Journal of Intelligent Systems and Internet of Things
Vol. 17, No. 02, PP. 458-487, 2025
DOI: https://doi.org/10.54216/JISIoT.170230

Comparative Evaluation of Information Technology Governance Frameworks for Ensuring Cybersecurity Compliance in the Internet of Things Era

Saleh Alharbi[1,*]

[1]College of Computing and Information Technology, Information Technology Department, Shaqra University, 11961, Riyadh 11961, Saudi Arabia

Email: Saleh@su.edu.sa

Abstract

The proliferation of Internet of Things (IoT) technologies has transformed digital ecosystems, creating highly interconnected environments that demand robust and adaptive cybersecurity governance. Despite their widespread adoption, existing Information Technology Governance (ITG) frameworks—such as the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, Center for Internet Security (CIS) Controls, and ISA/IEC 62443 vary considerably in scope, applicability, and alignment with the unique characteristics of IoT infrastructures. The absence of a unified approach to address IoT-specific challenges such as device heterogeneity, data provenance, and real-time monitoring underscores the need for a comprehensive comparative analysis. This study conducts a qualitative synthesis and thematic comparison of leading cybersecurity governance frameworks to evaluate their effectiveness in ensuring compliance and resilience within IoT-enabled environments. Each framework was examined across recurring governance domains, including risk management orientation, scalability, control comprehensiveness, interoperability, and contextual adaptability. The analysis integrated findings from scholarly literature, international standards documentation, and expert reports, allowing the identification of emergent patterns, convergences, and gaps in the frameworks' conceptual foundations and implementation practices. The findings indicate that NIST CSF provides a highly flexible, sector-neutral architecture fostering adaptive governance, whereas ISO/IEC 27001 offers formalized, audit-oriented structures suitable for organizations emphasizing certification and policy compliance. The CIS Controls framework emerges as practical and accessible, favoring rapid implementation and community-driven updates, while ISA/IEC 62443 demonstrates unparalleled domain specificity and defense-in-depth design for industrial and cyber-physical systems. Nevertheless, all frameworks exhibit limitations when addressing IoT-centric issues such as dynamic risk contexts, interoperability among heterogeneous devices, and integration of operational and information technology governance layers. The study concludes that a composite, layered governance approach—anchored in the structural rigor of ISO/IEC 27001, the adaptability of NIST CSF, the practicality of CIS Controls, and the industrial depth of ISA/IEC 62443—can offer a more holistic foundation for IoT cybersecurity compliance.

Received: January 27, 2025 Revised: March 29, 2025 Accepted: June 28, 2025

Keywords: Internet of Things (IoT); Governance structures; Cyber threats; Security incidents; IoT deployments; Security controls; Attack surface

1. Introduction

Several industries have been revolutionised by the IoT, and how organisations function has also been altered, thus bringing about a new dawn of enhanced opportunities and business processes [1]. The IoT has become one of the key components of modern business today because of its high growth rate and its ability to provide connectivity and data processing that increase efficiency and create new opportunities [2]. It is the interconnection of smart devices, sensors, and systems that has created new opportunities and transformed various industries into Industry

4.0 [3]. However, like any other disruptive technology, there has been a set of cybersecurity threats that should be detected and mitigated as early as possible [4]. The IoT is also an extremely large and highly sensitive ecosystem, naturally, which companies have to navigate through due to its enormous number of connected devices and data exchange [5]. Firms are extremely susceptible to various forms of cyber-attacks that can exploit the biased character of the offered interconnectedness to expand the possible attack vectors [6]. The issue of security is further complicated as the IoT is extended into other sectors in manufacturing, smart homes, healthcare, and transport [7]. The IoT has expanded at a highly rapid rate and has internalized the introduction of appropriate security practices, where organizations are struggling with the new millennium cyber threats [8]. The necessity to comply with cybersecurity in the Internet of Things, therefore, has become a burning problem in business organizations on a global scale. An IoT ecosystem cyber-attack can be devastating to the IoT ecosystem of the large infrastructures and potentially the lives of the masses, other than the affected organizations. To solve these problems and ensure the IoT environment is not vulnerable to cyber threats, organisations should ensure that they are more integrated and systematic in their approach to cybersecurity [9]. These models of governance offer a strategic guideline to the organisations in order to develop effective cybersecurity practices and procedures that are suitable to the organisational setting of their implementations of the IoT [10]. There is a possibility that organisations can develop a robust security system that is capable of reacting to the dynamic threat environment by the creation of good governance systems [11]. These models provide a comprehensive design of cybersecurity solutions in the era of IoT with policy design, risk evaluation, and incident response that extends beyond technology. By doing so, it can be stated that the IoT world and its complexity can be managed by businesses through proper governance frameworks that will ensure their cybersecurity and safeguard the IoT devices, networks, and data [12]. The overview of IT governance is presented in Figure 1.

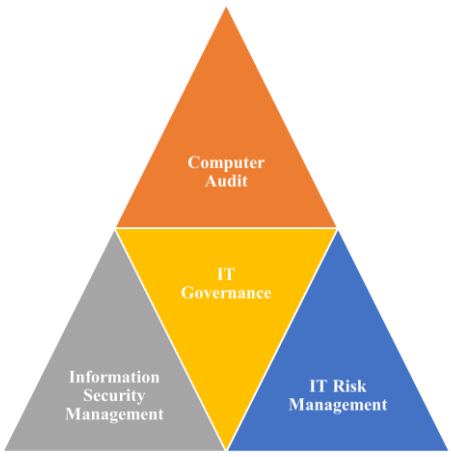

Figure 1. Overview of the ITG

Background and Significance

The Internet of Things has emerged and significantly transformed the environment of existing businesses, and changed it radically as a new paradigm. The IoT is a novelty, which centers on the integration of sensors, connectivity, and intelligence into ordinary equipment, apparatus, and objects to facilitate them to communicate with one another easily, gather data, and exchange information [13]. With such a networked network of smart devices, a whole new world of previously unseen possibilities and efficiency has begun and is no longer a novelty [14]. The IoT has revolutionized numerous sectors, such as the manufacturing industry, healthcare industry, agriculture industry, and transportation industry. The companies have acquired another chance to facilitate processes, customer satisfaction, and organizational efficiency [15]. Real-time data from connected devices helps businesses to make quick decisions on the go, which enhances operational flexibility and strategic planning. It has been realized that through the IoT, businesses have realized a lot of benefits in terms of productivity and efficiency. Integration of automated workflows as well as machine-to-machine communications has enhanced the speed of operations and reduced operating costs by reducing human intervention. The huge network of smart devices that constitutes the IoT has also made remote monitoring and control possible, thus allowing companies to monitor and control their operations and assets from any location, and therefore expand and go international [16]. Moreover, the IoT has been enhanced by the integration of AI and ML to make it even better. Through integrating the data from IoT sensors with AI analytics, companies have been able to implement predictive maintenance, anomaly detection, and personalised customer communication, which in turn, enhance customer satisfaction and loyalty. Furthermore, the IoT has been found to hold great potential in the enhancement of supply chains, real-time

identification and monitoring of assets and products, and effective utilization of resources. Because of the increased visibility into supply chain operations, lead times have been shortened, inventory management has improved, and waste has been decreased, promoting environmentally friendly behaviours. The need to make the IoT secure and seamlessly integrated is increasingly gaining importance as organisations keep on tapping into the massive potential of the IoT [17]. Although the advantages of the IoT are incomparable, it also presents a new range of cybersecurity threats to businesses. Interoperability of devices and data exchange provides bad actors with loopholes to exploit weaknesses as a disguise to carry out advanced cyberattacks. The necessity to solve the issue of cybersecurity concerning the IoT cannot be stressed. Any security breach may cause serious consequences in the IoT ecosystem, and the possible risks include data leakage, service failures, financial losses, and even a possible threat to population safety. The companies utilizing the IoT are advised to make sure that the information obtained is secure, that the systems that are considered important are upheld, and that the companies retain the confidence of their customers. [18].

Cybersecurity Challenges in the IoT Era

The IoT has also turned out to be the future of limitless opportunities, but it is also filled with numerous cybersecurity problems that cannot be underestimated. The IoT is merely a network of interconnected devices that are densely spread across industries and permeate every sphere of modern life. The large scale of the IoT makes the IoT vulnerable to a huge attack surface, which is vulnerable to a plethora of cyber-attacks, such as smart homes and autonomous vehicles, industrial control systems, and medical equipment. One of the most pressing problems is the increased exposure to cyber risks due to the interconnection of the IoT [19]. All connected devices become potential targets of bad actors who seek to use vulnerabilities and gain access to confidential data or vital systems. The vast number and variety of connected gadgets present a difficult challenge to companies that want to secure their IoT environments in their entirety. The common strategies are not always enough in the case of cybersecurity of IoT. The reason is that the security environment is varied because of the nature of devices that may be either old models or new models of technology. The IoT devices mentioned above have very limited memory and processing capabilities, and it is difficult to introduce strong security measures. Additionally, software updates and fixes do not necessarily have to be easily accessible, and leave the devices vulnerable to known threats longer. Moreover, the development of the IoT and its rapidity make cybersecurity an issue. This is because there is always continuous deployment and connection of devices in the IoT environment, and the possibility of frequent changes to the configuration [20]. The continuous development of the IoT means that a proactive and dynamic approach to cybersecurity is required, which can easily detect and respond to new threats. These challenges can be addressed through the creation of an elaborate strategy for cybersecurity compliance to guarantee the safety and privacy of IoT solutions. The organisations should therefore implement a proactive and preventive layered security. Some of the measures that are encompassed in this strategy include the use of strong encryption, safe authentication procedures, and intrusion detection systems.

Also, security integration should be among the concerns in designing IoT devices for businesses. Cybersecurity considerations can be incorporated into the development process since the security by design principles allow the vulnerabilities and weaknesses to be omitted. In order to identify and rectify such issues as soon as possible, security audits, security checks, and security penetration testing should be carried out periodically. As for the non-technical measures, the IoT cybersecurity compliance pays special attention to the awareness of the end-users and other interested parties. In awareness campaigns and training sessions, users can be prepared to notice malicious activity and report it, thus reducing the likelihood of human mistakes and social engineering attacks [21]. The entire sector needs to be collaborative, and information sharing is crucial. Cooperative initiatives are less difficult to spread threat intelligence and best practices because IoT is a trans-industrial and trans-legal entity. Towards a common understanding of cybersecurity compliance in the context of the IoT age, the industry standards and guidelines may be used.

Several issues that threaten the security and privacy of IoT solutions are depicted in Figure 2 as the cybersecurity issues of the IoT age. To begin with, as has been mentioned, the IoT has a vast number of potential entry points, which are connected devices, sensors, and networks. Moreover, the level of security is hard to standardize because the IoT devices are very diverse in terms of form, size, operating systems, and protocols. Since some IoT devices may not have the processing capabilities and memory to handle all the functions and have limited resources, the manufacturers may decide to compromise and make the IoT devices vulnerable. Furthermore, it is impossible to ensure that all IoT devices are protected to the same extent because there are no specific protocols used in their security that can be followed to the letter. One of the problems of insecure communications is that they can lead to leakage of data and unauthorized access to the information due to poor encryption, no authentication, and open data transfer channels. Many IoT devices have outdated software because some devices may not receive frequent software updates, and this makes them vulnerable to specific security risks that hackers can easily take advantage of. The nature of the IoT devices as the means of collecting and analyzing large volumes of personal data has raised the issue of privacy, which raises questions of what can be done with this information and how it can be

abused. We also have physical security threats, which should also be taken into account, especially in the SCADA systems and in the healthcare sector, where a hacker can physically get into the IoT devices. Their DDoS attacks are brought about by hacking the IoT devices and subsequently using them to make very large attacks that impact services and networks. This problem of securing the IoT ecosystem is compounded by the fact that the IoT devices can join botnets, be infected with malware, and collaborate to commit evil.

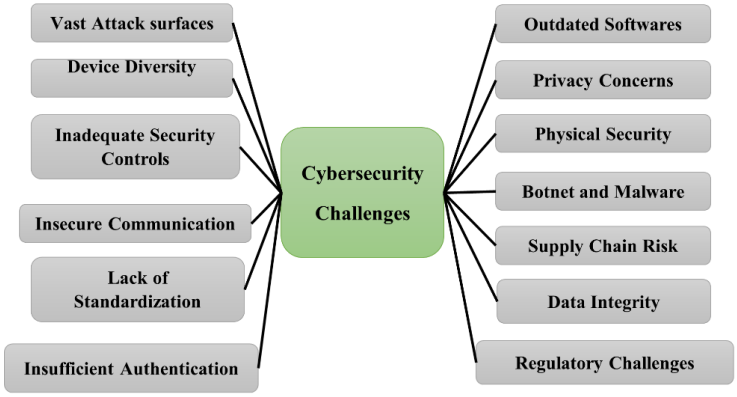

Figure 2. Cybersecurity Challenges in the IoT era

The IoT industry is a young one and is rapidly expanding, and this is the reason why the regulation of this industry is always evolving. Supply chain risks are also quite critical because they may compromise the security of the entire IoT landscape by bringing insecure components or applications. The IoT security is extremely reliant on the level of awareness among the users, since the absence of the same may lead to the development of vulnerabilities like poor passwords or unprotected settings. Integrity of data should be ensured to prevent such manipulations or fraud, which can be disastrous in the use of IoT. Moreover, the IoT devices use poor or inherited passwords, which present the issue of poor or no authentication, thus giving the attacker an easy access point into the system. These are the cybersecurity concerns that ought to be looked into to offer a secure and safe implementation of the IoT devices. In order to minimize risks in the IoT environment, one will need to implement sufficient security practices, promote the involvement of key actors, and enhance the level of cybersecurity on a regular basis.

The Role of ITG Frameworks

In this respect, the importance of implementing ITG frameworks in addressing the dynamics and the growth of cybersecurity threats cannot be overestimated. This study will thus make sure that enough focus is given to these frameworks and the several roles that these frameworks can assume in solving the multifaceted issues that are caused by the cybersecurity of the IoT. The process of cybersecurity must be methodical and intentional because more organizations have now understood that the IoT is a groundbreaking technology [22]. The ITG guidelines are critical in assisting organisations in addressing the problem of providing sufficient security to their IoT environments. These frameworks are the road maps, which entail the appropriate plan and the step-by-step approach of designing and executing effective cybersecurity that may be applied in the framework of the IoT. The ITG framework may be useful to organisations because it assists the organisation in tackling the problem of IoT security methodically. These frameworks are made up of various elements, which include best practices, policies, procedures, and guidelines, to manage the risks and attain the security standards [23]. This is one of the main reasons why ITG frameworks exist: to define precise and measurable goals that are in line with the company's security goals and overall business strategy. Such strategic objectives may help organisations to form an integrated vision of the current state of their cybersecurity and focus their efforts on a common goal. These frameworks offer a logical structure for developing broad policies and procedures that will encompass the IoT environment. Policies describe the guidelines and standards that define the proper deployment, usage, and management of IoT devices and information. Whereas procedures explain the flow of action to be followed while performing security audits, responding to security incidents, and other activities [24]. In particular, it is necessary to note that duties and responsibilities are assigned to organisational departments and individuals through the implementation of ITG frameworks. The frameworks help to make decisions, to coordinate, and to communicate in case of changing risks, as they define who is doing what in the field of cybersecurity. Risk management is one of the components that have been integrated into governance systems. These frameworks prompt businesses to conduct extensive risk assessments to identify and prioritize possible IoT deployment-specific risks and vulnerabilities. Organisations can therefore optimally allocate resources for the setting up of security measures where most required by

identifying threats [25]. Security controls are another component of ITG frameworks. These controls include the measures that are put in place at the organisational and technical level to ensure the safety of the IoT ecosystem against the dangers that prevail on the internet. They may include authentication, access controls, network segmentation, and encryption protocols, among others [26]. Event reaction plans are also highlighted as an aspect of governance frameworks, which means that organisations should be ready for reactions regardless of how proactive they are. Organisations are recommended to come up with clear processes of identifying, responding and recovering from security threats. This way, normalcy can be restored and the effects of breaches can be significantly minimized with prompt actions. Monitoring and assessment processes are also highlighted by governance frameworks as important concepts [27]. Real-time monitoring also enhances the ability of an organization to prevent the aggressors from inflicting severe harm since it enables the detection of deviation and possible threats as they occur [28]. Thus, the assessments and audits of the cybersecurity measures are conducted periodically to ensure that the organization's protection is still adequate and effective.

Research Objectives and Contributions

Therefore, the purpose of this paper is to evaluate the applicability of the current ITG frameworks for promoting cybersecurity compliance in the IoT environment. This paper reviews other frameworks as an attempt to assist organisations in selecting the most appropriate governance structure that fits their needs by providing them with all the requisite information.

The research questions that will guide this study in the light of the increasing complexity of cybersecurity in the era of the IoT are as follows:

RQ1. Which leading frameworks of IT governance, i.e., NIST CSF, ISO/IEC 27001, CIS Controls, and ISA/IEC 62443, conceptualize and operationalize the governance of cybersecurity in IoT-enabled ecosystems?
RQ2. What are the thematic differences and commonalities between these frameworks when dealing with crucial cybersecurity areas, including risk management, incident response, monitoring, and compliance assurance?
RQ3. To what extent do existing governance frameworks accommodate IoT-specific requirements, including device heterogeneity, interoperability, and real-time risk management?
RQ4. What are the conceptual gaps and integration opportunities of a qualitative synthesis of these frameworks to create a single governance model to determine the compliance of IoT cybersecurity?
RQ5. What is the proposal of a hybridized approach to governance that can enhance the resilience of cybersecurity and policy alignment in multi-layered IoT infrastructures?

The study has theoretical and practical implications for the areas of cybersecurity governance, IoT compliance, and policy alignment:

- Comprehensive Qualitative Synthesis: The study employs a qualitative, thematic synthesis approach to systematically analyze and interpret the conceptual foundations, structure, and domain coverage of NIST CSF, ISO/IEC 27001, CIS Controls, and ISA/IEC 62443 within the context of IoT security governance.
- Framework Comparison through Thematic Lenses: It develops a cross-framework comparative schema that categorizes each framework based on key governance domains— identifying risks, protecting, detecting, responding, recovering, scaling, and complying- theming convergence and divergence.
- Identification of IoT-Specific Gaps: The analysis exposes limitations of traditional IT governance frameworks in addressing IoT-specific issues such as device lifecycle management, real-time analytics, interoperability of cyber-physical systems, and secure data provenance.

The remainder of the paper is structured as follows: Section 2 will provide an in-depth literature review, showing past research on cybersecurity governance and the current IT governance models applicable in the IoT age. Section 3 describes the problem statement, identifying the lack of research and the necessity to carry out a comparative assessment. In section 4, the author has addressed the major elements of Information Technology Governance (ITG) that are the analytical basis of the present research. Section 5 gives a detailed comparative study of the chosen frameworks, NIST CSF, ISO/IEC 27001, CIS Controls, and ISA/IEC 62443 on the basis of the thematic synthesis and qualitative interpretation. Section 6 expounds on the implications of the findings on a practical level with a particular focus on their applicability to policymakers, practitioners, and organizations adopting IoT-based cybersecurity measures. Lastly, Section 7 sums up the research by concluding on the key findings, limitations, and recommendations for future research.

2. Literature Review

The literature indicates a wide area of concern in the field of IoT cybersecurity, including risk management, best practices in cybersecurity, legal implications, and economic implications. The studies offer helpful facts regarding the minimization of the threat of cyber-attacks and ensuring that the IoT technologies are created safely and ethically.

Lee (2020) examined the cyber risk and IoT cybersecurity tool control frameworks in the study [29]. The paper then suggested the four-layer model of dealing with cyber risk within an IoT setting. This paper allocates the financial resources of a high number of IoT cybersecurity projects by using a linear programming model.

To ensure high security of these interconnected devices, Amoo et al. (2024) [30] evaluate the best practices of ensuring cybersecurity hygiene in the IoT environment and the issues that should be considered. The vulnerabilities of the IoT devices and their impact on the overall system security and potential solutions to enhancing cybersecurity hygiene in the IoT environment were also discussed in this study.

Stoyanova et al. (2020) [32] presented a systematic review on the Internet of Things (IoT) forensics with a focus on the growing complexity of protecting and investigating interconnected IoT systems. Their work categorized the issues that are emerging as data acquisition, evidence preservation, and cross-domain interoperability, and highlighted the lack of standardized governance mechanisms of forensic preparedness in IoT infrastructures. The authors emphasized that current cybersecurity models are frequently unable to consider forensic-by-design as an important element, although forensic techniques have developed, and such principles are essential to ensure compliance and traceability in distributed systems.

In the same way, Kandasamy et al. (2020) [33] performed a holistic review of IoT cyber risk assessment models, determining the most important risk vectors, prioritization approaches, and ranking procedures. Their results showed that there were major differences between risk assessment frameworks in the scalability, data sensitivity handling, and responsiveness to attack surfaces unique to IoT. The paper highlighted the importance of governance models that could dynamically match cybersecurity risk assessment with heterogeneous device ecosystems. Taking this argument further into the legal and regulatory aspect, Babikian (2023) [34] examined the changing nature of cyber law in the light of the legal issues that accompany data privacy, digital forensics, and cross-border enforcement of cybersecurity. The paper highlighted that the disjointed strategies of legislation across jurisdictions pose significant challenges to the development of cohesive IT governance in the IoT settings.

Table 1 provides a comprehensive overview of major Information Technology Governance (ITG) frameworks relevant to cybersecurity and Internet of Things (IoT) compliance, comparing their origins, objectives, structural components, strengths, limitations, and contextual relevance. The NIST Cybersecurity Framework (CSF), developed by the U.S. National Institute of Standards and Technology (NIST), is one of the most widely adopted governance models emphasizing a risk-based and adaptive approach to cybersecurity. It is designed based on five main functions, which include Identify, Protect, Detect, Respond, and Recover, which together aid in the enhancement of resilience and regulatory alignment. Its major advantage is that it is flexible, scalable, and cross-sector, and thus organizations can implement it depending on their risk appetite. Nevertheless, it is still paper-intensive and expert-intensive, with minimal automation and explicit IoT device-level instructions, but can be modified to smart and connected contexts [3233, 36, 43].

Table 1: Literature Review Summary of Major ITG Frameworks for Cybersecurity and IoT Compliance

Framework	**Origin / Governing Body**	**Core Objectives**	**Key Components / Domains**	**IoT Relevance**
NIST Cybersecurity Framework (CSF) [32] [33] [36]	NIST, U.S. Department of Commerce, 2014, 2018, 2023	Risk-based approach, resilience enhancement, cybersecurity posture improvement, regulatory alignment	Identify, Protect, Detect, Respond, Recover, Implementation tiers, Profiles	Moderate, adaptable to IoT, limited device-specific controls, compatible with smart systems
ISO/IEC 27001 (ISMS) [38] [39] [40]	ISO and IEC Joint Standard, 2013, updated 2022	Information Security Management System (ISMS), confidentiality, integrity, availability, certification, and audit	Annex A controls, PDCA cycle, risk assessment, governance policy, internal audit, continual improvement	Moderate, adaptable, but lacks IoT device management, weak on real-time monitoring

CIS Controls v8 [35] [42] [43]	Center for Internet Security (CIS), 2021, community-driven	Prioritized security controls, cyber hygiene, practical implementation roadmap	18 Controls, IG1–IG3 groups, asset management, data protection, monitoring, incident response	Low–Moderate, suitable for IoT baseline, lacks OT depth
ISA/IEC 62443 [37] [39] [41]	ISA and IEC TC65, Industrial Automation Security Standard, 2010–present	Industrial cybersecurity, defense-in-depth, system integrity, OT/ICS resilience	Four levels (General, Policies, Systems, Components), Security Levels (SL1–SL4), and lifecycle management	High, designed for IIoT, OT, cyber-physical systems, strong lifecycle security
COBIT 2019 (for comparison) [40] [42]	ISACA, 2019	IT governance, value delivery, performance measurement, policy compliance	Governance and management objectives, performance metrics, design factors	Low, suitable for IT strategy, not IoT operations

The ISO/IEC 27001 Information Security Management System (ISMS) is a standard, that is, jointly published by ISO and IEC, offering a formal and certifiable framework of governance to keep confidentiality, integrity, and availability of information assets. It is based on the 114 controls and the Plan-Do-Check-Act (PDCA) cycle of Annex A that provides extensive governance coverage and integration with similar standards such as ISO 22301 and ISO 31000. Its global acknowledgment and certification system makes it more credible, but its cost of implementation is quite high, extensive documentation is required, and its ability to adapt to IoT-specific contexts, including controlling devices and real-time monitoring, is low, which hinders its usefulness in dynamic IoT ecosystems [38-40].

The Center for Internet Security (CIS) Controls v8, which was launched in 2021, is a pragmatic and community-based framework that focuses on practical cybersecurity hygiene by 18 prioritized controls organized into three implementation levels (IG1–IG3). It provides a low-cost and deployable roadmap to organizations that are in need of a fast security boost. Its simplicity, community-driven updates, and compatibility with NIST CSF make it particularly suitable for small to mid-sized enterprises. However, the lack of standard certification and coverage of industrial internet of things (IIoT) and operational technology (OT) security diminishes its use in more complicated enterprise settings [35,42,43]. The framework of the International Society of Automation (ISA) and the IEC Technical Committee 65 is named ISA/IEC 62443, and is specifically directed at industrial automation and control systems (IACS). It offers a defense-in-depth architecture that is organized into four levels of hierarchy, namely General, Policies and Procedures, System, and Component, and establishes Security Levels (SL1-SL4) to quantify system assurance. The framework is industrial-specific, lifecycle-oriented, and integrates IT/OT, and is thus very appropriate to Industrial IoT (IIoT) and cyber-physical systems. It is, however, technically challenging and resource-intensive and not very feasible in non-industrial or consumer IoT settings [37,41,39].

COBIT 2019, which is upheld by ISACA, is a strategic IT governance framework that is based on delivering value, measuring performance, and adhering to policies. It specifies governance and management goals as well as quantifiable design considerations and is therefore highly useful in harmonizing the business and IT objectives at the enterprise level. COBIT provides a great deal of strategic alignment and policy management, but it does not have the technical depth of cybersecurity and is ill-adapted to the operational governance of IoT because of its top-down management perspective [41,40].

3. Theoretical Foundation and Methodology used

The giant growth of the IoT has transformed our lives, work, and relationship with technology by bringing in the era of unparalleled connectedness and interactivity. The IoT has penetrated numerous sectors such as healthcare

and transportation, manufacturing, and smart cities, and is likely to enhance the efficiency and optimisation of operations. However, the fact that they are dependent on IoT devices and interconnection has exposed organisations to various cybersecurity threats that demand proactive and premeditated efforts.

A. Understanding the Complexities and Interconnectedness of IoT Devices

The IoT ecosystem is a dynamic and constantly evolving ecosystem that offers an attractive world of innovation and connectivity. An IoT environment can be described as a sophisticated network that comprises of massive number of smart devices, sensors, and networks, and they all share information continuously. Besides that, it creates a system of unmatched convenience and efficiency, and simultaneously a set of cybersecurity issues that should be observed at any given moment. Of more importance is the fact that this networked web offers a much larger attack area. It can be a smart thermostat, a fitness tracker, an industrial sensor, or an autonomous vehicle, but all IoT devices open the possibility to become a point of vulnerability to cyber threats in the digital environment of an organisation. The advantage of such a big network is that the consequences of successful cyber-attacks are even more dismal because a single device can potentially destroy the entire system of IoT [36]. The multiple IoT tools make the ecosystem protection even more complex, as stated above. All of them are unique and different in terms of usage and necessity. Any device poses a challenge to cybersecurity experts, starting with the simple and low-energy sensors and ending with advanced and high-energy industrial control systems [37].

The implementation of effective security measures may also be a great problem in devices that have limited resources because of their small computing and memory power. This vulnerability can be exploited by hackers who might be interested in interfering with such gadgets and using them as attack platforms. The second issue is that no universal security standards can be applied to all IoT devices, and thus, it is hard to ensure high and consistent security standards. Another aspect that makes the picture even more difficult is the integration of legacy technologies into the IoT environment. Some of the existing hardware and infrastructure might have been developed without the aspect of security as a core consideration, which makes them easy targets for modern, complex cyber-attacks. Due to the fact that IoT has a large number of communication protocols, there can be some security loopholes because of compatibility and interconnectivity issues [38]. It may be challenging to achieve the correct balance between security and usability of the devices and networks. The IoT environment is constantly and steadily growing, which adds to the challenge. The threat profile evolves over time due to the introduction of new technologies and gadgets into the environment. The cyber attackers are always smart enough to get into the newly identified vulnerabilities and loopholes, which makes it very important to always be on the lookout for new threats in the market and be able to come up with new ways of protecting the systems. This is why IoT cybersecurity in this setting must be grounded on the principles of constant monitoring, threat intelligence, and proactive defense. Organisations must be ready to adapt to new threats and risks at any given time and make sure that security controls are dynamic in relation to the ever-changing IoT environment [39].

B. Discussion on the Importance of Governance Structures

It is for this reason that the issue of strong governance frameworks is highly significant, especially given the increasing susceptibility to cyber threats because of the changing IoT landscape. These governance frameworks are beneficial to safeguard businesses and their complex IoT systems as they provide a coherent and comprehensive approach to address all the issues associated with IoT security. These governance frameworks are set after a good and strategic plan to help organizations that wish to have a good business plan in the area of cybersecurity. These plans begin with the concrete cybersecurity goals that are suitable for the general characteristics and the distinctiveness of the IoT assets of the organizations. These frameworks ensure that cybersecurity is integrated as a goal by linking these objectives to the overall mission and business strategy of the organization. First of all, governance structures intentionally allocate certain tasks and obligations in an organisation to individuals or groups. This division of labour ensures that cybersecurity is not only an idea but an area of responsibility and promotion by the right people [40]. This clear division of labour is beneficial in ensuring that there are no gaps and that there is a solid structure in place for cybersecurity operations by eliminating silos and promoting a culture of collaboration and awareness across the different tiers of an organisation. The risk management aspect of these governance structures works as a safeguarding system against possible risks and problems [41]. Risk analysis and assessment help organisations to understand the risk better and therefore identify which areas require more security. Potential vulnerabilities and failures can also be predicted and prevented because organisations can also identify what the vulnerabilities in the IoT environment are and what their impact is, so that they can prevent such failures in the future. The governance structures assist in the enforcement of the appropriate security policies in a manner that there is a barrier to the different online threats. These measures involve a range of activities such as the use of multi-factor authentication, an access management system, and encryption algorithms. With the help of such a security feature, the IoT environment is insured against such threats, and the stability of the connected devices is ensured. The applicability of the governance structures can be seen in the way the incident handling plans are well-organized in times of crisis and security issues. These response plans, as discussed in the framework in detail, provide organisations with a roadmap of how to respond to cyber threats

in a rapid and efficient way [42]. Some of the ways through which organisations can alleviate the impact of breaches, safeguard their information and infrastructure, and manage to restore order are by means of the mechanisms that enhance the capability of early detection, separation, and recovery of security threats. In addition, another attribute of all the systems of governance is the continuous assessment and scrutiny. By being vigilant at all times and undertaking frequent security audits, organisations can easily identify new threats and incursions within the organisation in real time [43].

C. Research Design

The research design used in this paper is a qualitative research that follows an interpretivist paradigm as it focuses on the investigation of meanings, interrelationships, and conceptual foundations of key ITG frameworks. The qualitative orientation can be used to comprehend the conceptualization of the Internet of Things (IoT)-enabled governance frameworks (namely NIST CSF, ISO/IEC 27001, CIS Controls, and ISA/IEC 62443) to cybersecurity compliance in a more profound way. The research does not aim to quantify effectiveness through numerical scoring; rather, it seeks to interpret thematic patterns, policy orientations, and contextual adaptability through comparative content analysis and thematic synthesis. The design incorporates three stages of methodology. To capture the development of cybersecurity governance, the systematic review of the documents involved a review of peer-reviewed publications, documentation of standards, white papers, and industry guidelines in the period between 2018 and 2025. Second, the thematic categorization was applied to group the framework attributes into the governance domains, which comprised risk management, policy structure, scalability, interoperability, and compliance monitoring. Third, an interpretive synthesis process was used to determine convergence, divergence, and contextual gaps across frameworks with a focus on their implications for IoT cybersecurity. The study design is compatible with the exploratory character of the study, and the intention to generate an integrative conceptual insight, but not to come up with prescriptive measures.

D. Scope

The area of the proposed study is limited to the comparative analysis of the major global IT governance models with particular reference to their relevance to the sphere of IoT cybersecurity. The reviewed frameworks include NIST Cybersecurity Framework (CSF), ISO/IEC 27001, CIS Controls, and ISA/IEC 62443, and they have been chosen because of their international popularity, cross-sector applicability, and proven application in cybersecurity governance. The paper addresses the conceptual, structural, and operational aspects of these frameworks and how they align with the changing needs of IoT-based infrastructures, which are heterogeneous, real-time, and cyber-physical interfaces. The study does not assess the framework performance using organizational case studies or empirical tests; rather, it focuses on policy design, structural flexibility, and theoretical synthesis. The review of official standards documentation, academic literature, and domain-specific commentaries will be included in the analysis to maintain triangulation and reliability. Its geographical focus is the worldwide one, including international adoption views, but the discussion mainly mentions the situations when the IoT implementations have already developed, including industrial automation, smart cities, and critical infrastructure industries.

E. Data Analysis and Synthesis

Data analysis was done under the qualitative synthesis method, where thematic analysis was used in combination with comparative interpretive synthesis to generate insights using textual data. All document framework publications, academic articles, and regulatory guidelines were imported into a qualitative analysis environment to be coded and categorized. The data were systematically reviewed, coded, and clustered into themes reflecting the recurring domains of governance and the following themes were identified in accordance with the six-step thematic analysis approach suggested by Braun and Clarke: (1) risk management orientation, (2) control comprehensiveness, (3) scalability and flexibility, (4) interoperability and compliance mapping, and (5) IoT readiness and contextual adaptability. A cross-framework synthesis matrix was then created to compare the chosen governance models in these themes and to find intersections, complementarities, and limitations. The interpretive synthesis focused on conceptual congruency and governance philosophy as opposed to statistical performance. The constant comparative analysis was conducted on each theme, which allowed identifying convergence patterns, including common principles of risk-based governance, and divergence patterns, including the difference in the formality of audit, scalability, and IoT-specific provisions.

4. Components of ITG Frameworks

The ITG frameworks are important in helping organisations in the complicated environment of the IoT to develop effective cybersecurity. These frameworks address many crucial issues that, in combination, make up a comprehensive and strategic approach to the security of IoT.

Figure 3 illustrates the most prominent aspects and functions of an ITG framework that is adjusted to the security of the IoT. It will strive to develop a comprehensive and efficient cybersecurity system and establish a setting in which IoT devices and data transmission will be secure. The first action in this connection. Is to “Define Strategic

Objectives. This involves the establishment of clear, specific, and consistent cybersecurity goals that are aligned with the general business strategy of the organization. It entails the study of the IoT environment, important assets, risks, and opportunities. At this point, one should realize how cybersecurity affects business processes and regulations. The second step of defining the strategic goals is to develop comprehensive policies, procedures, and controls of IoT security. To do this, the documentation of guidelines and standards of different IoT applications should be created. Such policies make sure that every cybersecurity project is consistent with the strategic plan of the organization and is not illegal. They are device management, incident response, access control, and data protection, among others. The third exercise will be Concerns and Responsibilities to Manage IoT Security. During this step, there is a need to determine the roles and the responsibilities of various stakeholders within various departments, since cybersecurity is the business of everyone. It is also worth mentioning that the IT department can implement access control and network monitoring, the operations department can implement physical security, the legal department can implement privacy policies and compliance, and the human resource department can implement training of the employees [44]. The given division of responsibilities contributes to the culture of responsibility and enables approaching the issue of IoT security as a systemic one. The framework components include Continuous Monitoring, Incident Response Plans, and Risk Management. Risk management is required in the case of the IoT due to the continuously changing risks and threats. IoT risk assessment demands that organizations determine, evaluate, and prioritize risks that are related to their IoT implementations. Incident response plans are a viable method of addressing cybersecurity attacks in case of any security threats. To identify and neutralize emerging threats in the shortest time possible, the system is actively monitored by actively scanning the system logs, network traffic, and activity of IoT devices.

This IoT security ITG framework provides an orderly method to improve the security measures. Following these recommendations and enacting strict policies and measures, organizations will be able to secure sensitive data, improve the credibility of the IoT environment, and avoid all types of cyber threats.

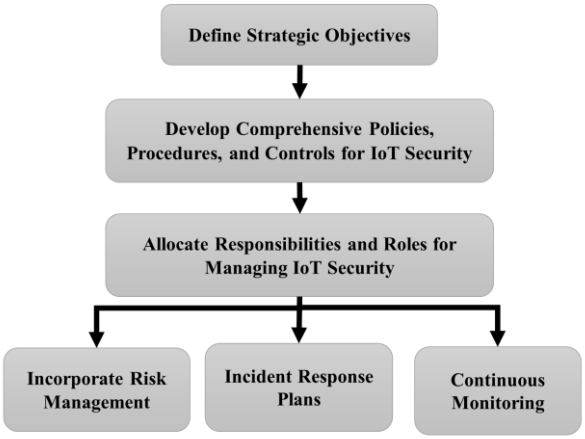

Figure 3. The key steps and components of an ITG Framework

F. Defining Strategic Objectives for Cybersecurity in the IoT Environment

The basis of a sound cybersecurity strategy in the constantly changing and integrated world of the IoT is to develop clear and achievable goals that support the overall business goals of the organization. These strategic objectives are the roadmap of the organization as far as cybersecurity is concerned, in order to be specific, flexible, and relevant to the opportunities and threats of the IoT environment. The recognition of the IoT environment of the organisation is the initial step towards effective cybersecurity goals. This is done by identifying and mapping key resources that include sensitive data, patents, critical structures, and connected consumer devices, among others. Knowing the degree of priority of these assets will help you know the degree of protection and investment they should be given. In addition to that, the evaluation will focus on threats and risks that could be present in the IoT environment. Through continuous evaluation of the vulnerabilities, the organizations are in a position to seal the gaps before the risky people can exploit them. The research has taken into account some factors, such as the communication protocols that will be employed, the type of IoT devices, and risks of data leakage or system compromise [45]. The strategic cybersecurity objectives must be aligned with the overall organizational business objectives to ensure that the commercial objectives of the company are achieved. To this end, it is essential to understand the impact of cybersecurity on the fundamental business operations, the confidence of the clients, and the reputation of the company. Irrespective of whether the main objectives are to improve customer satisfaction, innovation, or compliance with the industry standards, the specific strategic objectives should be aligned with and

supplemented by these more business-wide objectives. Strategic goals are also determined by taking into account market needs and legal provisions of the industry in which the organization operates, thereby ensuring that the developed IoT environment meets the data protection laws, privacy, and security regulations of particular industries. These rules keep the company out of legal trouble and, at the same time, increase the trust of the stakeholders and the customers. Cybersecurity goals can be specific and measurable, and they can be defined with an understanding of the organization's IoT environment, risks, objectives, and compliance requirements. These objectives must be SMART, i.e., specific, measurable, realistic, relevant, and time-bound, in order to enable organisations to effectively gauge their performance.

Strategic goals are carefully created to improve cybersecurity and protect the integrity of connected devices in the changing environment of the IoT ecosystem. These include a vast array of important topics, and all of them are aimed at ensuring the protection of private data, at the prevention of unauthorized access, and at shielding the IoT communication channels from possible threats in the online environment. The protection of data, which guarantees the confidentiality, completeness, and availability of the sent and processed data, is one of the most significant focuses. During the device onboarding, authentication and authorisation measures to restrict the access of the IoT network by unauthorised parties are enforced [46]. To minimize security risks throughout the device's lifecycle, proper means of registering, deregistering, and decommissioning the device have also been developed. Higher levels of encryption, segmentation of the network, and intrusion detection enhance the network protection and increase the total safeguard against cyber threats. Since prevention of possible attacks is the best form of defense, constant review and fixes on possible loopholes in the IoT devices and networks are accomplished. In order to respond to the cybersecurity threats, minimize their consequences, and quickly restore the system, strong incident response procedures are established. Also, the practice of security awareness and the constant reinforcement of cybersecurity training prepare the users and the staff to act on any potential threats. Thus, organisations may further enhance the security of the IoT environment and create a solid and secure base for IoT devices and data interactions by pursuing these strategic objectives continuously [47].

The strategic objectives become the guidelines for decision-making, resource allocation, and the process of putting in place security measures once these have been formulated. These are the goals that will help businesses in making proactive steps in the new threats and adapt to the dynamics of the IoT environment.

G. Development of Comprehensive Policies, Procedures, and Controls for IoT Security

As the IoT is ever-evolving, it is essential to have a sound base of cybersecurity in preventing various threats to organisations. ITG frameworks can be rather helpful in creating effective policies, procedures, and controls oriented to the needs of IoT security. These mandated documents provide specifications, standard procedures, and a viable action plan to protect the domain of the IoT and have an assuring and sound security position across the organization.

Policies: Establishing Security Guidelines for the IoT

The policies form the foundation of the governance system of IoT security. These standards cover all aspects of the implementation of the IoT and have many security recommendations. Such regulations establish the stance of the organization regarding cybersecurity matters, including device management, incident management, access control, and data protection. They are prepared to the letter to meet the strategic plan of the framework, legal requirements, and standard operating procedures. As an example, access control policies are defined in terms of how and when access to IoT devices and their data is granted or denied. Due to the strict data protection laws, data privacy rules define how the collected information through IoT devices should be processed, stored, and shared. IoT device management policies describe how IoT devices are to be registered, authenticated, and managed in a secure manner throughout their life cycle. Policies are beneficial to employees, contractors, and stakeholders because they provide a guideline for best practices by setting security rules in clear terms. They support the importance of cybersecurity in all aspects of IoT processes by promoting security consciousness and responsibility among the members of the organization [48].

Procedures: Implementing Standardized Security Processes

While rules prescribe what has to be done in the IoT environment for security, procedures provide comprehensive guidelines on how the security tasks are to be accomplished. These complex procedures ensure that the consistency and effectiveness of the organization's cybersecurity measures are well-protected. Procedures decrease the amount of human influence and remove uncertainty, which enhances the security position. In order to ensure that only the right devices are allowed to connect to the network, there might be some authentication and authorization process when adding new IoT devices to the network. The consequences of security incidents on the organisation would be minimised through the detection, containment, and prevention of cybersecurity breaches as depicted by incident response processes. It enables the employees to be armed with adequate knowledge and self-confidence to deal

with emergent security issues through documented procedures. They reduce the complexity of the security business, enabling organizations to manage their IoT environment and respond to emerging threats effectively.

Security Controls: Bolstering IoT Defenses

The security measures within the context of the governance framework serve as the first layer of protection against possible threats in the IoT environment. Such measures are organisational and technical that help enhance IoT security and protect the systems from intrusions and cyber threats. The technical security controls may include: use of multiple factors of identification to enhance the security of accessing IoT assets, use of subnets to isolate IoT assets from public networks, and use of secure protocols to enhance the security of data exchanges between IoT assets and servers. Some of the organisational security measures include: the constant updating of software and patches, programmes that educate the staff on the importance of security, security checks to ensure that all staff are following the rules and regulations, and employee training. The following is a list of measures that organisations can take to minimise the chances of successful cyber invasions and data breaches regarding IoT.

H. Allocating Responsibilities and Roles for Managing IoT Security

In the rapidly growing and interconnected IoT environment, security is everyone's concern and touches all aspects of the organization. Thus, the governance frameworks are vital in establishing and coordinating the responsibilities of different stakeholders within the organisation regarding IoT security. Internet of Things security is a much more complex problem than that of traditional cybersecurity, which can be solved by one department or a few IT specialists. It is a multi-disciplinary process that requires the coordination of people and entities in the management, engineering, IT, operations, and legal departments. It is integrated into the broad IoT security perspective that is considered by the governance frameworks and implies the engagement of all stakeholders in the process of protecting IoT assets and data of the organisation. These frameworks define the specific responsibilities, accountability, and the scope of work for each employee and department. The IT division can be involved in managing the access control, implementing strict technological security measures, and monitoring the network for possible attacks. It is likely that IoT device physical security will be the responsibility of operations teams, who will be responsible for the right installation, maintenance, and disposal at the end of the device's life cycle. Legal departments play a significant role in the development of privacy strategies, adherence to data protection laws, and evaluation of vendors' agreements from a security standpoint. To achieve these objectives, human resources departments' primary tasks are to raise employees' awareness of security threats and provide them with the necessary training and access control measures. IoT security initiatives, cybersecurity rules, and security culture within the organisation are supported by the management leaders through backing and funding. The organizational culture of accountability is developed through the definition of responsibilities and tasks, where every employee understands the significance of their position in the creation of a safe IoT environment. This culture encourages a proactive method of securing IoT resources, reporting potential security threats in time, and adhering to security standards. The entire staff of all the ranks of the corporate structure is occupied with the issue of cybersecurity protection as a priority, and can observe possible threats and vulnerabilities and respond to them in a timely and efficient way. Governance frameworks also support cross-functional integration, which means that departmental silos do not exist. The inter-relationship of IoT implies the need to have a strong defence strategy in which different teams must communicate on a regular basis. Organisations can benefit from the specialisation of their employees by encouraging teamwork, which leads to innovative and complex solutions to security issues that encompass a number of challenges. Thus, it can be concluded that, by applying an integrated approach, it is possible to enhance IoT security, protect valuable assets and information, and create a safe and secure IoT environment [49].

I. Incorporating Risk Management, Incident Response Plans, and Continuous Monitoring in Governance Frameworks

Risk Management: Safeguarding the IoT Ecosystem

Nevertheless, risk management is essential when it comes to creating effective structures when it comes to the management of information technology in the ever-evolving landscape of the Internet of Things (IoT), where threats and threats are always lurking. These frameworks assist them in securing the environment of their IoT as well as properly distributing resources by assisting the enterprises to recognize, assess, and rank threats and vulnerabilities related to the implementation of IoT. Risk analyses in governance structures require a total analysis of the entire IoT environment. These evaluations encompass the resources, data, networks, and other potential threats with respect to their ability to affect the operations and reputation of the organisation. When risk is studied to this extent, organisations are in a position to identify their specific risk profile and easily identify areas of risk and make sound decisions on resource allocation. Risk assessments enable organisations to evaluate risks based on their likelihood and their severity in case they occur. One can easily observe that organisations are capable of allocating their attention and resources to the most critical threats in the IoT environment. This approach also has the advantage of targeting specific areas of weakness and minimizing the risks that may be present, thus making

the deployment more secure and less vulnerable. IoT is a vast and complex environment for organisations; however, they should not feel lost in it as long as they follow sound risk management practices, secure their property and information, and mitigate the risks [50].

Incident Response Plans: Swift and Effective Incident Handling

This is because when a company or an organization is attacked, there is a need to respond and regain normalcy as soon as possible. The importance of incident response plans in the governance structures is that they provide a methodological way of identifying, managing, and restoring security threats. These incident response plans are detailed guidelines on dealing with security incidents, and they are found in the governance structures. It is characterized by identification, isolation, elimination, recovery, and use of information in regards to the occurrence. This can be done to ensure that all the staff members understand their roles and responsibilities in the different stages of the incident response, and this is well recorded at every step of the process. Some of the activities that are commonly practiced include rehearsals and exercises, which entail the management of various forms of cyber events to assess the preparedness of the response measures. Such training sessions are useful not only to refresh the knowledge of the staff and show them how it is possible to react in case of an incident, but also to identify the directions that require improvement. Therefore, it is advisable for organisations to practice incident response frequently in order to enhance their capacity to respond to security incidents as soon as they occur.

Continuous Monitoring: Proactive Threat Detection

This is because the threats in IoT are ever-evolving and thus require the IoT networks and devices to be scanned periodically. Therefore, the governance frameworks assist in monitoring and security audit as well as assessment of the vulnerabilities in order to address the new threats. Real-time monitoring means the process of watching system logs, network traffic, and IoT devices' activities in real-time. It also helps the organisations to detect new trends and threats that are typical of a security breach and to counter them in real time. Another point that can be associated with continuous monitoring is the security audits and the vulnerability assessments. These tests are more related to the hardware of the IoT, the network connectivity, and the security. Auditing and assessments are useful tools that assist organisations in identifying the loopholes in the security systems and rectifying them before they become a problem.

5. Evaluating Existing Governance Frameworks for IoT Security

The significance of adequate cybersecurity management models is increasingly gaining momentum as the IoT continues to reshape the contemporary world of interconnected devices. This part begins with the systematic discussion of the current governance structures that are being applied to the compliance of the IoT cybersecurity. We shall be comparing their performance in terms of vulnerability detection, mitigation of cyber risks, and security incident management.

A. Comparative Analysis of Governance Frameworks

The ever-shifting IoT cybersecurity environment has seen the development of a range of governance frameworks to offer organisations a systematised means of protecting their IoT ecosystems. This part discusses the possibility of carrying out a comparative analysis of a set of popular governance frameworks, all of which are specialised to address the specific issues presented by IoT deployments. We also hope to understand practical lessons about the advantages and disadvantages of the NIST Cybersecurity Framework, ISO/IEC 27001, CIS Controls, and ISA/IEC 62443 to enable organisations to make informed decisions about which framework fits their particular organisational requirements and IoT needs.

NIST Cybersecurity Framework

The most widespread and universal models of cybersecurity are the NIST Cybersecurity Framework, which was developed by the National Institute of Standards and Technology (NIST) [36]. Table 1 provides a comparative analysis of the NIST Cybersecurity Framework, highlighting its major strengths, limitations, and implementation challenges. The table also contrasts NIST CSF with other globally recognized frameworks such as ISO/IEC 27001 and COBIT 5, and outlines practical recommendations for enhancing its applicability, particularly in IoT-driven and resource-constrained environments.

Table 1: Comparative Analysis: Strengths, Limitations, and Implementation Considerations of the NIST Cybersecurity Framework

Aspect	Strengths	Limitations	Implementation Challenges	Comparison with Other Frameworks (e.g., ISO/IEC 27001, COBIT 5)
Risk-Based Approach	Emphasizes risk prioritization to address the most critical threats and vulnerabilities, improving organizational resilience.	May lack quantitative risk assessment methods for advanced cyber-physical systems.	Requires skilled personnel for accurate risk identification and scoring.	More adaptive than ISO/IEC 27001, but less prescriptive in risk quantification.
Flexibility and Scalability	Applicable to all organizational sizes and sectors, including SMEs and large enterprises.	Implementation consistency may vary, leading to uneven maturity levels.	Small enterprises may struggle with scaling due to limited resources.	More flexible than COBIT 5, which has complex control objectives.
IoT Integration	Provides a broad security posture adaptable to IoT networks.	Lacks detailed IoT-specific control guidelines for device heterogeneity and protocol variations.	Difficulties in mapping IoT device lifecycles to NIST CSF functions.	ISO 27001 Annex A includes more device-oriented controls.
Documentation and Maintenance	Ensures transparency and traceability through structured documentation.	Heavy documentation burden, especially for smaller organizations.	Maintaining continuous updates is time-consuming.	Less prescriptive than ISO 27001 but still documentation-heavy.
Clear Guidelines and Framework Structure	Defines five core functions—Identify, Protect, Detect, Respond, and Recover—enabling a holistic view.	It may be too generic for organizations requiring domain-specific compliance.	Requires customization for industry-specific applications.	Simpler and more intuitive than COBIT 5's process-based structure.
Integration Capability	Compatible with other international standards (e.g., ISO/IEC 27001, GDPR).	Limited interoperability with sector-specific regulations (e.g., HIPAA, PCI-DSS).	Mapping between standards can be ambiguous.	Offers higher adaptability but is less audit-oriented than ISO/IEC 27001.

Continuous Improvement Orientation	Encourages iterative risk management and self-assessment cycles.	Relies heavily on voluntary adoption; lacks enforcement mechanisms.	Sustaining long-term engagement and periodic reviews is challenging.	More improvement-oriented than COBIT 5, but lacks formal certification.
Cost-Effectiveness	Free to access and implement, reducing entry barriers for adoption.	Indirect costs (training, audits, integration) may still be high.	Cost justification can be difficult for low-risk organizations.	Lower entry cost compared to ISO/IEC 27001 certification.
Global Adoption and Recognition	Widely recognized in the United States and internationally endorsed by regulatory bodies.	Adoption outside North America remains slower compared to ISO standards.	Varying legal and compliance landscapes hinder universal adoption.	Less globally standardized than ISO/IEC 27001.

ISO/IEC 27001

The ISO/IEC 27001 is a global standard providing the requirements of the design of an Information Security Management System (ISMS). It offers a methodical way of handling the delicate data of a business, particularly the data pertaining to IoT [37], as shown in Table 2, which outlines its strengths and limitations.

Table 2: Comparative Analysis: Strengths, Limitations, and Implementation Considerations of the ISO/IEC 27001 Framework

Aspect	**Strengths**	**Limitations**	**Implementation Challenges**	**Comparison with Other Frameworks (e.g., NIST CSF, COBIT 5)**
Global Recognition and Standardization	Internationally recognized as a leading information security management standard, facilitating global compliance and interoperability.	May not address emerging region-specific regulations such as GDPR extensions or AI ethics compliance.	Aligning regional and organizational requirements can be complex.	More globally standardized than the NIST CSF, offering certification credibility.
Comprehensive Security Controls (Annex A)	Provides 114 detailed controls across governance, physical, and technical domains, adaptable to diverse infrastructures.	Controls may not sufficiently cover IoT device heterogeneity, network latency, and real-time risk factors.	Customizing controls for IoT and operational technology (OT) environments requires deep technical expertise.	More prescriptive than NIST CSF, but less flexible for real-time IoT systems.
Systematic Risk Management	Ensures a structured approach to identifying,	Risk identification may rely on	Implementing continuous risk monitoring tools	Offers stronger risk documentation

	evaluating, and mitigating risks through the ISMS framework.	static assessments that fail to capture dynamic cyber-physical risks.	can be technically demanding.	than COBIT 5, but is less adaptable than NIST CSF.
Continuous Improvement (PDCA Cycle)	Fosters an iterative "Plan–Do–Check–Act" process for sustained cybersecurity maturity.	Audit cycles can become repetitive and administrative without tangible outcomes.	Requires skilled auditors and continuous executive engagement.	More structured improvement model than the NIST CSF's voluntary self-assessment.
Audit and Certification	Provides an official certification pathway, enhancing trust and market competitiveness.	Certification and renewal processes can be cost-prohibitive for SMEs.	Maintaining compliance under resource constraints is difficult.	Unlike NIST CSF, ISO 27001 enables formal accreditation and external validation.
Information Security Management System (ISMS)	Promotes holistic governance integrating people, process, and technology dimensions.	Focuses heavily on confidentiality, integrity, and availability (CIA) but less on IoT resilience or adaptive intelligence.	Requires cultural change across departments and strong top management commitment.	More governance-oriented than NIST CSF's operational focus.
Documentation and Policy Integration	Establishes uniform policy frameworks, ensuring traceability and accountability.	Documentation burden can hinder agility and rapid adaptation to new threats.	Policy review and version control demand dedicated resources.	Similar documentation rigor to NIST CSF, but with formalized templates.
Integration with Other Standards	Seamlessly integrates with ISO 22301 (business continuity), ISO 31000 (risk management), and ISO 9001 (quality).	Integration complexity increases when aligning multiple management systems.	Harmonizing cross-standard audits and KPIs is resource-intensive.	More cohesive integration ecosystem than NIST CSF or COBIT 5.
Cultural and Behavioral Impact	Encourages security awareness and accountability across all levels of the organization.	May fail to engage non-technical staff effectively, leading to compliance fatigue.	Requires continuous training and communication mechanisms.	More compliance-oriented than awareness-focused NIST CSF.

CIS Controls

The CIS Controls, which used to be known as the SANS Top 20 Critical Security Controls, are a set of best practices meant to help organisations improve their cybersecurity posture [38], as shown in Table 3, which highlights their strengths and limitations.

Table 3: Comparative Analysis: Strengths, Limitations, and Implementation Considerations of the CIS Controls Framework

Aspect	**Strengths**	**Limitations**	**Implementation Challenges**	**Comparison with Other Frameworks (e.g., NIST CSF, ISO/IEC 27001)**
Prioritized and Actionable Controls	Provides 18 well-structured, prioritized security controls arranged by implementation groups (IG1–IG3) based on organizational maturity.	Lacks detailed contextual adaptation for IoT ecosystems and complex operational technologies.	Mapping CIS controls to specific IoT risk scenarios can be ambiguous.	More actionable than ISO/IEC 27001 but less comprehensive in governance scope.
Focus on Continuous Monitoring	Emphasizes automation, logging, and real-time threat detection through continuous monitoring mechanisms.	May require costly security information and event management (SIEM) tools for full implementation.	Limited by infrastructure and real-time analytics capabilities in smaller organizations.	Stronger operational monitoring emphasis than NIST CSF or ISO/IEC 27001.
Community-Driven and Open Framework	Supported by a global community of practitioners, ensuring regular updates and practical relevance.	Community updates may lack formal audit or certification alignment.	Absence of formal certification reduces perceived credibility in regulated industries.	More open and practitioner-driven than ISO/IEC 27001's formalized certification process.
Ease of Implementation	Designed for quick deployment with prioritized "basic, foundational, and organizational" controls.	May oversimplify complex enterprise security needs requiring multi-layered governance.	Scalability across large enterprises requires tailored mapping with other standards.	Easier to adopt than ISO/IEC 27001 but less robust in enterprise-grade risk governance.
Cost-Effectiveness	Freely accessible and easy to interpret, offering a low-cost entry point for improving cybersecurity posture.	May lack financial modeling or ROI guidance for long-term cybersecurity investment.	Organizations might deprioritize controls without a quantitative impact assessment.	More cost-effective than ISO/IEC 27001 and COBIT 5 implementations.

Automation and Control Verification	Includes tools such as CIS-CAT Pro for automated configuration assessment and compliance verification.	Tool coverage varies across technologies and may not fully support emerging IoT protocols.	Integration of automated verification tools into legacy systems can be complex.	Provides more automation options than NIST CSF, but is narrower in coverage.
Continuous Improvement and Maturity	Encourages iterative enhancement through maturity model alignment and periodic reassessment.	Lacks explicit PDCA or continuous improvement cycles compared to ISO/IEC 27001.	Sustaining maturity improvement requires strong leadership and resources.	Similar intent as ISO/IEC 27001's PDCA, but without a formal governance loop.
Alignment and Integration	It can be easily mapped to other frameworks such as NIST CSF, ISO/IEC 27001, and GDPR requirements.	Mapping guidance can be generalized and insufficiently detailed for complex architectures.	Manual crosswalking between standards may increase implementation time.	More adaptable for hybrid compliance than COBIT 5, though less formal.
Cyber Hygiene Emphasis	Promotes fundamental security practices like asset inventory, vulnerability management, and configuration control.	May not fully address advanced threat vectors such as AI-driven attacks or zero-day exploits.	Overreliance on foundational controls may limit coverage of advanced cyber threats.	Provides stronger preventive controls than NIST CSF's broader structure.

ISA/IEC 62443

The ISA/IEC 62443 family of standards is very significant for IoT deployments in the industrial sectors since it focuses primarily on industrial automation and control systems security [39], as shown in Table 4, which summarizes its strengths and limitations.

Table 4: Comparative Analysis: Strengths, Limitations, and Implementation Considerations of the ISA/IEC 62443 Framework

Aspect	**Strengths**	**Limitations**	**Implementation Challenges**	**Comparison with Other Frameworks (e.g., NIST CSF, ISO/IEC 27001, CIS Controls)**
Industry-Specific Focus	Purpose-built for industrial automation and control systems (ICS) and operational technology (OT), addressing both cyber-physical and safety-critical environments.	Limited applicability to non-industrial or consumer IoT domains.	Requires sector-specific tailoring for utilities, manufacturing, and critical infrastructure.	More domain-specific than NIST CSF or ISO 27001, but narrower in cross-sector scope.

Risk-Based and Lifecycle-Oriented Approach	Provides systematic methods to identify, assess, and mitigate cybersecurity risks throughout system design, integration, and maintenance phases.	Implementation complexity may deter smaller organizations lacking mature risk frameworks.	Continuous alignment between system lifecycle and security assurance levels (SL1–SL4) is resource-intensive.	More lifecycle-centric than ISO 27001's ISMS, offering granular protection levels.
Defense-in-Depth Architecture	Advocates multi-layered protection integrating physical, network, application, and human-factor controls.	Lacks prescriptive technical details for rapidly evolving IoT communication protocols.	Achieving full defense layering demands high coordination across vendors and integrators.	Stronger architectural segmentation than CIS Controls, but less adaptable for cloud-native environments.
Collaborative Development and Industry Alignment	Developed jointly by ISA and IEC with input from global industrial stakeholders, ensuring real-world relevance.	Consensus-driven updates can delay the incorporation of emerging technologies.	Version alignment across ISA/IEC 62443 parts (1-1 to 4-2) requires consistent governance.	Broader industrial stakeholder base than ISO 27001 or CIS Controls.
Security Levels and Maturity Metrics	Defines clear Security Levels (SL1–SL4) enabling measurable and auditable cybersecurity maturity.	It may not directly translate to enterprise-level risk indicators used in IT frameworks.	Mapping between SLs and corporate KPIs requires technical interpretation.	Offers more measurable asset-level granularity than NIST CSF maturity tiers.
Compliance and Interoperability	Harmonizes with ISO 27001, NIST SP 800-82, and EU NIS2 directives, fostering regulatory consistency.	Interoperability challenges may occur when aligning with mixed IT/OT standards.	Integration with legacy ICS components can be technically constrained.	More aligned with NIST SP 800-82 for industrial systems than general-purpose standards.
Incident Response and Resilience	Emphasizes incident preparedness, containment, and recovery within industrial contexts.	Limited guidance for adaptive or autonomous response systems using AI analytics.	Manual response models can slow reaction times in cyber-physical attacks.	Offers deeper operational response integration than ISO 27001 A.17 controls.
Cost and Resource Considerations	Offers scalability by defining security zones and conduits, enabling selective implementation.	High initial assessment and configuration costs for complex industrial networks.	Requires collaboration among multiple vendors and integrators for certification.	More resource-intensive than CIS Controls, but provides higher assurance for ICS security.

Global Recognition	Recognized by regulators and critical infrastructure sectors worldwide as the de facto industrial cybersecurity benchmark.	Awareness remains low outside industrial automation communities.	Cross-sector training and certification programs are limited.	Stronger in critical-infrastructure adoption than NIST CSF, but less in corporate IT environments.

B. Effectiveness in Identifying Vulnerabilities

The first and foremost objective of any successful governance framework for IoT security is to be able to detect threats within the intricate IoT environment. In this regard, the framework should be comprehensive and ambitious in the identification of such risks, which will then guide the firms to fully secure their IoT networks against cyber threats. At this point, the crucial aspects that define the degree to which the governance structures can expose the IoT vulnerabilities need to be taken into consideration. Risk assessments are a basic need of good governance systems. These tests, considering the assets of the IoT environment, information, and the necessity of its implementation, are essential to define the risks since they investigate the probability and impact of the threats. It can be useful for organisations to focus their security efforts on areas that need it most of the time by categorising the likelihood of the possible hazards. There are also some guidelines that have been set by various governance frameworks, and these include the fact that IoT networks and devices should be scanned for vulnerabilities from time to time in a bid to prevent such incidents. Vulnerability scanning technologies make sure that the Internet of Things infrastructure is scanned for any vulnerabilities and misconfigurations, and for any outdated firmware. The most important reason why organisations should identify their vulnerabilities is that it helps them to mitigate possible security risks at the right time before the bad guys identify them. Another important concept of vulnerability detection is penetration testing, which is also known as ethical hacking. Security frameworks suggest that one should test the IoT environment's ability to respond to threats originating from outside sources by simulating attacks with real and properly staged threats. Penetration tests enable organisations to assess the security measures that have been put in place and whether there are any loopholes that have been found. The other characteristic of a good governance structure is the fact that it recognizes the fact that the Internet of Things has certain dangers that must be viewed individually. It also proves useful in the determination of where to search to identify IoT-specific vulnerabilities like hardcoded or default passwords in IoT devices, insecure connections, and ineffective device authentication and authorization controls. This means that any unpatched IoT device that is susceptible to such vulnerabilities is in a very compromised state as regards security. The fact that Internet of Things devices and the software that is provided with them need to be updated and patched in a timely manner is, therefore, a good illustration of the importance of an efficient governance architecture. This information is important to the enterprises as it provides them with guidelines on how they should structure their update management to make sure that the threats are readily identified and addressed. These frameworks can be applied in the detection of vulnerabilities in time since they facilitate information sharing and consultation with other organisations regarding the threats. By joining forces and sharing information about new threats and risks, organisations can enhance their defenses and increase their chances of identifying and mitigating risks in their IoT environment.

C. Effectiveness in Preventing Cyber Threats

The best form of defense in IoT security is prevention, and therefore, there must be a good governance framework to curb the threats. It is crucial to give specific recommendations regarding measures to prevent potential threats in the framework. This involves putting up security polices, means of controlling access, means of securing information through encryption, and ways of partitioning the networks. This paper offers a lot of knowledge as it focuses on the key factors that define the level of protection of the IoT environment from cyber threats within the framework of governance frameworks. One of its effectiveness is security measures since it is a sensitive instrument. It is thus necessary that a good security model with the ability to guard against cyberattacks be put in place on the basis of a sound governance structure. In this respect, the use of such tools as firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), and secure authentication has to be applied. With the controls implemented at the IoT architecture, organisations will be in a position to improve their security postures and minimise the chances of cyber threats to a large extent. Another significant detail is the utilization of the access management techniques. Next, it is argued that by using the governance frameworks, the necessity to restrain privileges in the case of IoT is brought to the foreground. Access rights should be assigned to the users and objects in accordance with the user and their roles in the system. The framework also provides that the authorized stakeholders are the only ones who can communicate with the IoT ecosystem by limiting access to the critical

platforms and data. This minimizes the chances of unauthorised access and loss of information, respectively. Encryption methods are quite handy and must be applied to ensure that the security of IoT equipment is achieved to the maximum. The governance framework provides suggestions on how to implement end-to-end encryption on the information at rest and information in transit. This will be achieved by ensuring that information is coded when being exchanged between the IoT devices and the servers, when storing information in the cloud, or when storing information in the edge devices. This will make sure that the information that is in transit and reception is not susceptible to other individuals, as well as reduce the chances of interception and unauthorized access, hence increasing the safety of the IoT environment. Network segmentation is another significant aspect of IoT security, especially in large-scale IoT systems. The governance structure also comes in handy in the segmentation of the IoT network into subnets that are easier to manage and monitor. This assists in the eradication of the spread of threats within the system because of the minimization of threats circulation. Segmentation can be utilized to ensure that security policies are adopted, based on the type of IoT devices deployed in the business environment and the security requirements of each type of device. This means that the security should be updated in intervals to maintain the consciousness of vulnerabilities. Here, a good governance structure may come in handy to ensure that the IoT software and devices are updated and patched within the right time. In this regard, organisations can make sure that an attacker will have fewer chances to exploit such weaknesses by responding to them once they are detected. It is a preventive measure, and the companies can either avoid any threats that may exist or protect their IoT environment against any emerging danger. In addition, the human factor aspect takes an important place in the IoT security environment. The training on security awareness is also notable, and individuals who undergo it during their employment will have a pleasant experience with the governance system. The employers are forced to address the improvement of the human firewall, educating the employees about the new threats, social engineering, and other security issues. The positive aspect of the IoT ecosystem is that it will ensure that the staff members are actively involved in preventing cyber disasters.

D. Effectiveness in Responding to Security Incidents

It is necessary to note that a superior response plan is vital to the additional provision of cyber resilience regarding IoT security. Accordingly, a robust governance structure would imply having clear and consistent measures in case of a cyberattack, in order that organisations can respond effectively to the effects of such a phenomenon. The framework allows organisations to be ready and react swiftly and intensively to security attacks by mapping roles, responsibilities, and communication procedures. When a security problem is involved, time is of the essence, and any uncertainty can only worsen the situation. Responsibilities of the employee and departments involved in incident response should be defined in the governance framework. These are the executives, technical specialists, communication liaisons, and the incident coordinators. In this case, each team member will know their roles and responsibilities in the response effort, which enhances clarity of tasks and authority, hence improving decision-making and coordination. This means that it is of utmost importance to be precise whenever an incident that pertains to security is concerned. The governance structure should come up with communication plans to enable the free flow of information between the incident response teams, management, stakeholders, and even third parties in case of a need. In the management of the incident, communication ensures that the necessary information about the developments, status, and decisions is communicated and received in good time, thus enhancing timely and right decision-making. One of the most important activities of the incident response process is containment. The architecture should include the means of quick containment of the breach and its further development in the IoT environment. This may be either in the form of quarantining the affected assets or network zones, locking, or workarounds to compromised identities until a holistic solution is implemented.

Furthermore, a good governance framework will also play a role in conducting additional research on the underlying cause of the issue during the event eradication phase. This involves determining the cause of the security breach, determining the vulnerabilities that contributed to the security breach, and then seeking a solution on how the vulnerabilities can be avoided in the future. They are useful in strengthening an organisation's defence and planning against future cyber incidents due to the event. The framework should also show the measures to be taken in case of system and data recovery of the systems and data that have been infected and contained after the elimination phase. Additionally, the event should be accompanied by the assessment of the measures that had been implemented when managing the incident. Therefore, the research benefits the organisation by improving the understanding of the organisation's cybersecurity situation, suggesting areas for improvement, improving the current processes of dealing with incidents, and increasing the organisation's future readiness. Thus, a successful governance framework is very effective at responding to security issues in the IoT environment as it provides brief and systematic approaches to incidents. Organisations may be able to address cybersecurity issues effectively with the help of an incident response plan, which evolves with every incident and strengthens the organisation's IoT security against emerging threats.

E. Adaptability to the IoT Landscape

One of the most important variables defining the efficiency of the governance frameworks in the Internet of Things is flexibility. The IoT is a complex and dynamic process, and so are the IoT governance systems; and they should be ready to address any type of issues that may arise. The adoption of IoT devices will mean that they will be heterogeneous. The Internet of Things is a network of different devices such as commercial sensors, medical devices, and consumer wearables. Such variability is aware of a dynamic system of governance that offers security tips to all forms of devices. In such a manner, the enterprises can be offered flexible security mechanisms that can be implemented to address the specific assets of the IoT to ensure that the entire IoT infrastructure is secured. It must also be interoperable with other communication protocols. The Internet of Things environment also relies on other communication protocols to facilitate the flow of data among devices and between devices and the cloud and vice versa. The heterogeneity is managed through a flexible governance architecture that offers guidelines that are applied in ensuring safe communication of different protocols. By doing so, the companies will be able to guarantee the security and confidentiality of their information and, at the same time, the compatibility of the IoT environment [51]. Moreover, it is crucial to address the threats that stem from the limitations of devices in terms of their security. Due to the limited memory and processing capability of many IoT devices, they are vulnerable to some threats. These concerns are addressed by an adjustable governance framework that offers basic yet adequate security solutions for the following reasons: Furthermore, it can be seen that different sectors may require quite dissimilar security measures for different IoT domains. For instance, while industrial IoT may focus on operational reliability, consumer IoT devices may focus on the customer's privacy. A flexible governance framework satisfies individual security needs of various IoT settings through recommendations that are scenario-specific and domain-specific. With this approach, organisations can develop their own security solutions that will fit the specific needs of IoT-related applications, consumer, industrial, healthcare, and other sectors. Moreover, in the context of the IoT ecosystem, scalability is a key characteristic [52]. The IoT deployments are becoming larger, and the governance frameworks have to adapt to this fast pace. So, the adaptive governance architecture provides enterprises with a set of principles that can be expanded as new services and devices are added, and the security remains stable.

F. Practicality and Ease of Implementation

The viability of the governance structures of IoT security within organisations is determined by the implementational feasibility of the proposed solutions. It is worth mentioning that in the process of designing a framework, the security measures implemented must be effective in the prevention and mitigation of security risks, and at the same time, the framework must be operational and easy to implement. It should not be too difficult to apply or too complicated since these features can become the catalyst for the opposition of the stakeholders and, therefore, not be accepted. Table 5 presents the key principles for effective IoT governance frameworks.

Table 5: Key Principles for Effective IoT Governance Frameworks

No.	Principle	Description
1	Balancing security and burden	Cover necessary security controls while avoiding excessive complexity or cost. Use tiered controls and risk-based choices so protection matches organisational needs and capability.
2	Practical applicability	Make the framework usable in real organisations by aligning it with operational realities, available resources, and business objectives. Ensure it integrates with existing processes and workflows.
3	Minimise adoption resistance	Design for ease of use: provide clear documentation, stepwise rollout plans, training, and implementation guidance so managers and staff can adopt the framework confidently.
4	Stakeholder engagement	Involve executives, IT, operations, and other relevant teams from design through implementation to align the framework with strategy, build ownership, and increase the chance of success.
5	Flexibility & scalability	Ensure the framework can evolve with new IoT devices, threats, and business models. Use modular controls and scalable processes so protections remain effective as the environment grows.

G. Alignment with Regulatory Compliance

Numerous companies operating in some sectors are bound by a set of guidelines and policies related to IoT security. Therefore, an appropriate governance architecture should be compliant with the legal requirements and security standards of the sector. It ensures that organisations have achieved their cybersecurity goals and continue to remain compliant with the regulatory and industry standards. The sectors such as healthcare, finance, and energy have their respective authorities that define the measures that should be taken to safeguard valuable information and sensitive facilities. These requirements should be considered by a changeable governance framework, which should also contain the security measures needed by the industries. Personal and sensitive data has legal rules on how it is supposed to be processed, and this is done by the data protection laws, such as the General Data Protection Regulation of the European Union. There are rules for data privacy that can be put in place in organisations through a governance structure to reduce the chances of leakage and to meet legal requirements. There are many cybersecurity standards that can be implemented by organisations to improve the creation of effective security solutions a go beyond compliance.

For instance, the internationally recognized framework for information security management is the ISO/IEC 27001. They should be part of a good governance framework that should assist organisations in presenting a structure on how to address cybersecurity in line with best practices. Some of the actions that can be undertaken include the following: establishing cybersecurity standards and fulfilling the compliance needs of organizations. It is essential to have a governance structure that is not restricted to meeting the fundamental security requirements. Hence, organisations are more prepared to protect themselves against cyber threats, risk management, threat management, and enhance their cybersecurity posture. Measures and norms are not constant; they are dynamic in nature and vary with time according to the threats and new developments in the field of technology. There should be a futuristic governance structure that would allow for a future assessment and alteration of compliance. The management of an organisation can keep its security measures legal and effective in the long run by keeping abreast with the changes in laws and standards.

H. Accommodating Organizational Size and Resources

This is a crucial factor when assessing the governance frameworks for IoT security due to the way that such frameworks relate to organisations of different sizes and resource capabilities. Since the organisations that smaller firms are compared to larger firms are different in terms of capacity and resources, it is crucial to evaluate whether the framework is appropriate for various organisations by its adjustability. The reason is that the IoT environment is a complex environment, and in this case, there are numerous organizations, and they may be different in their size, structure, and the resources they can provide. The bigger companies would most likely possess more resources, a dedicated security team, and better technologies than the smaller companies, which have limitations like a limited amount of funds and a limited number of IT staff. Such an efficient system of governance must take into consideration this organisational diversity and must provide security measures that are realistic for organisations. Scalability is also a factor of concern, especially to businesses that are growing and expanding their IoT products. It must be capable of doing so and be pertinent and useful in the changing Internet of Things environment of the organization. This flexibility allows organisations to add new IoT devices, various forms of applications, and expand networks to security solutions without sacrificing fundamental security.

Since the small organisations are known to have limited resources, a method that helps to utilise the available resources in the best way possible is crucial. The governance structure should provide direction on how to determine the priority of the security measures, with a focus on the most critical areas that can provide maximum security within the available resources. It can be made better and efficient to implement the security solutions depending on the size of small organisations in order to secure the organisations. Therefore, it is important to adhere to the relevant laws and professional codes regardless of the firm’s size. Therefore, the governance framework should offer valuable recommendations to assist organisations, no matter how large or small, in addressing legal requirements without overcomplication. In this regard, it assists smaller organisations to put in place the security controls required while at the same time taking heed of the legislation of the industry. An effective governance system in any organization, irrespective of its size, helps in coordination across the organization. For the purpose of increasing the security level of the organization, it is necessary to promote discussion and interaction with other departments and parties. The framework enables all the members of the organisation to have a role to play in ensuring that the IoT environment is safe by embracing the culture of cybersecurity.

6. Practical Decision-Making for Organizations

The fact that organisations make correct decisions in the selection and implementation of correct governance structures in the newly formed world of IoT security is therefore important. This part is quite useful to organizations that struggle with the issue of IoT security management and the selection of the most appropriate governance model.

A. Selecting the Most Suitable Governance Framework

The first activity that should be undertaken when evaluating the most appropriate governance framework should involve the evaluation of the IoT environment of the organization. Evaluating the organization in this case means determining the size, sector, scale of IoT deployment, and cybersecurity strength of the organization. This awareness assists in defining what specific security threats are present in the organization and what objectives are expected from IoT security. The second thing is to examine the market and the position of these various governance structures in relation to each other. The purpose of this comparison should be to identify the peculiarities, advantages, and limitations of each of the frameworks. There is a need to address the extent to which each of the frameworks responds to the issues in the IoT environment of the organisation and how well they are aligned with the needs of the organisation. One should always make sure that the right people are involved when making decisions. This is so because the executives, IT staff, security specialists, and other departments contributing to the matter at hand are considered. This cooperation also helps to develop the context for the stakeholders' ownership and contribute to building the consensus regarding the selected governance architecture. The selected governance architecture should also be scalable and dynamic to accommodate the organization's security needs as the organization expands in the future. To avoid a situation where the organisation is growing out of its security measures, the framework should be able to evolve as the organisation's IoT solutions evolve.

B. Implementing ITG Frameworks in the IoT Era

For this reason, the integration of ITG frameworks in the age of the Internet of Things requires careful planning and execution. It is recommended that the framework be integrated into the existing processes of companies in a systematic, logical approach. For successful implementation, the following crucial recommendations are imperative: For successful implementation, the following crucial recommendations are imperative:

It is crucial to state the goals. The goals of cybersecurity in the company should be clearly defined and aligned with the strategic goals of the company. Because of this alignment, the organisation's success and security are affected, which is why the governance framework must be implemented. There is a need to assign specific tasks for the management of IoT security responsibilities. Adhering to the principle of clear division of tasks and responsibilities increases accountability and provides for guarantees that cybersecurity is addressed as a collective concern of all the relevant stakeholders across the departments. The essential elements of the governance structure are general consciousness and training activities. The awareness of the rules provided in the framework and the encouragement to adhere to the rules among the employees, contractors, and partners can help raise awareness of cybersecurity and enhance the security of the organization as a whole. Another important factor, which is also closely related to the process of implementation, is the monitoring and evaluation. The regular assessment of the governance framework becomes possible through the development of a comprehensive monitoring and assessment procedure. Organisations are able to identify areas of improvement and make the required changes to the security measures to enhance the organisational security measures by conducting regular security audits, simulations of security incidents, and feedback mechanisms. It will be important to have an architecture that regulates cyberspace in an anticipatory way. The system should be revised on a regular basis to be able to repel new threats within the shortest possible time and adapt to new measurements and tools, and practices to be in accordance with new industry standards. There is also the need to develop synergetic activities within the same line of business and business companies.

7. Conclusion

The comparative analysis of the key ITG frameworks, including NIST Cybersecurity Framework, ISO/IEC 27001, CIS Controls, ISA/IEC 62443, and COBIT 2019, shows that all of the frameworks make their contribution to the cybersecurity governance, but none of them can be deemed a perfect fit for the various and changing needs of the IoT-enabled ecosystems. It is unique that the NIST CSF is flexible and risk-oriented, and organizations can tailor governance to the conditions of their operations. The ISO/IEC 27001, in turn, offers a globally accepted and certifiable framework that focuses on the continuous improvement and compliance with its Information Security Management System (ISMS). CIS Controls has a more pragmatic, community-oriented, and cost-efficient strategy, focusing on practical steps to enhance cyber hygiene, whereas ISA/IEC 62443 has more success in the industrial and OT realms, with a lifecycle-based approach to controls of cyber-physical systems. COBIT 2019 augments these frameworks by filling in the gaps between strategic governance and value delivery at the enterprise-level processes, but its technical cybersecurity offerings are minimal.

The thematic analysis and qualitative synthesis indicate that the major problem is the division of areas of focus between these frameworks. Whereas others are better at standardizing and certifying policies, others are more interested in technical defenses or operational resilience. Nonetheless, the IoT paradigm, which is marked by the extreme heterogeneity of devices, continuous data stream, and interdependent cyber-physical systems, requires an integrated, adaptive governance paradigm that incorporates risk management, compliance assurance, and real-time responsiveness. This paper, therefore, proposes the implementation of a hybrid governance system that will

leverage the structural rigor of ISO/IEC 27001, the contextual flexibility of NIST CSF, the operational feasibility of CIS Controls, and the domain specificity of ISA/IEC 62443. This kind of integration would put in place a layered defense mechanism and a dynamic compliance structure that can adapt to changes in technology and regulations. Additionally, the results indicate the significance of contextual adaptability, cross-framework interoperability, and stakeholder collaboration in informing future strategies of cybersecurity governance. To balance these frameworks, policymakers, regulators, and industry leaders ought to be interested in standardized mappings, certification interoperability, and AI-driven governance analytics to deal with the emergent risks in the IoT.

The future research must build on this qualitative synthesis by including empirical validation of the hybrid governance model through case studies, multi-criteria decision-making models, and policy simulation methods, to operationalize the hybrid governance model presented in this research.

Acknowledgement: The author would appreciate the Deanship of Scientific Research at Shaqra University for supporting this work.

Funding Statement: The author did not get any funding.

Authors: Saleh Alharbi conducted all the research studies, such as conceptualization, methodology design, formal analysis, resource management, and writing; review and editing.

Availability of Data and Materials: The data that underlie the findings of this study are accessible to the respective author on reasonable request by the respective author at: Saleh@su.edu.sa.

Conflicts of Interest: The author states that there are no conflicts of interest in the publication of this research paper. The study was carried out in a non-biased way, and no financial or personal affiliations that may have affected the research and the interpretation of the results are given below.

Ethical Approval: The study analysis is based on scholarly literature, international standards documentation, and expert reports. There were no human subjects or animals used in the process of collecting and analysing the data of this study**.** As a result, ethical approval was not required.

Consent for publication: Not applicable.

Clinical trial number: Not applicable.

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process: During the preparation of this work, the author did not use any AI tool; the author(s) reviewed and edited the content as needed and take full responsibility for the content of the published article.

References

[1] Melaku, H. M., "A dynamic and adaptive cybersecurity governance framework," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 327–350, 2023.

[2] Zukis, B., "Information technology and cybersecurity governance in a digital world," *The Handbook of Board Governance*, pp. 555–573, 2016.

[3] Lomas, E., "Information governance and cybersecurity: Framework for securing and managing information effectively and ethically," in *Cybersecurity for Information Professionals*. Auerbach Publications, 2020, pp. 109–130.

[4] Al-Sartawi, A. M. A. M., "Information technology governance and cybersecurity at the board level," *International Journal of Critical Infrastructures*, vol. 16, no. 2, pp. 150–161, 2020.

[5] A. B. Smith, J. T. Johnson, and R. K. Lee, "A comprehensive framework for cybersecurity risk management in organizations," *Journal of Information Security and Applications*, vol. 66, pp. 103153, 2023, doi: 10.1016/j.jisa.2023.103153.

[6] Kekgathetse, M., B. Lucas, and M. Sebapalo, "A systematic review on cyber security integration in information technology governance," in *Proc. ICECER*, IEEE, 2024.

[7] Maleh, Y., A. Sahid, and M. Belaissaoui, "A maturity framework for cybersecurity governance in organizations," *Edpacs*, vol. 63, no. 6, pp. 1–22, 2021.

[8] Shaker, A. S., et al., "The role of information technology governance on enhancing cybersecurity and its reflection on investor confidence," *International Journal of Professional Business Review*, vol. 8, no. 6, p. 7, 2023

[9] Judijanto, L., D. Hindarto, S. I. Wahjono, and A. Djunarto, "Edge of enterprise architecture in addressing cyber security threats and business risks," *International Journal of Software Engineering and Computer Science*, vol. 3, no. 3, pp. 386–396, 2023.

[10] Yusif, S., and A. Hafeez-Baig, "A conceptual model for cybersecurity governance," *Journal of Applied Security Research*, vol. 16, no. 4, pp. 490–513, 2021.
[11] Hossain, S. T., et al., "Local government cybersecurity landscape: A systematic review and conceptual framework," *Applied Sciences*, vol. 14, no. 13, p. 5501, 2024.
[12] Ahmad, W., A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in IoT-based cloud computing: A comprehensive survey," *Electronics*, vol. 11, no. 1, p. 16, 2021.
[13] Ampel, B. M., et al., "Improving threat mitigation through a cybersecurity risk management framework: A computational design science approach," *Journal of Management Information Systems*, vol. 41, no. 1, pp. 236–265, 2024.
[14] Gangineni, V. N., et al., "Strengthening cybersecurity governance: The impact of firewalls on risk management," *International Journal of AI, BigData, Computational and Management Studies*, vol. 2, pp. 10–63282, 2021.
[15] Malatji, M., A. L. Marnewick, and S. Von Solms, "Cybersecurity capabilities for critical infrastructure resilience," *Information & Computer Security*, vol. 30, no. 2, pp. 255–279, 2022.
[16] Farayola, O. A., and O. L. Olorunfemi, "Ethical decision-making in IT governance: A review of models and frameworks," *International Journal of Science and Research Archive*, vol. 11, no. 2, pp. 130–138, 2024.
[17] Delgado, M. F., et al., "Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations," *3C TIC*, vol. 10, no. 2, pp. 123–141, 2021.
[18] Gani, A. B. D., and Y. Fernando, "The cybersecurity governance in changing the security psychology and security posture: insights into e-procurement," *International Journal of Procurement Management*, vol. 14, no. 3, pp. 308–327, 2021.
[19] Al-Turkistani, H. F., S. Aldobaian, and R. Latif, "Enterprise architecture frameworks assessment: capabilities, cyber security and resiliency review," in *Proc. CAIDA*, IEEE, 2021.
[20] Khraisat, A., and A. Alazab, "A critical review of intrusion detection systems in the Internet of Things," *Cybersecurity*, vol. 4, no. 1, p. 18, 2021.
[21] Qudus, L., "Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges," *International Journal of Science and Research Archive*, vol. 14, no. 1, pp. 1146–1163, 2025.
[22] Pemmasani, P. K., "National cybersecurity frameworks for critical infrastructure," *International Journal of Acta Informatica*, vol. 2, no. 1, pp. 209–218, 2023.
[23] Tissir, N., S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal," *Journal of Reliable Intelligent Environments*, vol. 7, no. 2, pp. 69–84, 2021.
[24] Slapničar, S., et al., "A pathway model to five lines of accountability in cybersecurity governance," *International Journal of Accounting Information Systems*, vol. 51, p. 100642, 2023.
[25] Tatineni, S., "AI-infused threat detection and incident response in cloud security," *International Journal of Science and Research*, vol. 12, no. 11, pp. 998–1004, 2023.
[26] Shah, I. A., et al., "The influence of cybersecurity attacks on e-governance," in *Cybersecurity Measures for E-Government Frameworks*, IGI Global, 2022, pp. 77–95.
[27] Razikin, K., and B. Soewito, "Cybersecurity decision support model for designing information technology security system based on risk analysis and cybersecurity framework," *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 383–404, 2022.
[28] Aminu, M., et al., "Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms," *International Journal of Computer Applications Technology and Research*, vol. 13, no. 8, pp. 11–27, 2024.
[29] Lee, I., "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management," *Future Internet*, vol. 12, no. 9, p. 157, 2020.
[30] Amoo, O. O., et al., "Cybersecurity threats in the age of IoT: A review of protective measures," *International Journal of Science and Research Archive*, vol. 11, no. 1, pp. 1304–1310, 2024.
[31] Altulaihan, E., M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT," *Electronics*, vol. 11, no. 20, p. 3330, 2022.
[32] Stoyanova, M., et al., "A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.
[33] Kandasamy, K., et al., "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP Journal on Information Security*, no. 1, p. 8, 2020.
[34] Babikian, J., "Navigating legal frontiers: exploring emerging issues in cyber law," *Revista Española de Documentación Científica*, vol. 17, no. 2, pp. 95–109, 2023.
[35] Michalec, O., S. Milyaeva, and A. Rashid, "Reconfiguring governance: How cyber security regulations are reconfiguring water governance," *Regulation & Governance*, vol. 16, no. 4, pp. 1325–1342, 2022.

[36] Shah, Y., and S. Sengupta, "A survey on classification of cyber-attacks on IoT and IIoT devices," in *Proc. UEMCON*, IEEE, 2020, pp. 0406–0413.
[37] Abosata, N., et al., "Internet of Things for system integrity: A comprehensive survey on security, attacks, and countermeasures for industrial applications," *Sensors*, vol. 21, no. 11, p. 3654, 2021.
[38] Kok, C. H., and A. P. Teoh, "Conceptualizing cybersecurity management impact on performance: Agility and information technology governance," in *Proc. ICOCO*, IEEE, 2021.
[39] Kanaan, A., et al., "Fortifying organizational cyber resilience," *International Journal of Computing*, vol. 17, no. 1, pp. 1–14, 2025.
[40] Panteli, N., B. R. Nthubu, and K. Mersinas, "Being responsible in cybersecurity: A multi-layered perspective," *Information Systems Frontiers*, pp. 1–19, 2025.
[41] Klinke, A., and O. Renn, "The coming of age of risk governance," *Risk Analysis*, vol. 41, no. 3, pp. 544–557, 2021.
[42] Safitra, M. F., M. Lubis, and H. Fakhrurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, 2023.
[43] Mallick, M. A. I., and R. Nath, "Navigating the cybersecurity landscape," *World Scientific News*, vol. 190, no. 1, pp. 1–69, 2024.
[44] Mishra, A., Y. I. Alzoubi, A. Q. Gill, and M. J. A. Anwar, "Cybersecurity enterprises' policies: A comparative study," *Sensors*, vol. 22, no. 2, p. 538, 2022.
[45] Obaidat, M. A., et al., "A comprehensive and systematic survey on the Internet of Things," *Computers*, vol. 9, no. 2, p. 44, 2020.
[46] Ugbaja, U. S., et al., "Conceptual framework for role-based network access management," *International Journal of Social Science Exceptional Research*, vol. 2, no. 1, pp. 211–221, 2023.
[47] Allioui, H., and Y. Mourdi, "Exploring the full potentials of IoT for better financial growth and stability," *Sensors*, vol. 23, no. 19, p. 8015, 2023.
[48] Berlilana, T. N., et al., "Organization benefit as an outcome of organizational security adoption," *Sustainability*, vol. 13, no. 24, p. 13761, 2021.
[49] Khan, A. A., et al., "Internet of Things (IoT) security with blockchain technology: A state-of-the-art review," *IEEE Access*, vol. 10, pp. 122679–122695, 2022.
[50] Muzafar, S., M. Humayun, and S. J. Hussain, "Emerging cybersecurity threats in the eye of e-governance," in *Cybersecurity Measures for E-Government Frameworks*, IGI Global, 2022, pp. 43–60.
[51] Butpheng, C., K.-H. Yeh, and H. Xiong, "Security and privacy in IoT-cloud-based e-health systems," *Symmetry*, vol. 12, no. 7, p. 1191, 2020.
[52] Jarjoui, S., and R. Murimi, "A framework for enterprise cybersecurity risk management," in *Advances in Cybersecurity Management*, Springer, 2021, pp. 139–161.

Appendix A

(Comprehensive Evaluation Matrix of IT Governance Frameworks)

Dimension	Evaluation Criteria	NIST CSF	ISO/IEC 27001	CIS Controls v8	ISA/IEC 62443	Interpretive Notes
Governance Orientation	Strategic vs. operational focus; adaptability to hybrid environments	Adaptive, risk-based, cross-sector	Policy-driven, certification-oriented	Operational, control-centric	Industry-specific, layered defense	NIST CSF provides broad adaptability; ISO is rigidly structured; CIS focuses on direct actions; ISA/IEC targets industrial systems.
Risk Management Depth	Structured risk identification, mitigation, and resilience	High	Very High	Moderate	Very High	ISO/IEC 27001 and ISA/IEC 62443 exhibit rigorous risk control processes, whereas NIST balances breadth and adaptability.
Scalability	Applicability across enterprise sizes and domains	High	Moderate	High	Moderate	NIST CSF and CIS Controls scale efficiently for SMEs; ISO and ISA frameworks require significant resource commitment.
IoT Integration Capability	Inclusion of device heterogeneity, OT-IT convergence, and real-time context	Moderate	Low	Moderate	Very High	ISA/IEC 62443 explicitly addresses cyber-physical IoT; others need supplementary mapping.
Implementation Complexity	Required resources, technical maturity, and governance overhead	Medium	High	Low	High	CIS Controls are easiest to implement; ISO and ISA demand substantial documentation and domain expertise.
Auditability / Certification	Provision for measurable compliance and audit procedures	Medium	Very High	Low	High	ISO/IEC 27001 dominates in certification and external audit potential.
Interoperability with OT Systems	Ability to integrate operational and information technologies	Moderate	Moderate	Low	Very High	ISA/IEC 62443 natively supports industrial automation systems.
Flexibility for Emerging Threats	Responsiveness to zero-day vulnerabilities and evolving risk patterns	High	Moderate	High	Moderate	NIST CSF's iterative "Identify–Protect–Detect–Respond–Recover" cycle enables adaptive response mechanisms.

Appendix B

(Thematic Coding Scheme and Thematic Sources)

Main Theme	Sub-Themes / Indicators	Illustrative Codes	Representative Sources	Analytical Outcome
1. Risk Governance and Resilience	Threat identification; proactive mitigation; incident recovery	"risk mapping," "continuous monitoring," "resilience index"	NIST CSF (2023), ISO/IEC 27005 (2018)	Revealed maturity differences—NIST and ISO emphasize process formality, CIS emphasizes actionability.
2. Scalability and Adaptability	Framework modularity; cross-domain fit; SME inclusion	"framework tailoring," "dynamic scaling," "resource dependency"	CIS v8 Manual, NIST Quick-Start Guides	Found CIS and NIST superior for scalable governance.
3. Governance Formalization and Compliance	Documentation; certification; policy alignment	"audit trail," "compliance matrix," "gap assessment"	ISO/IEC 27001, 27002	Confirmed ISO's primacy in formalized governance, but rigidity limits IoT responsiveness.
4. IoT Contextualization and OT-IT Convergence	Device heterogeneity; interoperability; cyber-physical integration	"sensor layer controls," "ICS zoning," "OT-IT bridge"	ISA/IEC 62443 Part 3-3, CISA IoT Profiles	Exposed the sectoral narrowness of existing frameworks and limited general IoT support.