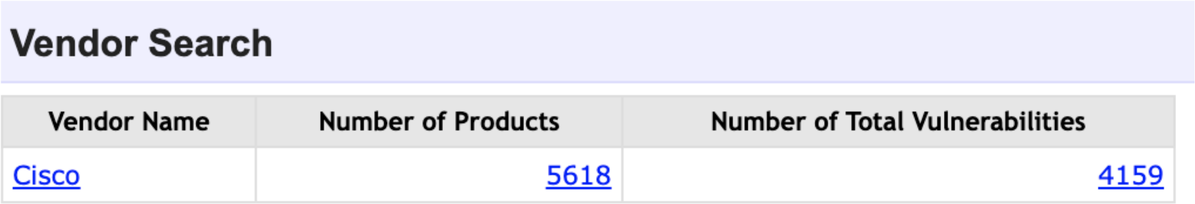
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	737	0.40
1-2	1150	0.70
2-3	7857	4.60
3-4	8519	5.00
4-5	40619	23.70
5-6	32604	19.00
6-7	25426	14.80
7-8	34304	20.00
8-9	841	0.50
9-10	19288	11.30
Total	171345	

Weighted Average CVSS Score: **6.5**

Vulnerability Distribution By CVSS Scores

The database also contains ‘Search Option’ for: Vendor, Product, Version, Vulnerability search. Accredited vendors can be recognised by their confidence in presenting their vulnerabilities – for each product, in open access – see example of Cisco product vulnerabilities in Table 7.

Table 7: Vendor search - Current CVSS Score Distribution For All Vulnerabilities - Cisco Systems

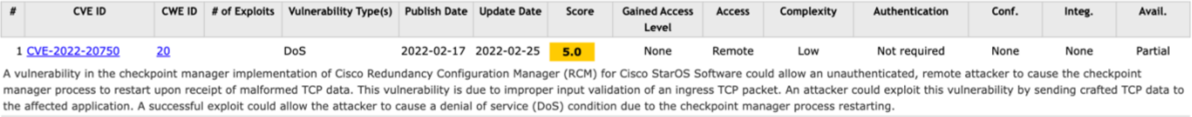


Vendor Search

Vendor Name	Number of Products	Number of Total Vulnerabilities
Cisco	5618	4159

Vulnerabilities are scored in accordance with their score, complexity, authentication, etc. – see Table 6. For better visibility, this exercise can be performed (repeated) on any computer connected to the internet, by using the links provided in this text.

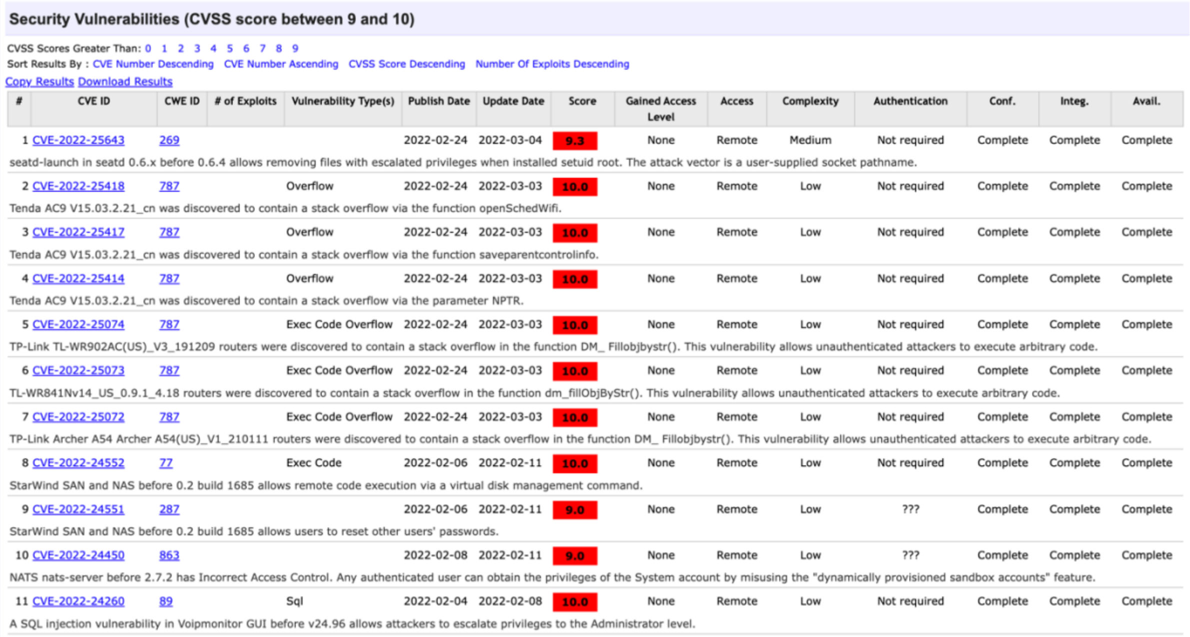
Table 8: Example of open access vulnerability scoring - Cisco



#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2022-20750	20		DoS	2022-02-17	2022-02-25	5.0	None	Remote	Low	Not required	None	None	Partial
A vulnerability in the checkpoint manager implementation of Cisco Redundancy Configuration Manager (RCM) for Cisco StarOS Software could allow an unauthenticated, remote attacker to cause the checkpoint manager process to restart upon receipt of malformed TCP data. This vulnerability is due to improper input validation of an ingress TCP packet. An attacker could exploit this vulnerability by sending crafted TCP data to the affected application. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to the checkpoint manager process restarting.														

The CVE database contains a detailed list of over 170,000 known vulnerabilities, including a long list of 386 pages of Security Vulnerabilities with CVSS score between 9 and 10 – see Table 6.

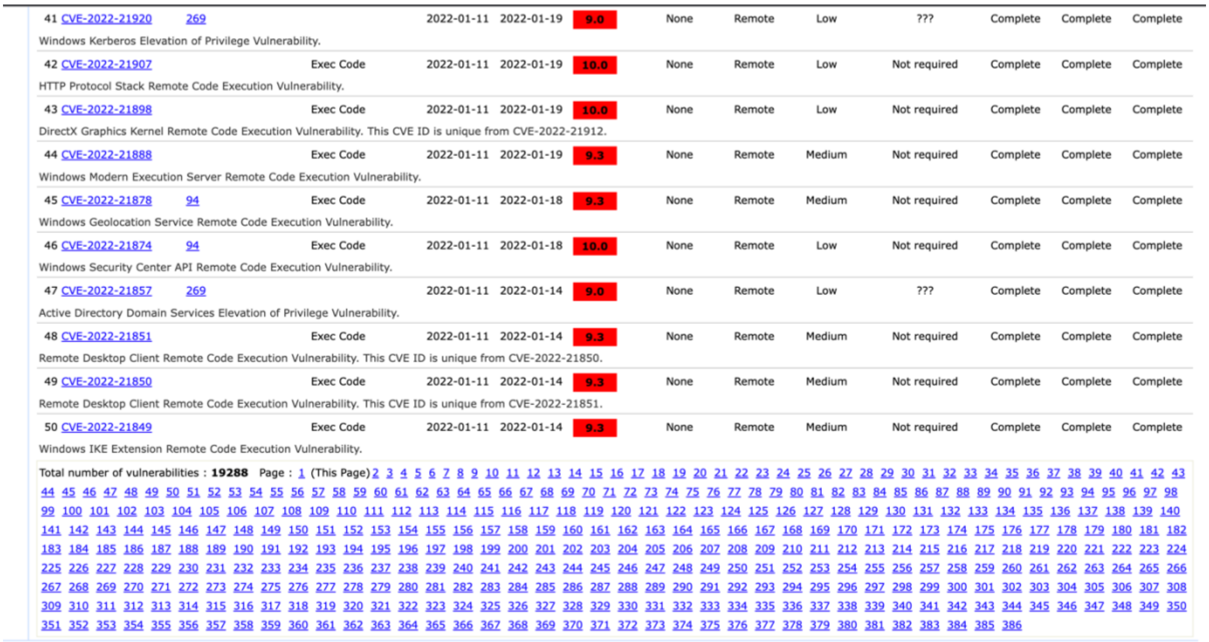
Table 9: Security Vulnerabilities with CVSS score between 9 and 10



Security Vulnerabilities (CVSS score between 9 and 10)

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2022-25643	269			2022-02-24	2022-03-04	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
seatd-launch in seatd 0.6.x before 0.6.4 allows removing files with escalated privileges when installed setuid root. The attack vector is a user-supplied socket pathname.														
2	CVE-2022-25418	787		Overflow	2022-02-24	2022-03-03	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Tenda AC9 V15.03.2.21_cn was discovered to contain a stack overflow via the function openSchedWifi.														
3	CVE-2022-25417	787		Overflow	2022-02-24	2022-03-03	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Tenda AC9 V15.03.2.21_cn was discovered to contain a stack overflow via the function saveparentcontrolinfo.														
4	CVE-2022-25414	787		Overflow	2022-02-24	2022-03-03	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Tenda AC9 V15.03.2.21_cn was discovered to contain a stack overflow via the parameter NPTR.														
5	CVE-2022-25074	787		Exec Code Overflow	2022-02-24	2022-03-03	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
TP-Link TL-WR902AC(US)_V3_191209 routers were discovered to contain a stack overflow in the function DM_ Fillobjbystr(). This vulnerability allows unauthenticated attackers to execute arbitrary code.														
6	CVE-2022-25073	787		Exec Code Overflow	2022-02-24	2022-03-03	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
TL-WR841Nv14_US_0.9.1_4.18 routers were discovered to contain a stack overflow in the function dm_fillObjByStr(). This vulnerability allows unauthenticated attackers to execute arbitrary code.														
7	CVE-2022-25072	787		Exec Code Overflow	2022-02-24	2022-03-03	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
TP-Link Archer A54 Archer A54(US)_V1_210111 routers were discovered to contain a stack overflow in the function DM_ Fillobjbystr(). This vulnerability allows unauthenticated attackers to execute arbitrary code.														
8	CVE-2022-24552	77		Exec Code	2022-02-06	2022-02-11	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
StarWind SAN and NAS before 0.2 build 1685 allows remote code execution via a virtual disk management command.														
9	CVE-2022-24551	287			2022-02-06	2022-02-11	9.0	None	Remote	Low	???	Complete	Complete	Complete
StarWind SAN and NAS before 0.2 build 1685 allows users to reset other users' passwords.														
10	CVE-2022-24450	863			2022-02-08	2022-02-11	9.0	None	Remote	Low	???	Complete	Complete	Complete
NATS nats-server before 2.7.2 has Incorrect Access Control. Any authenticated user can obtain the privileges of the System account by misusing the "dynamically provisioned sandbox accounts" feature.														
11	CVE-2022-24260	89		Sql	2022-02-04	2022-02-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
A SQL injection vulnerability in Voipmonitor GUI before v24.96 allows attackers to escalate privileges to the Administrator level.														



41	CVE-2022-21920	269		2022-01-11	2022-01-19	9.0	None	Remote	Low	???	Complete	Complete	Complete
Windows Kerberos Elevation of Privilege Vulnerability.													
42	CVE-2022-21907		Exec Code	2022-01-11	2022-01-19	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
HTTP Protocol Stack Remote Code Execution Vulnerability.													
43	CVE-2022-21898		Exec Code	2022-01-11	2022-01-19	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
DirectX Graphics Kernel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21912.													
44	CVE-2022-21888		Exec Code	2022-01-11	2022-01-19	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Windows Modern Execution Server Remote Code Execution Vulnerability.													
45	CVE-2022-21878	94	Exec Code	2022-01-11	2022-01-18	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Windows Geolocation Service Remote Code Execution Vulnerability.													
46	CVE-2022-21874	94	Exec Code	2022-01-11	2022-01-18	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Windows Security Center API Remote Code Execution Vulnerability.													
47	CVE-2022-21857	269		2022-01-11	2022-01-14	9.0	None	Remote	Low	???	Complete	Complete	Complete
Active Directory Domain Services Elevation of Privilege Vulnerability.													
48	CVE-2022-21851		Exec Code	2022-01-11	2022-01-14	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21850.													
49	CVE-2022-21850		Exec Code	2022-01-11	2022-01-14	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Remote Desktop Client Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21851.													
50	CVE-2022-21849		Exec Code	2022-01-11	2022-01-14	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Windows IKE Extension Remote Code Execution Vulnerability.													

Total number of vulnerabilities : **19288** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98
99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140
141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182
183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224
225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266
267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308
309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350
351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386

4.3. NIST Endpoint security and Blockchain Technology

In NIST 'Endpoint Protection Platform' is defined as: 'Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, antimalware, personal firewalls, host-based intrusion detection and prevention systems, etc.).' The main SP on End-point Protection is NIST SP 800-128 and the SP argues that the 'secure configurations for a system are most often achieved through the application of secure configuration settings to the IT products (e.g., operating systems, databases, etc.) used to build the system.'. The NIST SP 800-128 lists 4 main categories for implementing endpoint protection platforms, those are: Anti-malware, Personal Firewalls, Host-based Intrusion Detection and Prevention System (IDPS) and restrict the use of mobile code. In the text below, the use of mobile code is discussed in more detail.

The general recommendation from NIST is to restrict the use of mobile code, hence caution should be exercised in allowing the use of 'mobile code' in Blockchain projects, e.g., ActiveX, Java, and JavaScript. An attacker can easily attach a script to a URL in a Web page or email that, when clicked, will execute malicious code within the computer's browser. The associated NIST [SP 800-53] controls are: SC-7, SC-18, SI-3, SI-4.

5. Discussion on new and emerging technologies – IoT and Blockchain Metaverses

New technologies such the internet-of-things (IoT) and Blockchain Metaverses are also affecting the cyber and cloud security. For example, IoT devices have been used for a Distributed Denial of Service (DDoS) attacks on cloud infrastructure. The increased usage of new IoT devices is creating different types of cyber risk that are not fully understood by cyber security practitioners. This is mainly because of the fast developments in these technologies. While with traditional IT infrastructures, like desktop computers, the communication protocols are quite consistent. The operating models are also limited in number (e.g., Windows, iOS, Linux). But with IoT technologies, there is a vast number of communication protocols (e.g., LoRa, ZigBee, 5G). There is also a vast number of different devices, designed for specific and difficult to solve problems. Their main strengths are their low cost, low computational power, low memory, and low energy consumption. These characteristics also make IoT devices the most vulnerable from all IT systems. It seems really challenging to secure a device that cannot run most antivirus programs. We can expect such solutions to emerge in the future, just based on the rapid number of IoT devices added to the network.

Second major technological trend in 2023 is the Blockchain Metaverses. The term Metaverse originates from a 1992 science function novel from Neal Stephenson [58], but since then, it has become a definition for the future version of the immersive Internet. The Metaverse concept relies on a coordinated integration of a specific set of new technologies, which include the Cloud, IoT, and Blockchains. Some of these technologies are regulated individually (e.g., the Cloud), and some are not regulated at all (e.g., cryptocurrencies).

The Blockchain started with the emergence of Bitcoin in 2009, but at present (29th March 2023), there are over 23,09921,872 Crypto projects [59]. According to the same source, the total market cap was almost $2 trillion (January 2022), and at that time, the Crypto market had over $100 billion in trading volume per day, traded on over 475 different exchanges. These figures are confirmed (in January 2022) by a different source, which stated that the total market cap is over $2 trillion, the trading volume per day is over $100 billion, and crypto is traded on over 587 different exchanges [60]. Although the market cap has reduced since these dates, the Market Cap is still significant ($853bn – on 28th of November 2022, and $1.1 trillion as of 29th of March 2023) [60]. These new technologies have increased the cyber-attack surface, and currently there are almost no regulations or security guidance on these technologies. It feels as if MiCA bill comes too late, because many of the issues the bill is designed to prevent, already happened. But at least they are coming in, and it will help prevent future crashes with the likes of Terra Luna.

6. Conclusion

While cybersecurity awareness is increasing, some of the main cyber risks remain. The review includes the newest security standards on cryptocurrencies, internet-of-things, and blockchain technologies, which have not been reviewed in combination with other cybersecurity standards. Organisations need to take action to prevent hackers from accessing their critical data and technologies. This review article is focused on multiple standards and regulations, while NIST and ISO27001 are used for comparison. New standards are also discussed, like ENISA. Although these standards are still in their infancy comparing to NIST, their contributions should not be ignored. Some of the key findings from this review study are:

1. ENISA follows the NIST approach but provides a different perspective on how cyber risk should be assessed.
2. ENISA seems to be following the non-technical design of the NIST standards, but the technical guidance from the NIST cryptographic algorithms is missing from the ENISA cyber risk assessment guidance documents.
3. Future research is needed to help understand the new risks from increased adoption of new technologies (e.g., IoT and Blockchain).
4. There are no current standards to govern the use of Blockchains, and their value has increased to over a trillion.
5. Failure of one main stable-coins, like USDT, USDC, or BUSD, could trigger a domino effect in other stable-coins, and spill over into a crypto winter for all Blockchains.
6. The Federal Reserve has been slow in responding to the systemic risk created by stable coins and cryptocurrencies.
7. The continuous funding of new reports on CBDC has not resulted with any significant advancements in the developments a USA regulated CBDC.
8. The asset value (as of 28th November 2022) of USDT was $65bn, of the USDC was $44bn, and BUSD was $22bn, and those are just 3 cryptos out of 21,872 cryptos and these projects operate with almost no regulation from any government in the world.
    a. The current asset value (as of 29th March 2023) of USDT is changed to $79.5bn, of the USDC is $33bn, and BUSD is $7bn.
    b. This change was caused by the depegging of the USDC that traded over 12% below the US dollar beginning of March 2023, following the collapse of Silicon Valley Bank (SVB).
    c. The BUSD was partially affected by the collapse of SVB, but also by other factors, for example, today, investors decided to 'pull $1.6 billion from Binance after CFTC lawsuit' [61]
9. Financial regulators have ignored the cryptocurrencies, but without regulations, we can expect these assets to remain volatile and many individuals will lose their savings.
10. The crypto market is difficult for EU and US regional regulators to supervise, because many project are based abroad and operate on the Internet. One of the key measures for success is to regulate crypto exchanges that are allowed to operate in the region, and not push the exchanges away into countries that are out of their jurisdictions.
11. The EU is much further away than the US, from regulating the crypto market and bringing it into the mainstream. The MiCA is not perfect, but at least it's a framework and infrastructure to use as a guidance point.
12. It looks like layer one coins will be exempted - in the EU at least.

This review of cybersecurity and cyber risks in 2022 has covered a variety of risks, starting from Cloud security, IoT security, cybersecurity risk assessment and governance, and Blockchain technologies, including cryptocurrencies. The overarching conclusion is that many cyber risks remain unregulated, including IoT and crypto. With this analysis, we can forecast that:

A). DDoS attacks will continue in 2022 and beyond and become more sophisticated.

B). Crypto markets are likely to cause significant loss of savings for individuals that invest in them.

These forecasts are not based on any specific risk factor that makes these new technologies more risky than other technologies. The main factor for the cyber risk from these two technologies is the lack of regulations, in the US, EU, UK, and globally.

6.1. Limitation of this study

This study is based on a literature review and case study of existing documents and secondary data. Many of the new and emerging regulations for Blockchain security are still in the infancy, and it is hard to assess their value without a detailed guidance on cryptography, because Blockchain computing is simply a virtual computer operating in a virtual database, and the main risk is the data. The remaining aspects of cybersecurity are relatively similar to the cyber risk before Cloud computing (e.g., access management). It is also quite difficult to assess individual risk from various cryptos because they do not disclose any data, not even how and where their funds are stored. Many of the 21,872 cryptos do not even have a white paper published on their projects. The value of this study is purely to present a snapshot in time, so future researchers can refer to the known cyber risks of the 2022, that remained ignored for far too long, and already triggered some major losses for investors (e.g., FTX collapse). Worth mentioning that the number of cryptos and the market cap has changed multiple times during the writing of this paper. We can assume that the data will be very different at the time this paper is published and has reached the readers.

Competing interests: No conflict nor competing interest. The author declares no conflicts of interest.

Funding: This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC [under grant number EP/S035362/1] and by the Cisco Research Centre [grant number CG1525381].

Acknowledgements: Eternal gratitude to the Fulbright Visiting Scholar Project.

7. References:

[1] J. Srinivas, A. K. Das, and N. Kumar, “Government regulations in cyber security: Framework, standards and recommendations,” *Future Generation Computer Systems*, vol. 92, pp. 178–188, Mar. 2019, doi: 10.1016/J.FUTURE.2018.09.063.

[2] K. de Fine Licht and J. de Fine Licht, “Artificial intelligence, transparency, and public decision-making,” *AI & SOCIETY*, pp. 1–10, Mar. 2020, doi: 10.1007/s00146-020-00960-w.

[3] G. Falco, A. Noriega, and L. Susskind, “Cyber negotiation: a cyber risk management approach to defend urban critical infrastructure from cyberattacks,” *Journal of Cyber Policy*, vol. 4, no. 1, pp. 90–116, Jan. 2019, doi: 10.1080/23738871.2019.1586969.

[4] M. D. Workman, J. A. Luévanos, and B. Mai, “A Study of Cybersecurity Education Using a Present-Test-Practice-Assess Model,” *IEEE Transactions on Education*, vol. 65, no. 1, pp. 40–45, 2021.

[5] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2003.

[6] G. Watson, A. Mason, and R. Ackroyd, *Social engineering penetration testing: executing social engineering pen tests, assessments and defense*. Syngress, 2014.

[7] A. Smith, M. Papadaki, and S. M. Furnell, “Improving awareness of social engineering attacks,” in *Information Assurance and Security Education and Training*, Springer, 2013, pp. 249–256.

[8] J. Long, *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. Syngress, 2011.

[9] A. McIlwraith, *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge, 2021.

[10] P. Dixit and S. Silakari, “Deep learning algorithms for cybersecurity applications: A technological and status review,” *Computer Science Review*, vol. 39, p. 100317, 2021.

[11] B. Zohuri, M. Moghaddam, and F. Mossavar-Rahmani, “Business Resilience System Integrated Artificial Intelligence System,” *International Journal of Theoretical & Computational Physics*, vol. 3, pp. 1–7, 2022.

[12] D. U. Case, “Analysis of the cyber attack on the Ukrainian power grid,” *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[13] V. Schlatt, T. Guggenberger, J. Schmid, and N. Urbach, “Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity,” *Int J Inf Manage*, vol. 68, p. 102470, Feb. 2023, doi: 10.1016/J.IJINFOMGT.2022.102470.

[14] S. Mahmood, M. Chadhar, and S. Firmin, “Cybersecurity Challenges in Blockchain Technology: A Scoping Review,” *Hum Behav Emerg Technol*, vol. 2022, pp. 1–11, Apr. 2022, doi: 10.1155/2022/7384000.

[15] V. Wylde *et al.*, “Cybersecurity, Data Privacy and Blockchain: A Review,” *SN Computer Science 2022 3:2*, vol. 3, no. 2, pp. 1–12, Jan. 2022, doi: 10.1007/S42979-022-01020-4.

[16] S. He *et al.*, “Blockchain-based automated and robust cyber security management,” *J Parallel Distrib Comput*, vol. 163, pp. 62–82, May 2022, doi: 10.1016/J.JPDC.2022.01.002.

[17] A. Hazra, A. Alkhayyat, and M. Adhikari, “Blockchain-aided Integrated Edge Framework of Cybersecurity for Internet of Things,” *IEEE Consumer Electronics Magazine*, 2022, doi: 10.1109/MCE.2022.3141068.

[18] Y. I. Ll. Lucio, K. Marceles Villalba, and S. A. Donado, “Adaptive Blockchain Technology for a Cybersecurity Framework in IIoT,” *Revista Iberoamericana de Tecnologias del Aprendizaje*, vol. 17, no. 2, pp. 178–184, May 2022, doi: 10.1109/RITA.2022.3166857.

[19] O. Cheikhrouhou, I. Amdouni, K. Mershad, M. Ammi, and T. N. Gia, “Blockchain for the Cybersecurity of Smart City Applications,” Jun. 2022, Accessed: Mar. 29, 2023. [Online]. Available: https://arxiv.org/abs/2206.02760v1

[20] M. Liu, W. Yeoh, F. Jiang, and K. K. R. Choo, “Blockchain for Cybersecurity: Systematic Literature Review and Classification,” *https://doi.org/10.1080/08874417.2021.1995914*, vol. 62, no. 6, pp. 1182–1198, 2021, doi: 10.1080/08874417.2021.1995914.

[21] A. Deshmukh, N. Sreenath, A. K. Tyagi, and U. V. E. Abhichandan, “Blockchain Enabled Cyber Security: A Comprehensive Survey,” *2022 International Conference on Computer Communication and Informatics, ICCCI 2022*, 2022, doi: 10.1109/ICCCI54379.2022.9740843.

[22] R. Prakash, V. S. Anoop, and S. Asharaf, “Blockchain technology for cybersecurity: A text mining literature analysis,” *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100112, Nov. 2022, doi: 10.1016/J.JJIMEI.2022.100112.

[23] M. in C. R. (MiCA), “Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA),” 2022.

[24] NIST, “NIST Version 1.1,” *National Institute of Standards and Technology, U.S. Department of Commerce*, 2018. https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

[25] NIST, “Cybersecurity Framework,” 2022. https://www.nist.gov/cyberframework/getting-started

[26] Advisera, “What is the meaning of ISO 27001?,” 2022. https://advisera.com/27001academy/what-is-iso-27001/

[27] NIST 800-53, “Security and Privacy Controls for Information Systems and Organizations,” 2020.

[28] ISO, “ISO/IEC 27001 and related standards Information security management,” 2022.

[29] M. Petrov, “Adapted SANS Cybersecurity Policies for NIST Cybersecurity Framework,” 2021.

[30] J. E. Catril Opazo, “NIST cybersecurity framework in south america: Argentina, Brazil, Chile, Colombia, And Uruguay,” 2021.

[31] M. J. ALDhanhani, “Review of Cyber Security on Oil and Gas Industry in United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 11, pp. 714–720, 2021.

[32] A.-M. Udroiu, M. Dumitrache, and I. Sandu, “Improving the cybersecurity of medical systems by applying the NIST framework,” in *2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, IEEE, 2022, pp. 1–7.

[33] NIST, “NIST Special Publication 800-128,” 2011.

[34] NIST, “Block Cipher Techniques,” 2020. https://csrc.nist.gov/Projects/block-cipher-techniques

[35] NIST, “Hash Functions,” *2020*. https://csrc.nist.gov/Projects/Hash-Functions

[36] NIST, “Key Management - Symmetric Block Ciphers, Pair-Wise Key Establishment Schemes,” 2022.

[37] NIST, “Post-Quantum Cryptography PQC,” 2022. https://csrc.nist.gov/Projects/post-quantum-cryptography

[38] NIST, “Lightweight Cryptography,” 2022. https://csrc.nist.gov/Projects/lightweight-cryptography

[39] NIST, “Privacy-Enhancing Cryptography PEC,” 2022. https://csrc.nist.gov/Projects/pec

[40] MITRE, “MESSAGETAP,” 2020.

[41] T. Kovanen, J. Pöyhönen, and M. Lehto, “Cyber-Threat Analysis in the Remote Pilotage System,” in *ECCWS 2021 20th European Conference on Cyber Warfare and Security*, Academic Conferences Inter Ltd, 2021, p. 221.

[42] Y. Cao, H. Jiang, Y. Deng, J. Wu, P. Zhou, and W. Luo, “Detecting and mitigating ddos attacks in SDN using spatial-temporal graph convolutional network,” *IEEE Transactions on Dependable and Secure Computing*, 2021.

[43] CISCO, “Cisco Firepower Next-Generation Firewall Overview,” 2022. https://www.router-switch.com/cisco-firepower-ngfw.html#:~:text=The Cisco Firepower^{TM} Next,the network to the endpoint.

[44] S. Creese, W. H. Dutton, P. Esteve-González, and R. Shillair, “Cybersecurity capacity-building: cross-national benefits and international divides,” *https://doi.org/10.1080/23738871.2021.1979617*, vol. 6, no. 2, pp. 214–235, May 2021, doi: 10.1080/23738871.2021.1979617.

[45] Y. Hong and S. Furnell, “Understanding cybersecurity behavioral habits: Insights from situational support,” *Journal of Information Security and Applications*, vol. 57, p. 102710, Mar. 2021, doi: 10.1016/J.JISA.2020.102710.

[46] W. Kitler, *Cybersecurity in Poland: The Cybersecurity Strategy of the Republic of Poland*. 2021. doi: 10.1007/978-3-030-78551-2.

[47] F. R. Moreira, D. A. Da Silva Filho, G. D. A. Nze, R. T. De Sousa Junior, and R. R. Nunes, “Evaluating the Performance of NIST&#x2019;s Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology,” *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3113178.

[48] R. T. Williams and A. Capstone, “Banking and Cybersecurity Governance,” Utica College, Utica, New York, 2021.

[49] A. Khan and M. Malaika, “Central Bank Risk Management, Fintech, and Cybersecurity - Mr. Ashraf Khan, Majid Malaika - Google Books,” 2021.

[50] P. Cheng, “Decoding the rise of Central Bank Digital Currency in China: designs, problems, and prospects,” *Journal of Banking Regulation 2022*, pp. 1–15, Feb. 2022, doi: 10.1057/S41261-022-00193-5.

[51] T. Hansen and K. Delak, “Security Considerations for a Central Bank Digital Currency,” *FEDS Notes*, vol. 2022, no. 2970, Feb. 2022, doi: 10.17016/2380-7172.2970.

[52] The Federal Reserve, “Central Bank Digital Currency (CBDC),” 2022.

[53] The Federal Reserve, “Research & Publications - Central Bank Digital Currency (CBDC),” 2022. https://www.federalreserve.gov/cbdc-research-and-publications.htm

[54] ENISA, “EUCS – Cloud Services Scheme,” 2020.

[55] ENISA, “Cloud Computing Risk Assessment,” 2009.

[56] NIST, “Product Integration using NVD CVSS Calculators,” 2022.

[57] CVE, “Current CVSS Score Distribution For All Vulnerabilities,” 2022.

[58] N. Stephenson, *Snow crash: A novel*. Spectra, 2003.

[59] Coinmarketcap, “Cryptocurrency Prices by Market Cap,” 2022. https://coinmarketcap.com/

[60] Coingecko, “Cryptocurrency Prices by Market Cap,” 2022. https://www.coingecko.com/

[61] E. Howcroft, “Investors pull $1.6 billion from Binance after CFTC lawsuit | Reuters,” *Reuters*, Mar. 2023. https://www.reuters.com/legal/investors-pull-16-billion-binance-after-cftc-lawsuit-2023-03-29/ (accessed Mar. 29, 2023).