Applied Computing Journal https://doi.org/10.52098/acj.202364
ISSN: 2788-9688 Volume 3, Issue 1, pp 245-255, February 2023
Received: 12/1/2023 Revised: 26/1/2023 Accepted: 6/2/2023

CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001

Marwan Alshar'e[1,*]
[1] Faculty of Computing Information Technology, Sohar University, Sohar, Oman
* Corresponding author: Marwan Alshar'e[1], mshare@su.edu.om

Abstract

Plans for preventing and mitigating vulnerabilities in computer networks are known as cybersecurity frameworks. With the assistance of the Cybersecurity Framework, organisations are able to reduce their vulnerability to cyber-attacks and improve the strength of their defences. The cybersecurity framework has made the decision to take part in trials so that it may improve its ability to handle long-term security frameworks. This gives rise to concerns about cost and time rather than safety at this point in time because of the situation that is occurring. A firm may utilise the similarities that are shared by many cyber security frameworks as a reference to assist it in selecting the framework that is the most suitable for the needs that are unique to the organisation. This study investigated the literature to compare the two-cybersecurity framework NIST and ISO27001 adequacy and selection criteria. According to the findings of this study, the risk maturity level, cost, and certification are the three most significant components of CSF implementation for firms.

Keywords*:* Cyber security; Cyber Security Framework; CSF; Selection; NIST; ISO 27001

Author(s) and ACAA permit unrestricted use, distribution, and reproduction in any medium, provided the original work with proper citation. This work is licensed under Creative Commons Attribution International License (CC BY 4.0).

1. Introduction

It is a huge difficulty for service providers to deal with attack actors whose aims include accessing either system data or consumer data. In spite of the widespread belief that security providers include cyber protection as an essential component of the services they provide, a recent survey conducted by Insight revealed that over seventy percent of business owners do not have confidence that their companies can withstand an attack launched via cyberspace (M. I. Alshar'e, Sulaiman, Mokhtar, & Zin, 2014); (ALSHAR'E et al., 2015); (Najar et al., 2020),(Alshar'E et al., 2015); (Roy, 2020), (Mustafa et al., 2022); (M. Alshar'e et al., 2022).

The first thing to understand is that security needs are different for every organization. This means that there is no one-size-fits-all solution for securing an organization's information assets. Every business has unique requirements and those requirements change over time, which makes it even more important to work with a security consulting firm that understands your business and its unique needs. Security risks can be reduced by implementing the right controls in place, but they cannot be eliminated entirely without putting your company at risk of a breach (Mustafa et al., 2021); (Olayah et al., 2022); (JAWARNEH, 2022). The best way to reduce the risk of a breach is by identifying where vulnerabilities areis the best way to reduce the risk as a consequence of taking a break (Saini, D. & Yousif, J., 2021). A breach in data security occurs when sensitive information may be accessed, modified, or removed without the owner's knowledge or consent. Any component of the hardware, any network node, any application, or any component of the operating system might contain a security issue (M. Alshar'e & Mustafa, 2021) ; (Alshar'e, Albadi, et al., 2022).

A "cyber security framework" is a collection of international standards and best practises that are referred to collectively as a "cyber security framework" (Atoum et al., 2014); (Mustafa et al., 2020), (Bian et al., 2022). This framework is necessary for the protection of information and IT infrastructure against cyber-attacks and other security hazards. It's possible that when you hear the phrase "cyber security framework," what you're really referring to is an international set of principles for keeping networks secure. It is possible for companies to utilise the frameworks as a jumping off point in order to improve the security of their computer networks. Cybersecurity frameworks are designed to assist businesses and other organisations in the case of a cyberattack by assisting them in analysing the situation, keeping track of threats, and taking the required action. Businesses are able to manage their cyber security risks in a way that is both voluntary and straightforward because to the frameworks for cyber security, which are founded on a set of previous principles and standards. Both the government and the private sector have contributed to the

construction and development of cyber security regimes. Components of cyber security frameworks include rules, standards, practises, and ideas that ensure robust safety. These may be broken down into four categories: rules, practises, and suggestions.

There are cyber security frameworks available that are aimed to assist businesses not just with risk reduction but also with the coordination and communication of its partners (Boneh & Shoup, 2020); (Smail et al., 2022). Cybersecurity frameworks are constructed consisting of separate elements, each of which is responsible for a certain purpose. The fundamental component of the framework is in charge of standardising the process of tracking and defending against cyber threats and assaults. The management of cyber security via the use of specific protocols is the responsibility of the various implementation tiers. Thirdly, profiles are vital in identifying and putting into action efficient measures to increase cyber security all across an organisation (Forouzan & Mukhopadhyay, 2015). Some of the most common cyber security models include the following. Although at first glance the frameworks seem to be quite distinct from one another, in reality they are all working toward the same goal. There is a degree of diversity across the various cyber security frameworks; this provides companies with the opportunity to make well-informed decisions based on considerations such as appropriateness and usefulness.

2. Background

Before a cyber-attack can take place, companies and organisations need to establish the best possible frameworks to keep track of, manage, and eliminate any threats to their online safety. The creation of a cyber security framework is the most effective technique for guaranteeing that users are protected in an online setting (M. I. Alshar'e, Sulaiman, Mokhtar, & MohdZin, 2014); (M. Alshar'e et al., 2022). Because it contains all of the essential processes and instruments, this structure is an excellent choice for protecting the organization's resources. In the real world, a framework is the system of beams that holds up a building; however, in the realm of ideas, it refers to the framework that identifies a system and its data, as well as the way of organising that data and any other responsibilities that may be associated to it (Panda & Bower, 2020). In the real world, a framework is the system of beams that holds up a building; however, in the realm of ideas, it refers to the framework that identifies a system and its

The term "cybersecurity framework" refers to a set of rules, procedures, and standards that are designed to combat threats that may be found online (Chidukwani, A. et al., 2022).

The security objectives that are intended to be met by the frameworks include things like making it more difficult for criminals and hackers to take advantage of the system by removing its vulnerabilities and researching its weak points (Kahyaoglu & Caliyurt, 2018).

The use of cyber security frameworks may be advantageous for security provider managers (SPMs) since these frameworks give a standardised and logical approach to the mitigation of cyber risk. The seven cyber security frameworks that are utilised the most often are SOC2, "ISO 27001/27002 and NIST Cyber Security framework," FISMA, GDPR, and HIPAA. NERC CIP is the seventh most utilised cyber security framework. By establishing a consistent lexicon and set of criteria for security provider managers across a variety of industries and corporations, the goal of these frameworks is to provide organisations with a road map for analysing, monitoring, and removing cyber security threats (Asaad R. & Saeed V., 2022). This will be accomplished by offering organisations a road map. This is done in order to provide companies with a map of the actions and procedures that they need to carry out in order to protect themselves against cyberattacks (Shackelford, Russell, et al., 2015); (Sabillon et al., 2017), (Azmi et al., 2018).

One of the most significant components of sec helpful is the cyber security framework, which has gained broad acceptance across large and small enterprises equally (Srinivas et al., 2019). Because it impacts many other sectors in addition to manufacturing, it is one of the most essential aspects of sec useful. Due to the fact that it is used in a wide variety of sectors and businesses, it may be considered a rather comprehensive structure. There are three types of cyber security frameworks based on the needed function, which are:

- Control frameworks: These give an overall strategy for the cybersecurity team of an organisation, provide a basic set of security controls, and assist to prioritise the implementation of such measures.
- Program frameworks: With the help of this framework, an analysis of the state of the organization's security programme and an evaluation of its degree of safety were carried out.
- Risk frameworks: Frameworks of this kind are used so that the procedures that are necessary for risk assessment can be specified, and so that the proper security measures and activities may be prioritised. Threats to the organization's security are also characterised, quantified, and evaluated in this process.

A framework for cyber security provides users with several advantages. To begin, it provides a comprehensive language and a systematic strategy to lowering the risk associated with cyber security. One further advantage of implementing a cyber security framework is that it will combine together a variety of different protective

responsibilities, which can then be tailored to the requirements of a certain company. On the other hand, framework profiling enables businesses and other organisations to focus in on the areas in which they may either build whole new processes or make enhancements to the ones they already have. The combination of these features with the simple vocabulary used in the frameworks makes it easier to have clear communication across the board and with consumers. It may be beneficial for organisations to employ frameworks since doing so provides them with an understanding of how the organisation as a whole handles the management of cyber security risks. As a result, the framework is used as a tool for evaluation, during which the budget, the importance of the mission, and the appetite for risk are evaluated (Donaldson et al., 2015); (Shackelford, Russell, et al., 2015). In any case, the integration of the cyber risk management framework with the organization's risk management strategy is one of the primary reasons why the cyber security framework is one of the most effective methods for preventing cyberattacks. Any company or other organisation, regardless of its size or purpose, that does not implement any kind of cyber security policy stands the danger of suffering from three different kinds of harm. Due to the absence of a comprehensive cyber security framework, a company is unable to determine which security programmes and firewalls are required to protect its data from being compromised by potentially hazardous online behaviour. The organisation does not have the resources required to either avoid cyber security attacks or react to those that have already occurred. Because of this, the organisation does not have the resources necessary to mount a defence against the threat. Companies are unable to develop a transparent command structure from the moment an attack is discovered if they do not have an established cyber security architecture (Radanliev et al., 2018); (Malatji et al., 2019); (Kim et al., 2021).

3. Comparison of the Two Frameworks

When it comes to the protection of sensitive information, organisations have access to hundreds of different cyber security frameworks from which to choose. The Cyber Security Framework developed by the National Institute of Standards and Technology (NIST) and the one developed by the International Organization for Standardization (ISO) are two of the most common examples (Ajijola et al., 2014); (Thakur et al., 2015); (Shackelford, Proia, et al., 2015); (Radanliev et al., 2019); (White & Sjelin, 2022). Each of these architectures places an emphasis on achieving a high level of security as one of its key aims. Both share certain qualities while also revealing some obvious differences between the two.

3.1 National Institute of Standards and Technology Cyber security Framework (NIST) Framework

It comprises three main components that may assist a business owner evaluate and rank the state of his company's risk maturity, as well as the steps he has to take to enhance it.

- Core: Identification, protection, reaction, and recovery are the five essential functions that make up the core processes. In order to address concerns around cyber security, the framework used these elements. These actions, which were split down into a total of 23 activities, covered everything from the fundamentals of developing a cyber security programme to the fundamental aspects of risk management systems.
- Implementation tiers: The NIST CSF employed a scoring system with points ranging from 0 to 4 on a scale from 0 to establish an overall score that the firm could use as a benchmark for its level of risk maturity.
- Profiles: It is beneficial to organisations in evaluating their current risk tolerance level. Aside from that, it educates the organisation on how to reduce risks and gives security measures a higher priority, both of which are positive outcomes. If the company compares its present profiles to its ideal profiles, it may be able to more effectively deploy its resources to improve its security management over time, which will help the company expand.

3.1.1 Strengths of the NIST framework

- Make it possible for management of cyber risks and safety to continue for the long term.
- The internet really needs to have greater safeguards in place.
- Connect the links between the world of business and the community of technical innovators.
- Make sure you are well-prepared for the time when you will be required to comply with the requirements.

3.1.2 Weakness of the NIST framework

When it comes to the protection of cloud environments or cloud computing systems, there are very few hazards. It is not possible to get international accreditation using this method.

3.2 ISO Framework

The International Organization for Standardization (ISO) is a non-governmental organisation with its headquarters in Geneva that has published more than 22600 standards for use in a diverse array of industries. It encompasses a wide range of processes involved with the management of IT risk and with the protection of data. The framework for the development of an information systems management system is described. It is generally agreed upon that the set of

standards known as ISO 27001 provides a trustworthy basis for security management. Determination is made on the prerequisites for creating, implementing, and improving information security management systems. Increasing the security of a company's sensitive data may be accomplished in a number of ways, one of which is through adopting ISO. The implementation of ISO guarantees that data can be relied on, that it is always available, and that it is always maintained safe. An audit against an ISO framework is conducted in two stages. The first step of the audit is referred to as the "documents review," and it is during this phase that the auditor looks into the written records of the system's operations, policies, and procedures to determine whether or not they comply with ISO 27001. An on-site review is part of the second step, which is known as the "certification audit." The goal of this phase is to verify whether or not the organisation in question has implemented an ISMS in line with ISO 27002. However, ISO certification has a time limit of three years before it must be renewed(Middleton, 2022).

3.2.1 Strengths of ISO

An important competitive advantage in the market Recovering from financial failures brought on by security breaches requires specific expertise. The reduction of the costs associated with breaching the law led to cost savings. It brings about a huge improvement in the overall order inside.

3.2.2 Weakness of ISO

The additional cost incurred as a result of needing to do more work.

- It is required to be updated once every three years.
- It is imperative that cash be set aside for IT. However, ISO 27001 does not provide a clear definition of scope.
- Because of this, it is simple for clients to be deceived into thinking that the certification applies to the whole organisation rather than simply a particular sector of the business.

3.3 The similarities between ISO and NIST

Both of these all-encompassing frameworks address the management of the risks associated with cybersecurity. Because there is considerable interest among companies in adopting the NIST framework and in satisfying the standards of ISO, the 27001 recommendations ought to be easy to put into practise. Many of the framework-specific controls, as well as the definitions and codes that are used in one framework, may be used in another framework. This is also true for the majority of the controls. Both of these frameworks make use of vocabulary that is globally known,

which makes it easier for professionals working in a broad variety of fields to communicate clearly and effectively about challenges related to cyber security.

3.4 The differences between NIST and ISO

There are some differences between NIST CST and ISO such as cost, certification, and risk maturity.

- Cost: While the resources of the NIST may be accessed without charge at any time, those of the ISO cannot. Most new and developing organisations want to start their cyber security risk management programme with NIST, and as they grow, they will want to raise their investment in ISO 20071, which is where they will want to manage their cyber security risk.
- Certification: You have the opportunity to get third-party certification with ISO 20071, which will be acknowledged in any region of the globe. Although this may come at a high cost, there is a possibility that it may assist the organisation in gaining the trust of its stakeholders and consumers. Despite this, NIST does not provide any type of certification of any kind.
- Risk maturity: If your firm is just getting started on formulating a plan for mitigating the dangers posed by cyberspace and you want to make sure you don't make the same errors again, NIST could be the way to go. If your organisation is already well-established and ready to seek certification, ISO 20071 is a good standard to adopt.

3.5 The Complexity of ISO 27001 and NIST

You should anticipate that ISO 27001 will be as complicated as it must be for a firm of Your Size and Type in order to be successful. To maintain adequate control over its vulnerabilities, a bigger company will need to take into consideration and put into practise an increased number of precautions, regulations, and processes. In addition to bigger activities, actions involving a large number of employees should be carried out. One example of this would be making certain that every employee had exceptional cyber security expertise. The framework developed by NIST is more complicated than the one developed by ISO. The NIST framework is difficult to implement in many companies' operations because such companies lack the in-house NIST knowledge necessary to do so. CyberStorngTM and cyber saint® are two products that were created with the goal of making this procedure easier. Cyber strong simplifies the process of adopting NIST by dividing it up into five distinct steps: identifying, protecting, detecting, reacting, and

recovering. As a consequence of this, consolidate all of the operations into a single system. Table 1 provides a summary of the key differences between the cyber security frameworks developed by NIST and ISO.

Table 1. Key Difference between NIST and ISO 27001

NIST	ISO 27001
Has policies and procedures adhered to.	Uses security policies
Uses standard operation procedures	Follows Asset Management
Emphasizes on personal security	Emphasizes on human resources security
Involves awareness and trainings	Focuses on communication and management of operations.
Risk mitigation	Focuses on business continuity

4. Conclusion and Recommendations

Because of the intended organisational structure of the NIST Cybersecurity Framework (CSF), associations' boards of directors and monitoring programs are susceptible to attacks on the data security of the associations. In order to establish insurance coverage, the criteria developed by the National Institute of Standards and Technology (NIST) for nanotechnology are used (and even have their superhero ratings). Framework, Execution Levels, and Profiles are the three pillars that make up the NIST CSF. They work together to give a comprehensive assessment of the risks associated with your affiliates and a clear image of the actions that must be taken to manage those risks.

Failure to conform to the 27,000 standards established by ISO, which are among the most widely recognised standards in the world, may place the board of directors in peril. The International Organization for Standardization (ISO) 27001 is a set of guidelines for establishing and maintaining effective information security management systems (ISMS).

A report may be used to organise the findings of any network security audits carried out with the assistance of ISO 27001. This helps to guarantee that all of the required criteria and requirements for unquestionable information security architecture have been reached (ISMS). It is also possible to get formal ISO 27001 permanence, a commentator that cannot be violated. ISO 27001, much like NIST CSF, does not improve upon cycles or things explicit; nonetheless, the architecture of ISO 27001 provides more precision than NIST on security measures and is integrally tied to ISO revisions. IEC TS 27008 2019 has been revised to address the most recent insurance risks.

The differences between the two frameworks are broken down in terms of risk maturity, certification, and cost as follows:

In contrast to NIST CSF, which may be more appropriate for companies in critical times to promote organisational security that executives are anticipating or trying to allay previous dissatisfaction with data breaches, ISO 27001 is a better choice for young companies seeking accreditation due to its lower risk maturity. The International Organization for Standardization created ISO 27001. (ISO). The National Institute of Standards and Technology created the NIST Common Security Framework (NIST).

Products and services globally have been independently audited and certified as ISO 27001 compliant. Even so, an outside audit might be crucial to building confidence with a potential long-term partner in your business. The NIST CSF does not provide certificates of this kind. Cost, it is further explained that a newbie should begin damaging the council's program with the NIST CSF, as opposed to ISO 27001. This is because the NIST CSF is needlessly accessible, whereas ISO 27002 directs access to its documents. This is due to the fact that the NIST CSF may be accessed with little effort. ISO. 27001.

Acknowledgment

The research leading to these results has received no Research Project Grant Funding.

References

[1]. Ajijola, A., Zavarsky, P., & Ruhl, R. (2014). A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev. 1: 2014 and ISO/IEC 27037: 2012. *World Congress on Internet Security (WorldCIS-2014)*, 66–73.

[2]. Alshar'e, M., Albadi, A., Jawarneh, M., Tahir, N., & Al Amri, M. (n.d.). Usability evaluation of educational games: an analysis of culture as a factor Affecting children's educational attainment. *Advances in Human-Computer Interaction*, *2022*.

[3]. Alshar'e, M., Albadi, A., Mustafa, M., Tahir, N., & al Amri, M. (2022). Hybrid User Evaluation Methodology for Remote Evaluation: Case study of Educational games for children during Covid-19 Pandemic. *Journal of Positive School Psychology*, *6*(3), 3049–3063.

[4]. Alshar'e, M., al Nasar, M. R., Kumar, R., Sharma, M., Dharamvir, & Tripathi, V. (2022). A Face Recognition Method In Machine Learning (ML) For Enhancing Security In Smart Home. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 1081–1086. https://doi.org/10.1109/ICACITE53722.2022.9823833

[5]. Alshar'e, M. I., Sulaiman, R., Mokhtar, M. R., & MohdZin, A. (2014). DESIGN AND IMPLEMENTATION OF THE TPM USER AUTHENTICATION MODEL. *Journal of Computer Science*, *10*(11), 2299–2314. https://doi.org/10.3844/jcssp.2014.2299.2314

[6]. Alshar'e, M. I., Sulaiman, R., Mokhtar, M. R., & Zin, A. M. (2014). Design and Implementation of the TPM User Authentication Model. *J. Comput. Sci.*, *10*(11), 2299–2314.

[7]. Alshar'e, M., & Mustafa, M. (2021). Evaluation of autistic children's education in Oman: the role of eLearning as a major aid to fill the gap. *Elementary Education Online*, *20*(5). https://doi.org/10.17051/ilkonline.2021.05.623

[8]. Alshar'e, M., Mustafa, M., & Bsoul, Q. (2022). Evaluation of E-Learning Method as a Mean to Support Autistic Children Learning in Oman. *Journal of Positive School Psychology*, *6*(3), 3040–3048.

[9]. ALSHAR'E, M., Zin, A. M., Sulaiman, R., & Mokhtar, M. R. (2015). EVALUATION OF THE TPM USER AUTHENTICATION MODEL FOR TRUSTED COMPUTERS. *Journal of Theoretical \& Applied Information Technology*, *81*(2).

[10]. Alshar'E, M., Zin, A. M., Sulaiman, R., & Mokhtar, M. R. (2015). Evaluation of the TPM user authentication model for trusted computers. *Journal of Theoretical and Applied Information Technology*, *81*(2).

[11]. Asaad, R. R., & Saeed, V. A. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. Applied computing Journal, 227-244.

[12]. Atoum, I., Otoom, A., & Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, *22*. https://doi.org/10.1108/IMCS-02-2013-0014

[13]. Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, *3*(2), 258–283.

[14]. Bian, L., Chen, J., Soni, M., Bhola, J., Kumar, H., & Jawarneh, M. (2022). Research on computer 3D image encryption processing based on the nonlinear algorithm. *Nonlinear Engineering*, *11*(1), 664–671.

[15]. Boneh, D., & Shoup, V. (2020). A graduate course in applied cryptography. *Draft 0.5*.

[16]. Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access, 10, 85701-85719.

[17]. Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). Cybersecurity frameworks. In *Enterprise Cybersecurity* (pp. 297–309). Springer.

[18]. Forouzan, B. A., & Mukhopadhyay, D. (2015). *Cryptography and network security* (Vol. 12). Mc Graw Hill Education (India) Private Limited New York, NY, USA:

[19]. JAWARNEH, M. (2022). An Enhanced UTAUT Framework for Students Perception on Acceptance of Educational Games. *Iconic Research And Engineering Journals*, *6*(6), 254–261.

[20]. Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*.
[21]. Kim, K., Alfouzan, F. A., & Kim, H. (2021). Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework. *Applied Sciences*, *11*(16), 7738.
[22]. Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*.
[23]. Middleton, T. T. (2022). *Effective Cybersecurity Risk Management Policies for the Residential Real Estate Industry*. Capella University.
[24]. Mustafa, M., Alshare, M., Bhargava, D., Neware, R., Singh, B., & Ngulube, P. (2022). Perceived Security Risk Based on Moderating Factors for Blockchain Technology Applications in Cloud Storage to Achieve Secure Healthcare Systems. *Computational and Mathematical Methods in Medicine*, *2022*, 6112815. https://doi.org/10.1155/2022/6112815
[25]. Mustafa, M., Alzubi, S., & Alshare, M. (2020). The Moderating Effect of Demographic Factors Acceptance Virtual Reality Learning in Developing Countries in the Middle East. *Communications in Computer and Information Science*, *1244*, 12–23. https://doi.org/10.1007/978-981-15-6634-9_2
[26]. Mustafa, M., Virmani, D., Kaliyaperumal, K., Phasinam, K., & Santosh, T. (2021). Towards Investigation of Various Security And Privacy Issues In Internet Of Things. *Design Engineering*, 1747–1758.
[27]. Najar, F., Bourouis, S., Alshar'e, M., Alroobaea, R., Bouguila, N., Badi, A. H. Al, & Channoufi, I. (2020). *Efficient Statistical Learning Framework with Applications to Human Activity and Facial Expression Recognition*. https://doi.org/10.1109/atsip49331.2020.9231759
[28]. Olayah, F., Anaam, E. A., Bakhtan, M. A., Shamsan, A., Al Mudawi, N., Alazeb, A., Alshehri, M., & Jawarneh, M. (2022). Online Security on E-CRM System. *Telematique*, 7427–7443.
[29]. Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment*, *11*(4), 507–518.
[30]. Radanliev, P., De Roure, D., Nurse, J. R. C., Nicolescu, R., Huth, M., Cannady, S., & Montalvo, R. M. (2018). Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0. *Living in the Internet of Things: Cybersecurity of the IoT-2018*, 1–6.
[31]. Radanliev, P., Montalvo, R. M., Cannady, S., Nicolescu, R., De Roure, D., Nurse, J. R. C., & Huth, M. (2019). *Cyber Security Framework for the Internet-of-Things in Industry 4.0*.
[32]. Roy, P. P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, 1–3.
[33]. Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, 253–259.
[34]. Saini, D. K., & Yousif, J. H. (2021). Vulnerability and Attack Detection Techniques: Intrusion Detection System. In Cybersecurity (pp. 17-26). CRC Press.
[35]. Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Tex. Int'l LJ*, *50*, 305.
[36]. Shackelford, S. J., Russell, S., & Haut, J. (2015). Bottoms up: A comparison of voluntary cybersecurity frameworks. *UC Davis Bus. LJ*, *16*, 217.
[37]. Smail, B., Sanchez, D. T., Peconcillo Jr, L. B., de Vera, J. v, Horteza, A. L. D., Jawarneh, M., & others. (2022). Investigating different applications of Internet of Things towards identification of vulnerabilities, attacks and threats. *International Journal of Next-Generation Computing*, *13*(3).
[38]. Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188.
[39]. Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015). An investigation on cyber security threats and security models. *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 307–311.
[40]. White, G. B., & Sjelin, N. (2022). The NIST Cybersecurity Framework. In *Research Anthology on Business Aspects of Cybersecurity* (pp. 39–55). IGI Global.

Author(s) and ACAA permit unrestricted use, distribution, and reproduction in any medium, provided the original work with proper citation. This work is licensed under Creative Commons Attribution International License (CC BY 4.0).