International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 15s, 2025
https://www.theaspd.com/ijes.php

# Unified Cybersecurity Risk Management Frameworks For Cloud And Ai-Powered Enterprises: A Literature Review And Research Gap Analysis

**ThamaraiSelvan M[1], Mrs. Udhaya.M[2], Dr.A. Arun[3]**
[1]Research Scholar, Department of Management, Sree Saraswathi Thyagaraja College, Pollachi
[2]Assistant Professor, Department of management, Rathinam College of Arts and Science, Pollachi, Tamil Nadu, India.
[3]Professor, Rathinam School of Business at TIPS Global, Coimbatore.

***Abstract***
*Massive implementation of cloud computing and Artificial intelligence (AI) changed the landscape of enterprise operations and posed complicated cybersecurity threats. Conventional risk-based management models are incapable of keeping abreast with the dynamic and highly fluid nature of threats promoted by AI and cloud risks. The increasingly complex nature of cyber threat environment poses serious difficulties on the efficiency of the current cybersecurity risk management frameworks. In this paper, the author performs an in-depth study of the salient frameworks, such as ISO/IEC 27001, the NIST Cybersecurity Framework. Although these frameworks provide a systematic approach to information security, most institutions have found it challenging to implement the frameworks due to operational constraints, fast rate of technology changes, and complexity of the cyber threats like Advanced Persistent Threats (APTs). In addition, the use of a fix, past-oriented data tends to make such frameworks inefficient to combat new and real-time threats.*

## INTRODUCTION

In the digital economy, cloud platforms and AI-based applications are used by enterprises with increasing reliance, and this trend places enterprises at risk of new and advanced cyber threats. The recent rampant data breaches, security-related attacks on exploded AI models, and cloud misconfigurations demonstrate why risk management systems are important. However, the standard models like the NIST Cybersecurity Framework or ISO/IEC 27001 were originally not designed to encompass the individual complexities of AI- and cloud-based securities.

Cybersecurity has become one of the imperative organizational problems in various fields of endeavors in the current digital era. Increased frequency and sophistication of cyber related incidents (such as data breaches, ransomware attack, and insider threats) call attention to the need of proper cybersecurity practices. According to the projections by Cybersecurity Ventures in 2021, by the year 2025, the entire world will be spending more than 10.5 trillion US dollars fighting cybercrimes--much of which makes the implementation of in-depth cybersecurity measures a necessity.

This review assesses critically available cybersecurity risk management frameworks, their difficulties that enterprises face when attempting to implement them, and the existence of gaps in suitable research. In such a way, it outlines the scope of the future investigation that is ready to contribute to the creation of more flexible and sector specific models that will help to handle modern cybersecurity issues.

## LITERATURE REVIEW

### Overview of Prominent Cybersecurity Risk Management Frameworks

#### NIST Cybersecurity Framework

The comprehensive yet flexible approach to cybersecurity risks management is considered to be the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Organized into five mutually supportive functions (Identify, Protect, Detect, Respond and Recover), it presents organizations with a structured mechanism with which to assess their cybersecurity position and integrate the necessary controls.

Although recognized as adjustable, the high degree of applicability that the framework suggests might create differences in application of the framework in organizations. Shackelford et al. (2016) argue that organizations often become challenged by ensuring that the individual demands of their operations may match the generic advice issued by NIST. Also, findings of cyber threats are always on the rise, in as much as maintaining the practices to reflect various updates to newer versions of the framework may be too expensive and time consuming.

**ISO/IEC 27001:**

ISO/IEC 27001 is a universal standard worthy of Information Security Management Systems (ISMS), and it is focused on safeguarding sensitive data by ensuring its confidentiality, integrity, and availability. The standard outlines certain controls and practices that companies are supposed to implement so as to receive certification (ISO, 2013).

There are challenges of the ISO/IEC 27001 despite its strength, especially among the small and medium-sized enterprises (SMEs). Most of the SMEs do not have the corporate capabilities that will enable them to meet full compliance of the standard due to the complexity and the cost of carrying out an exercise of certification and maintenance (Jouini et al., 2014). In addition, the process-oriented approach of the framework can conceal the importance of implementing dynamic risk-management practices that can accommodate new threats that are in a constant state of change.

FAIR (Factor Analysis of Information Risk) and OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) are classical approaches to cyber-risk analysis that people use in modern information security practice. Both are significantly distinct: FAIR, being a quantitative risk exposure modelling, and OCTAVE, being context and organizational goal-focused. The discourse below outlines the fundamental assumptions of the two frameworks as well as their main shortcomings.

**FAIR**

FAIR puts the risk management in the quantitative risk management arena that allows the organization to communicate exposure to a cyber-threat using monetary measurement. The quantification of the latter by decision-makers can thus determine security capital allocation in a more precise and rational manner than subjective means usually allow. However, this adoption is still lopsided due to its limitation of data maturity of firms. The inability to collect adequate data and analyse it necessitates the investment of resources, and many medium and small organizations do not have them, obstructing the accuracy of assessment in the form of FAIR (Boehmer, 2018). In addition, individual characteristics and organizational culture, which are the subjects of qualitative attributes, may be overlooked in the context of assessing statistical variables, which determine the level of risk in a subjective but irrevocable way.

**OCTAVE**

OCTAVE, created by Carnegie Mellon University, is based on the fact that cybersecurity risk management must match the overall organizational goals. It guides companies to list their vulnerabilities, locate critical assets and design risk mitigation strategies according to their individual operation realities. Despite the high-quality guidance that OCTAVE provides in terms of this process, it has its limitation due to the self-guiding nature of the process it deliberately offers: professionals in the field are necessary to implement OCTAVE and not all enterprises may have access to them (Gordon et al., 2020). What worsens this matter even more is the fact that regular updates of the framework are not common, and this can negatively affect its effectiveness in addressing the modern challenges of cybersecurity.

**Challenges in the Adoption and Implementation of Frameworks**

In as much as cybersecurity frameworks are known to be useful, there exists a complex of barriers in implementing them in real life. Organizations are again faced with challenges to successful implementation, especially the ones related to complexity, scalability issues, and the constant development of cybersecurity threats.

**Scalability Limitations**

Most of the current frameworks are tailored to suit the needs of big businesses as their audience and thus might not be suitable to small and medium business (SMEs). With the latest empirical research proving that SMEs are overrepresented as the target of cyber-attacks, many of them are ill-equipped with the

capabilities of meeting such measures as the comprehensive ISO/IEC 27001 standard due to a lack of financial and human resources (Rees et al., 2011; Alotaibi et al., 2020).

In curbing such discrepancies, scholars have tabled the ideas of simplifying option, focusing on key controls and best practices that would give SMEs the opportunity to implement a risk-management approach without the drainage of resources (Gupta et al., 2018; AlHogail, 2018).

**Implementation Complexity**

The nature of structure like NIST and ISO/IEC 27001 often hinders compliance by organizations due to its complexity. Businesses claim that the time and effort spent on the full conformity consume a lot of time, distracting the main functioning of the company (Cole et al., 2017).

To that end, companies are forced to dedicate a lot of resources to training staff, updating policies documentation, and integrating security controls, all of which may interfere with the ordinary course of things. In addition, the worldwide lack of cybersecurity workers means that numerous companies will struggle to recruit the skills they require to operate within such complex systems (Oltsik, 2019; Bansal et al., 2021).

**Dynamic Rise of Threats**

Advances in technology and the growing complexity of cyber threats destroy the effectiveness of frameworks that are based on historical data and are non-adaptive to changes. One such replenishment is witnessed in the advent of advanced persistent threats (APTs), which have increasingly challenged organizations to be more proactive and progressive in terms of their approach to security (Fernandes et al., 2014; Shafique et al., 2020).

Traditional frameworks also might fail to meet the changing risks and many organizations state that they are incapable of synchronizing their cybersecurity arrangements with emerging risks (Sadeghi et al., 2015; Tharwani et al., 2022). This predicament highlights the necessity of structures perfect to not only adapt to transforming and ever-evolving threat environment but also to assimilate real-time threat intelligence.

**Threat to Cybersecurity in Clouds and AI**

**Cybersecurity Threats that are Cloud Specific**

- Losses to data harms due to incorrectly set up cloud storage and poor encryption.
- Insider threats that arise when appropriate access control methods are not used; and when security awareness is poor.
- API vulnerabilities which make cloud services accessible to external threats because of a poor authenticating information system.
- The misunderstandings related to the shared responsibility model that cause security gaps and the failure of compliance.
- Multi-tenancy threats in which various cloud clients accidentally make vulnerabilities open.
- Unsecure third party extensions which open backdoor exploit.

**Cybersecurity risks related to AI Accounting Compliance Exceptions to Shopping Malls**

- AI-model poisoning and adversarial attacks, where attackers can get incorrect results in which they can manipulate inputs to attack an AI model.
- The privacy of data and their compliance during AI training reasons and outcomes are ethical dilemmas and breaching of regulation.
- AI security concerns with explainability and transparency, and the restricted ability to rely upon threat assessments generated by AI.
- AI-controlled threat detection and response systems bias, which generates false positives or inefficacy regarding security policies.
- Algorithms backdoors (the introduction of undetected flaws by attackers in the learning process of AI).
- Deepfakes ADP powered by AI that are aimed at getting around authentication systems.

**Existing Cybersecurity Frameworks and deficiency to them**

**Cybersecurity Framework NIST**

Pros: A properly structured risk management strategy, and broad industrial applicability, and corresponds to cloud security models. Limitations: It cannot be applied to fast evolving AI threats because it lacks AI specific recommendations and cloud-native security controls.

**ISO/IEC 27001**

Strengths: It has good governance ideals of information security, the world knows how well regulated it is. Weakness: Harsh compliance regime and the inability of SMEs to be fully compliant with them, does not specify protection against cybersecurity risks that can be attributed to AI.

**CSA Cloud Controls Matrix (CCM)**

Strengths: The security control is cloud-native, suits to the shared responsibility model, and provides fine-grained control of security over the design of clouds. Weaknesses: Minimal knowledge of AI governance and not connected to specially designed AI threat models.

**NIST AI RMF AI Risk Management Framework (NIST AI RMF)**

Strengths: reduction of the security risk when working with AI, emphasis on transparency, explainability, ethical in AI. Weak points: It does not completely address the level of cybersecurity threats posed by the cloud as well as the potential future threats of adversarial AI in a real-time manner.

**RESARCH GAPS**

The present body of literature on cybersecurity risk management frameworks has several gaps that have been identified as critical. The gaps have a chance of future-research to enhance the attractiveness and relevance of these frameworks in various fields.

**Gap 1: Insufficiency of Industry Specific modifications**

Current cybersecurity operating models tend to present broad-based instructions that fail to grasp the nature of specific requirements by various industries. As an example, the healthcare industry has certain regulatory needs and weaknesses associated with the security of patient data. Greene et al. (2019) propose that frameworks require contextualization to make them more effective and responsive to the industry challenges, which results in variations of the same framework across industries.

**Future research direction:**

Future studies ought to be aimed at creating frameworks that meet the special requirements of the different sectors. The joint work of the experts in the industry and cybersecurity specialists will result in developing guidelines that will take into consideration the best practices in the particular industry and statutory compliance.

**Gap 2: Adapting the Framework to the Emerging Technologies**

Emerging technologies (AI, IoT, blockchain), in turn, cause the emergence of new security issues that are not covered by the current frameworks. To give an example, incorporating IoT systems in business settings might bring new flaws that legacy systems will struggle to address (Deogirikar & Vidhate, 2017; Burch et al., 2020).

**Nature of Future Research:**

The research must consider the development of adaptive structures that expressly factor in the security issues of the new age technologies. That involves establishing the protocols on how to ensure the security of IoT devices and stewardship of AI-related security measures that are receptive to whatever the threats are.

**Gap 3: Strike Balance between the Qualitative and the Quantitative Risk Assessment**

The existing frameworks focus on either qualitative or quantitative measurement of risk or the unbalance of risk management solutions is a result. The strictly qualitative evaluation can miss vital evidence-based insights, whereas the strictly quantitative one can miss the more subtle nature of organizational culture and human behaviour (Yang et al., 2021).

**Nature of Future Research:**

In future, studies might be developed to develop hybrid models that would combine qualitative and quantitative risk evaluation methods. These models have the potential of also using data analytics as well

as factoring in aspects of culture in an organization and human behaviour with the possibility of a more thorough look at risk.

**Gap 4: Streamlining Frameworks of SMEs**

Whereas big organizations can afford to implement an elaborate cybersecurity model, most SMEs are unable to do so due to lack of sufficient resources. The studies show that minimalistic frameworks targeting critical controls would give SMEs the power to take a proactive stance on cybersecurity (Rees et al., 2011; AlHogail, 2018).

**Nature of Future Research:**

The research elements should be aimed at coming up with simplified and flexible structures that suit the peculiar needs of the SMEs. These involve developing toolkits containing step-by-step instructions to the implementation of key cybersecurity prevention measures that do not require much resources.

## RESEARCH METHODOLOGY

In this research a mixed-methods approach is deployed:

- **Case Study Analysis:** The analysis of practical cloud, AI security breaches, including Capital One data breach and possible adversarial AI attacks on autonomous systems.
- **Survey & Interviews:** The questionnaire application aimed at collecting information about the best practices of cybersecurity specialists, AI researchers, and cloud architectures.
- **Comparative Analysis:** Comparison of the existing frameworks to new AI and cloud threats to reveal the gaps and offer the best means of improvement.
- **Framework Enhancement:** Suggestion of an adaptive risk management model of cybersecurity that includes AI-based threats intelligence and automation.

**Suggested framework on cybersecurity risk management**

**Risk Identification**

A well-guided process of targeting AI and cloud-specific threats, comprising vulnerability evaluation methods, and threat intelligence acquisition by constant tracking enforcement with the help of AI-powered defence analytics.

**Risk Analysis/ Assessment**

- Applying Artificial Intelligence-wise risk assessment techniques to measure real-time threats.
- Utilizing movable risk assessment models of the cloud.
- Combining the regulatory compliance analysis (GDPR, NIST, ISO) with automated auditing to maintain the consistent security status.
- Evaluation of the ethical ramifications of the AI mechanism-based security.

**Controls Implementation**

- Implementation of **Zero Trust Architecture (ZTA)** and the strong **IAM** models in order to limit the unauthorized access.
- Implementation of **multi-layer encryption** in securing sensitive information within cloud environment.
- Providing specially designed protection against AI like **bias detection tools** and **adversarial robustness testing**.
- Utilizing identity management blockchain to increase access control of cloud services.

**Risk Mitigation Continuous Monitoring**

- Always on-the-spot artificial intelligence-based **Security Operations Center (SOC)** functionalities that keep the threat under constant surveillance and automatically defences themselves.
- Acceleration and protection of workloads, automated threat mitigation with cloud-native application protection platforms (CNAPP).
- Secure Develops practices to incorporate security in the software development lifecycle.
- Anomaly detection with the use of AI to anticipate risk.

**Compliance Governance**

- Setting up AI ethics policies and governing structures to maintain open and responsibility in security decision-making.
- Subordination of cybersecurity policies to existing industry policies and appropriate AI ethics.
- AI-enhanced anomaly detection and forensic analysis to improve the process of security auditing.

**Case Studies**

Detailed analysis of case studies will be applied to various industries such as healthcare industry, financial industry, manufacturing sector and education. These case examples will look at the approaches used by organizations to apply cybersecurity models such as their challenges and success of the strategies adopted. Through comparing successful implementations and unsuccessful ones, it can be possible to learn a lot about some best practices and possible pitfalls.

To give an example, one case study dealing with healthcare can examine how a hospital implemented the NIST framework in order to comply with HIPAA specifications whereas another one in the manufacturing sphere can discuss the adoption of ISO/IEC 27001.

**Surveys**

The case studies will be supplemented by surveys addressing cybersecurity experts in different fields. The surveys will collect information about perception towards the current ones, implementation difficulties and recommendations. Stratified sampling of the different sizes and types of organization would be used to have data of different organizations and have a solid analysis of such trends and correlations.

Some of the questions to be asked in the survey would involve effectiveness of the currently existing frameworks, hindrances to implementation, and the cybersecurity issues specifically raised by the organization in various sectors.

**In-Depth Interviews**

Cybersecurity leaders and decision-makers are going to be interviewed in-depth, and qualitative data will be used to gather information on the strategic approach towards framework implementation. The following interviews will aim at revealing reasons of selecting respective frameworks, its perceived quality, and implementation spots.

**Data Analysis**

Thematic analysis will be used to analyse data gathered through case studies, surveys and interviews to provide a statistical interpretation. Thematic analysis will allow defining general themes and problems in various areas, whereas statistical analysis will allow understanding general relations between the variables, e.g., organizational size and framework effectiveness.

## RESULTS AND DISCUSSION

The study reveals the most significant vulnerabilities in the current cybersecurity systems and implies the necessity of an approach that would combine AI-aware risk evaluation and cloud protection solutions. Organizations have to move to round-the-clock supervision, AI-aided automation of security, and risk mitigation strategies.

According to the findings, even though NIST CSF and ISO/IEC 27001 offer a beneficial framework, they are less specific in implementing AI-related security solutions and cloud-native flexibility. Using proactive security analytics, AI-based anomaly detection, and automatic compliance structure may heavily increase the resilience of cybersecurity in enterprises.

## CONCLUSION AND FUTURE DIRECTIONS OF A RESEARCH

In the study, a framework of cybersecurity risk management is proposed, which attempts to address cloud and AI security issues in a modernized approach. The future problem needs to be studied: the real-time methods of risk evaluation by AI, and the standardization of the best practices of AI security governance. Enterprises capable of incorporating AI-powered security monitoring technologies and dynamic frameworks may respond dynamically to minimize cybersecurity threats. Enterprise security needs the change in strategy that move beyond the traditional use of risk management practices to adaptive measures that make use of AI.

The ethical implication of AI-driven cybersecurity solutions should also be the subject of future researches. With all the positive aspects of automation, the question of privacy, accountability, and bias in the system of an artificial intelligence-based security system appear. This must be a balanced strategy in which security and ethical compliance are guaranteed to secure resilience with time in cybersecurity.

To sum up, this literature review has underlined the issue of utmost importance that cybersecurity risk management frameworks play to enterprises operating within an even more complicated threat environment. Although the current frameworks, including NIST, ISO/IEC 27001, FAIR, and OCTAVE are reasonable recommendations, there are still major gaps that should be filled. In further studies, it is essential to build adaptation of the industry, domain-specific models, and simplify implementation in SMEs. Filling out these gaps may allow the researcher to come up with more effective and flexible cybersecurity frameworks that will be able to meet the needs of the various enterprises of today.

**REFERENCES**

1. Alberts, C., Dorofee, A., Killcrece, G., & Lucier, C. (2003). *OCTAVE: A Framework for Managing Information Security Risks*. Carnegie Mellon University.
2. AlHogail, A. (2018). *Challenges in Implementing Cybersecurity Frameworks for SMEs*. International Journal of Computer Applications, 182(10), 1-6.
3. Alotaibi, R., Alshahrani, M., & Khan, A. (2020). *Systematic Review of Cybersecurity Frameworks for SMEs*. International Journal of Information Security, 19(5), 467-489.
4. Bansal, S., Choudhary, A., & Dhiman, G. (2021). *Addressing the Cybersecurity Workforce Shortage: A Review*. IEEE Security & Privacy, 19(3), 65-75.
5. Boehmer, K. (2018). *Integrating Qualitative and Quantitative Risk Assessment Methods*. Journal of Cybersecurity Research, 4(2), 123-139.
6. Burch, J., et al. (2020). *Best Practices and Frameworks for IoT Security*. Journal of Internet Services and Applications, 11(1), 1-18.
7. Cole, E., Grance, T., & Furlong, J. (2017). *Information Security and Privacy Controls for Organizations*. NIST Special Publication 800-53.
8. Cybersecurity Ventures. (2021). *Global Cybercrime Costs Projected to Reach $10.5 Trillion by 2025*. Retrieved from https://cybersecurityventures.com
9. Deogirikar, A., & Vidhate, A. (2017). *Challenges and Solutions in IoT Security*. International Journal of Advanced Research in Computer Science, 8(5), 123-130.
10. Fernandes, A., Soares, F., & Nunes, B. (2014). *A Risk Management Framework for Advanced Persistent Threats*. Information Security Journal: A Global Perspective, 23(2), 101-113.
11. Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Evaluating the Impact of Security Investments on Business Performance. Information Systems Research, 31(1), 75-93.
12. Greene, K. R., Szor, M., & Li, Z. (2019). Healthcare Sector Security Frameworks: A Comprehensive Review. Journal of Information Privacy and Security, 15(4), 199-215.
13. Gupta, S., Saini, A., & Sharma, A. (2018). Streamlining Cybersecurity Frameworks for Small Businesses. International Journal of Computer Applications, 182(26), 10-15.
14. Jouini, M., Rabai, L., & Aroua, A. (2014). Empirical Analysis of ISO 27001 Adoption in SMEs. Computers & Security, 41, 158-168.
15. Jones, A., & Estey, B. (2014). Introduction to the Factor Analysis of Information Risk (FAIR) Framework. Information Systems Security Association Journal, 12(4), 183-194.
16. Oltsik, T. (2019). Current State and Future Trends of the Cybersecurity Skills Shortage. ESG Research Report.
17. Rees, D., Wager, D., & Sokolowski, A. (2011). Bridging the Cybersecurity Gap for SMEs. Journal of Small Business and Enterprise Development, 18(3), 457-474.
18. Sadeghi, A., Wachsmann, C., & Waidner, M. (2015). Security and Privacy Challenges in Industrial IoT. 2015 2nd World Forum on Internet of Things (WF-IoT), 1-6.
19. Shackelford, S. J., et al. (2016). Managing Cybersecurity Risks Using the NIST Cybersecurity Framework. Harvard Kennedy School.
20. Shafique, M. U., et al. (2020). Real-Time Threat Intelligence for Cybersecurity Frameworks. Journal of Information Security and Applications, 52, 102-113.
21. Tharwani, H., Sharma, D., & Choudhary, A. (2022). Dynamic Cyber Threat Management Strategies. International Journal of Cybersecurity and Digital Forensics, 11(1), 45-58.
22. Yang, J., Qiu, C., & Wang, H. (2021). Integrated Cyber Risk Assessment Methods. IEEE Transactions on Dependable and Secure Computing, 18(1), 1-13.
23. Yu, S., Zhang, L., & Sun, Y. (2023). Adapting Cybersecurity Frameworks to Emerging Threats. Future Generation Computer Systems, 133, 152-166.

24. Zhang, Z., Wang, L., & Zhu, W. (2020). Incorporating Real-Time Threat Intelligence into Cybersecurity Strategies. IEEE Access, 8, 224067-224079.
25. National Institute of Standards and Technology (NIST). (2018). Improving Critical Infrastructure Cybersecurity: Framework Overview. Retrieved from https://www.nist.gov/cyberframework
26. International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013 - Information Security Management Systems. Retrieved from https://www.iso.org
27. Cloud Security Alliance (CSA). (2021). Cloud Controls Matrix (CCM) v4.0. Retrieved from https://cloudsecurityalliance.org
28. National Institute of Standards and Technology (NIST). (2023). AI Risk Management Framework (AI RMF). Retrieved from https://www.nist.gov/itl/ai-risk-management-framework
29. Gartner. (2022). Emerging AI Security Threats in Cloud Environments. Gartner Research Report.
30. IBM Security. (2021). Annual Data Breach Report: Key Insights and Trends. Retrieved from https://www.ibm.com/security/data-breach
31. McKinsey & Company. (2022). AI's Role in the Future of Cybersecurity. Retrieved from https://www.mckinsey.com
32. Verizon. (2023). Data Breach Investigations Report (DBIR). Retrieved from https://www.verizon.com/business/resources/reports/dbir/
33. Cybersecurity and Infrastructure Security Agency (CISA). (2022). Zero Trust Maturity Model. Retrieved from https://www.cisa.gov/zero-trust-maturity-model
34. Microsoft Security. (2023). AI and Cloud Security: Best Practices for Threat Mitigation. Retrieved from https://www.microsoft.com/security
35. Google Cloud Security. (2022). Developing Secure AI Solutions in Cloud Environments. Retrieved from https://cloud.google.com/security
36. Alberts, C., Dorofee, A., Killcrece, G., & Lucier, C. (2003), Octave: A Risk Management Framework for Information Security, Carnegie Mellon University.
37. AlHogail, A. (2018), The Challenges of Cybersecurity Framework Implementation in SMEs, International Journal of Computer Applications, 182(10), 1-6.
38. Alotaibi, R., Alshahrani, M., & Khan, A. (2020), Cybersecurity Frameworks for SMEs: A Systematic Review, International Journal of Information Security, 19(5), 467-489.
39. Bansal, S., Choudhary, A., & Dhiman, G. (2021), A Review of Cybersecurity Workforce Shortages, IEEE Security & Privacy, 19(3), 65-75.
40. Boehmer, K. (2018), Balancing Qualitative and Quantitative Risk Assessments, Journal of Cybersecurity Research, 4(2), 123-139.
41. Burch, J., et al. (2020), IoT Security: Frameworks and Best Practices, Journal of Internet Services and Applications, 11(1), 1-18.
42. Cole, E., Grance, T., & Furlong, J. (2017), Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53.
43. Cybersecurity Ventures. (2021), Cybercrime to Cost the World $10.5 Trillion Annually by 2025, Retrieved from [Cybersecurity Ventures](https://cybersecurityventures.com).
44. Deogirikar, A., & Vidhate, A. (2017), IoT Security Challenges and Solutions, International Journal of Advanced Research in Computer Science, 8(5), 123-130.
45. Fernandes, A., Soares, F., & Nunes, B. (2014), A Risk Management Framework for Advanced Persistent Threats, Information Security Journal: A Global Perspective, 23(2), 101-113.
46. Gordon, L. A., Loeb, M. P., & Zhou, L. (2020), The Impact of Information Security Investments on Firm Performance, Information Systems Research, 31(1), 75-93.
47. Greene, K. R., Szor, M., & Li, Z. (2019), Industry-Specific Security Frameworks: A Review of Healthcare, Journal of Information Privacy and Security, 15(4), 199-215.
48. Gupta, S., Saini, A., & Sharma, A. (2018), Simplifying Cybersecurity Frameworks for Small Businesses, International Journal of Computer Applications, 182(26), 10-15.
49. ISO (International Organization for Standardization). (2013), ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements, ISO.
50. Jouini, M., Rabai, L., & Aroua, A. (2014), Adoption of ISO 27001 in Small and Medium-Sized Enterpris