https://doi.org/10.58086/znz7-my85

AUDITING NETWORK SECURITY IN REMOTE WORK ENVIRONMENTS: A BIBLIOMETRIC REVIEW

Filipe Costa[1]✉, **Mário Dias Lousã**[1,2], **José Carlos Morais**[1,3]

[1] Instituto Superior Politécnico Gaya (ISPGAYA), Portugal.
[2] Insight - Piaget Research Center for Ecological Human Developement, Portugal.
[3] CEOS.PP, ISCAP, Polytechnic of Porto, Portugal.
✉ Corresponding authors**:** ispg2019101490@ispgaya.pt

Abstract

The remote work trend has changed the organizational network architectures of firms, thereby increasing the attack surfaces in cybersecurity and auditing. It has thus become increasingly important to understand security controls, risk management practices, and how audit mechanisms are implemented in distributed environments. This research employs a bibliometric review, conducted in accordance with the PRISMA protocol, along with a qualitative interpretative analysis to understand scientific literature on cybersecurity, network security, and auditing in remote work contexts. The Lens database was used to collect metadata for publications from 2019 to 2025, which led to a dataset of 1,868 documents. After screening and eligibility assessment, 1868 documents were included in the final bibliometric and qualitative synthesis. The results show a significant increase in research output after 2020, associated with the global expansion of remote work. The analysis also highlights gaps related to remote auditing automation and monitoring in unmanaged environments. Overall, the results underscore the strengthening of technical security measures that are closely aligned with the ongoing gaps in auditing practices, thus indicating key areas for further research and the development of professional practice.

Keywords: Compliance Monitoring; Continuous Auditing; Cybersecurity Frameworks; Endpoint Security; Zero Trust Architecture.

1. Introduction

Therefore, a bibliometric review is an invaluable tool in this context. A bibliometric study gives a detailed and organized quantitative view of the progress of scientific research on

remote work cybersecurity, the research topics that attract more scholars, the collaboration networks, and the keyword patterns that influence the development of the field. This paper uses such an approach by examining the publications stored in The Lens, a well-rounded database that merges academic research, policy documents, and technical reports. The search was done for the documents published between 2019 and 2025, which represents the period of the rise, the settling, and the fine-tuning of remote work as a standard organizational model.

To ensure methodological clarity and serve as a guide for analysis, this research is organized by the following research questions:

RQ1: What are the key cybersecurity and network security issues related to remote work that can be identified from scientific literature using bibliometric mapping and keyword co-occurrence analysis?

RQ2: What parts of the existing literature talk about the increased attack surface and the vulnerabilities arising from remote working environments?

RQ3: How far do the present cybersecurity standards and frameworks reflect the auditing challenges that have been identified in the remote and distributed work scenarios?

By integrating bibliometric indicators with a thoughtful review of cybersecurity frameworks, sectoral guidelines, and on-the-ground evidence from technical reports, this article offers a thorough understanding of how network security auditing is evolving because of the transition to remote work. Apart from determining the major risks and vulnerabilities that distributed work entails, the article is also keen on pointing out the ways in which audit processes are transformed by gradually shifting to automation, continuous monitoring, and evidence-based verification across decentralized infrastructures.

2. Methodology

The search strategy was created in an iterative manner, mixing exploratory queries with words taken from cybersecurity frameworks like ISO/IEC 27001, NIST CSF, and CIS Controls v8. The last query used in The Lens was: ("remote work" OR "work from home" OR telework OR WFH OR "remote access") AND ("network security" OR cybersecurity OR "information security" OR "data security" OR "secure communication") AND (“audit” OR “assessment” OR “monitoring” OR “compliance” OR "security management") AND ("risk

management" OR "security controls"). The query, limited to publications from 2019 to 2025, was carried out on the 30th of November 2025 and returned 1868 results, which is an indication of the rapid growth of research activities in the area since the worldwide teleworking has been expanded. The search was limited to the metadata fields: title, abstract, and keywords, and it did not include full-text search. The Lens interface filters used were Document Type → "Article"; Document Set → "All Documents"; Language → English. There were no other disciplinary, institutional, or geographic filters applied.

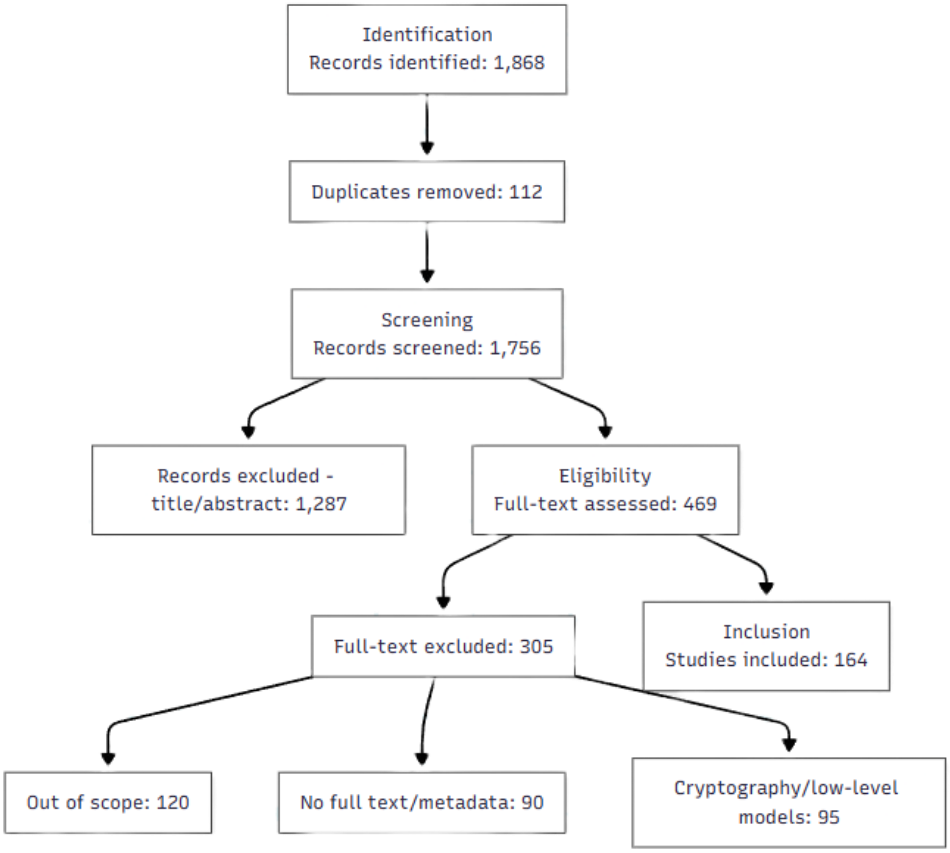

Fig 1. PRISMA Fluxogram
Source: Author's elaboration (2025).

According to the PRISMA protocol (Figure 1), after an initial metadata cleaning and consolidation process, 112 records were removed due to redundancy, resulting in 1,756 documents retained for bibliometric screening.

Next, the metadata (titles, abstracts, keywords, authorship, affiliation, and citation links) were analyzed with VOSviewer, which made it possible to create co-authorship networks and keyword co-occurrence maps. All the analyses were conducted using VOSviewer version 1.6.20. The mapping operations utilized the full counting method, which indicates that each author, keyword, or link was counted fully for every document in which it appeared.

3. Remote Work and Corporate Network Security

The bibliometric mapping that helped to qualitatively describe the literature over time, a descriptive analysis of the number of publications per year was carried out. This study reveals the development path of research on cybersecurity and remote work in a very clear way, especially showing the rise of scientific output after the worldwide change to remote work in 2020 (Figure 2).

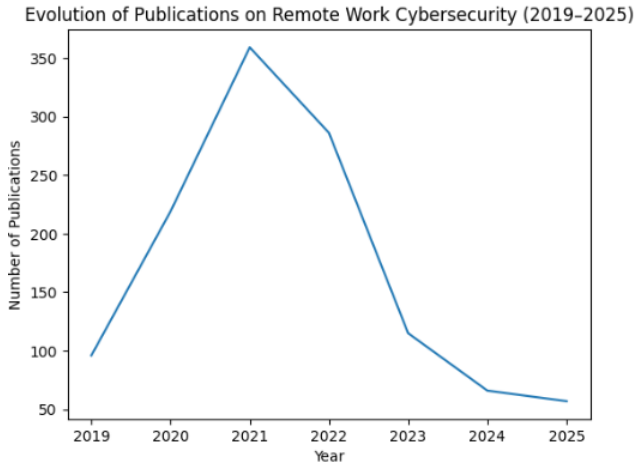

Fig 2. Evolution of Publications
Source: The Lens database (2025).

A descriptive overview of the central publication venues was also created, besides network-based visualizations, to provide a context for the spread of research in this field. Table 1 shows the journals with the greatest number of publications in the analyzed dataset, thus giving a picture of the journals that are the most influential in the academic discussion on cybersecurity, network security, and auditing in remote work environments.

Table 1. Most Impactful Journals

Journal	Total Citations
Ad Hoc Networks	3178
IEEE Access	2297
Sensors	1964
PLoS Medicine	1387
Sustainability	1353
Journal of Management Information Systems	1349
IEEE Communications Surveys & Tutorials	1324
Communications in Computer and Information Science	697
Applied Sciences	694
IFIP International Federation for Information Processing	624

Source: Authors' elaboration based on data from The Lens database (2025).

The co-authorship network uncovered several collaborative clusters that were structured around the most influential contributors, including authors linked to NIST's cybersecurity documentation. This configuration reveals the importance of standards-related research as the core of the field and visually demonstrates, through the cluster structure (Figure 3), that these distinct communities are working on cybersecurity controls, risk management, and remote working infrastructures.

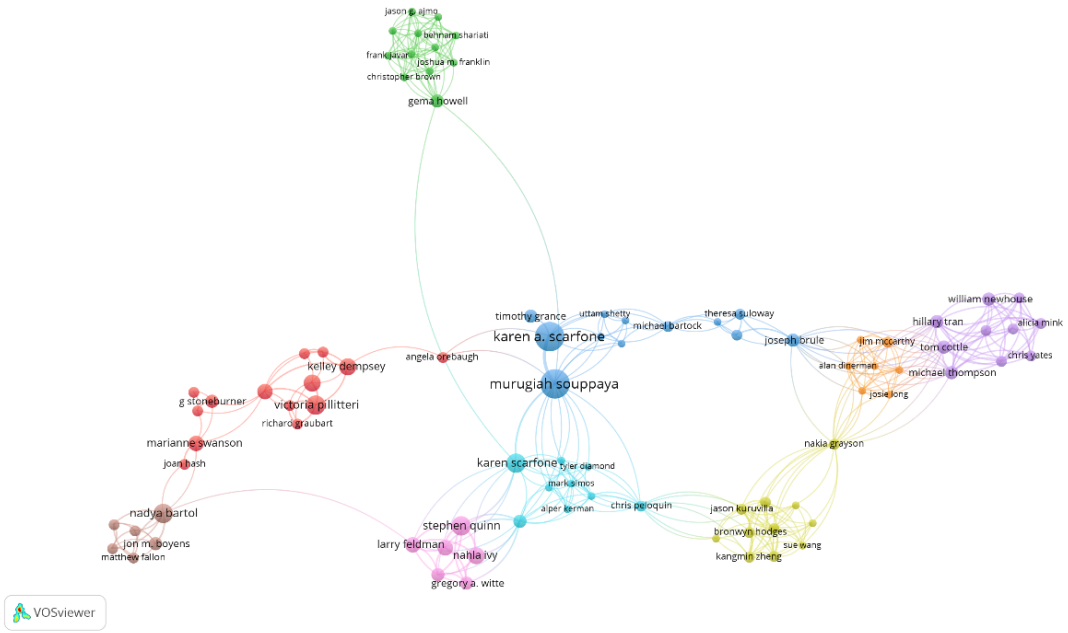

Fig 3. Authors Cluster Map
Source: Authors' elaboration based on VOSviewer outputs and The Lens metadata (2025).

3.1. Results addressing RQ1: Key cybersecurity and network security issues in remote work

The keyword co-occurrence visualization was a main instrument in reorganizing the article's analytical sections. The VOSviewer map highlighted the most frequently used keywords in the articles under review, such as "cybersecurity", "remote work", "risk management", "information security", "Zero Trust", and "endpoint security", which appeared to be the most consolidated clusters (Figure 4). These clusters were a guide for the thematic organization of sections three to six, as well as confirming the topics' relevance, such as identity management, distributed risks, human factors, and control frameworks in remote work

security. Besides, some low-frequency words like “VPN vulnerabilities”, “phishing”, and “home networks” were helpful in pointing out the necessity of technical misconfigurations and user behavior prediction.

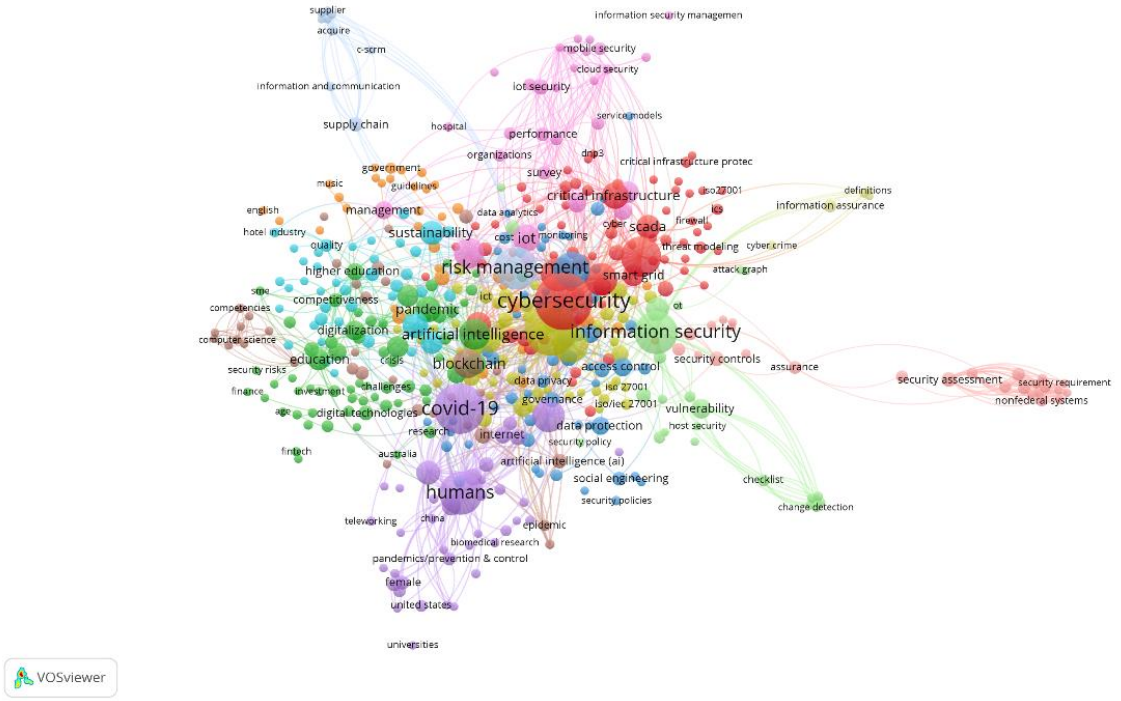

Fig 4. Keywords Cluster Map
Source: Authors’ elaboration based on VOSviewer outputs and The Lens metadata (2025).

Since 2020, organizations have become increasingly dependent on remote, hybrid, and distributed work models, a change that has significantly impacted how organizations operate and the security of their infrastructures. Remote work refers to employees performing professional activities from home, hybrid work is a mix of home-based and office-based activities, and distributed work involves teams operating with varying degrees of autonomy (Bhagat, 2023). These models have reshaped enterprise IT environments and introduce new structural and security challenges.

3.2. Results addressing RQ2: Increased attack surface and vulnerabilities in remote working environments

Human error remains a dominant factor, with studies showing that remote workers comply with security guidelines only partially (Nyarko & Fong, 2023). Home Wi-Fi networks are frequently misconfigured, often relying on old routers or default administrative passwords,

which increases the risk of cyberattacks (Klint, 2023). Mixing personal and corporate digital activities leads to additional concerns about data exposure and unauthorized access.

3.3. Results addressing RQ3: Adequacy of cybersecurity standards and frameworks for remote auditing

Distributed networks introduce vulnerabilities that differ from those typically found in traditional on-premises systems. Misconfigurations of VPN gateways, home routers, and firewalls are usually a result of the fast deployment and lack of oversight in home environments (Treacy et al., 2023). The practice of BYOD further complicates security, as personal devices generally lack enterprise-level protections such as EDR/XDR, centralized patch management, or secure configurations (Bhagat, 2023). Sharing of devices or leaving them unattended in-home settings increases exposure and is a source of physical security risks as well (Klint, 2023).

Lack of proper network segmentation makes it possible for corporate devices to be on the same networks with personal electronics and IoT appliances, which facilitates lateral movement (Silva Atencio, 2025). Security teams are having difficulties with limited visibility, as remote endpoints are often in areas with unstable connectivity or lack standard monitoring tools. Various industry reports reveal that there are persistent difficulties in log forwarding, forensic data collection, and monitoring coverage in non-controlled networks (Deloitte NASCIO Cybersecurity Study, 2024). These gaps in visibility are a direct indication of auditing processes, as auditors frequently report partial evidence and restricted access to remote configurations (Celestin, 2019).

VOSviewer's keyword co-occurrence analysis identified cybersecurity frameworks and auditing procedures as recurrent and significant themes in the bibliometric dataset. Based on these findings, sections three through six were organized according to the thematic structure derived from keyword mapping. While section three explicitly addresses the results related to the research questions, sections four and five provide a more detailed analysis of auditing requirements and the applicability of existing cybersecurity standards, such as ISO/IEC 27001 and the NIST Cybersecurity Framework, in remote and distributed work environments. In this context, although current cybersecurity frameworks remain applicable, their effective implementation increasingly requires the integration of governance-oriented

controls with advanced technical solutions, including Zero Trust architectures and continuous endpoint monitoring tools.

4. Auditing in Remote Work Environments

4.1 Traditional security auditing

Traditionally, security auditing relied on centralized systems, standardized device baselines, and direct access to corporate infrastructures. On-site audits followed structured stages such as defining the scope, reviewing documents, conducting interviews, gathering evidence, and testing configurations (Ilori et al., 2022). The methods used were built on the idea that resources were kept inside a secure perimeter and managed through corporate tools.

Under these models, system logs, configuration files, and event reports were collected from authenticated connections to internal networks. Compliance verification relied heavily on the direct observation of security measures, patch management activities, and intrusion protection. As the infrastructures were centrally managed, auditors were able to work in safe and less challenging contexts.

4.2 Challenges of auditing remote environments

Traditional audit models, which were not designed for decentralized contexts, have been under significant pressure due to remote work. One of the main problems is that it is difficult to get reliable evidence from devices that are operating outside of corporate networks. Remote endpoints may not be permanently connected and enterprise-level monitored, so there may be gaps, delays, and inconsistencies in the data obtained from the audit (Celestin, 2019).

Besides, the lack of visibility is also a major challenge. Device logs are often incomplete and not forwarded to SIEM systems due to bandwidth limitations or misconfigurations. Home networks are generally non-segmented, and even when they are securely configured, auditors find it hard to determine the efficiency of security measures because they must rely on these networks (Klint, 2023). Without reliable telemetry, audit teams hardly find a way to carry out patching, encryption, authentication, and compliance mechanisms.

The problem of user-managed devices has been around for a very long time, and now it has become worse since remote workers might be sharing hardware, turning off security features, postponing updates, or even installing unauthorized software, thus breaking the assumption of controlled configurations and enforced baselines. The authentication and access management processes have been made difficult by the adoption of cloud platforms and federated identity systems. This transition requires MFA, secure channels, and continuous verification. Audits done remotely are still hard when people use outdated VPNs or unsegmented access paths (Allah Rakha, 2023). Patch management is made more difficult by poor or intermittent connectivity leading to devices being left unpatched or outdated (Treacy et al., 2023).

Forensic validation is also confronted with similar issues: severely limited physical or administrative access makes it particularly difficult to confirm logs, check system integrity, and reconstruct incidents. These constraints point to the necessity of modifying audit methods so that they are in line with the distributed infrastructures in contemporary remote work contexts.

4.3 Emerging audit requirements

As companies move to remote and hybrid work styles, the auditing procedures should be changed accordingly. One of the main necessities is utilizing the tools for remote auditing, which should be able to collect the evidence in a standardized, automated manner and be tamper resistant. These are secure remote-access platforms, cloud-integrated dashboards, and endpoint-monitoring systems (Celestin, 2019).

Automation is the main actor in the play. Contemporary auditing is turned more and more towards automated methods of evidence gathering, configuration scanning, and continuous monitoring that can be accomplished using technologies such as EDR/XDR, SIEM, and cloud-native telemetry. The research is quite clear in its findings to support this statement that the automation elevates the exactness of detection and lessens the audit fatigue by on-the-spot identification of anomalies (Ilori et al., 2022).

Accountability for remote work must also be established through proper governance policies. The organizations have implemented policies that regulate the configurations of secure home networks, requirements for endpoint protection, communication by means of

encrypted channels, and procedures for identity verification (Rakha, 2023). The policies must be subject to audit and should be convertible as far as the changes in threats are concerned.

Moreover, it is also very important for the company to be closely linked with the endpoint-security technologies. EDR/XDR technologies offer the transparency necessary to confirm that the latest changes have been made, that the system is free of malware, and that access control requirements have been met, which in turn contributes to the reduction of the auditing evidence shortages (Silva Atencio, 2025).

Considerations related to the human factor should not be forgotten as well. Behavioral risks are intensified by remote work; therefore, auditors need to assess training effectiveness, phishing-resistance programs, and compliance with remote work guidelines (Bhagat, 2023).

In addition, cybersecurity frameworks such as ISO/IEC 27001, NIST CSF, and CIS Controls are putting an ever-greater emphasis on risk-based and continuous monitoring approaches that are very compatible with remote environments (Folorunso et al., 2024). They provide support for adaptable audit models that combine governance reviews, technical controls, and real-time telemetry.

5. Security Frameworks and Their Applicability to Remote Work

The literature obtained from bibliometric research illustrates how cybersecurity frameworks-ISO/IEC 27001, NIST Cybersecurity Framework (CSF), and CIS Controls-have been instrumental in defining security and auditing practices for distributed environments. The central theme, however, revolves around the fact that these frameworks were initially conceptualized for more centralized infrastructures. Still, their fundamental ideas are often mentioned in the documents analyzed, suggesting that they are still viable models for security governance in remote work (Bhagat, 2023).

To sum up, the research works demonstrate that although the present frameworks are still applicable, their efficient implementation in remote work situations requires additional measures and appropriate contextual adaptation. Integrated interpretation, as supported by bibliometric evidence, is a strong argument for the necessity of combining governance, risk-based, and technical layers in remote work security rather than depending on a single framework.

6. Discussion

The keyword co-occurrence analysis (Figure 4) reveals that the most central concepts, remote work, cybersecurity, network security, risk management, and audit, are the main core around which other themes revolve. This suggests that literature is increasingly combining the aspects of technical risks, access control, and auditing practices for the formation of a single conceptual framework. The emergence of several clusters also implies that there is a certain degree of fragmentation in the field, with some research focusing on technical vulnerabilities and others emphasizing organizational and human-factor aspects. In addition, the bibliometric evidence suggests relevant geographical and institutional differences in how remote work cybersecurity is approached. Publications originating from North America and Northern Europe tend to emphasize technical controls, automation, and Zero Trust architectures, while studies from other regions place greater focus on regulatory compliance, privacy, and legal constraints. This divergence reflects distinct organizational cultures, regulatory environments, and maturity levels in cybersecurity governance. From an auditing perspective, these differences highlight the need for flexible audit frameworks that can accommodate both highly automated technical environments and compliance-driven contexts without compromising assurance quality.

7. Conclusions

The bibliometric review offered through this article provides a comprehensive understanding of how remote work has changed network security risks, as well as the auditing practices that are necessary to tackle them. The Lens dataset and VOSviewer visualizations (Figures 1 and 2) provided the results that depicted a research landscape influenced by operational, regulatory, and technological pressures.

References

Bhagat, N. (2023). Cybersecurity in a Remote Work Era: Strategies for Securing Distributed Workforces. *Review Article Nikhil Bhagat, Sr. Technical Account Manager Network Specialist Independent Scholar*, *2*(2), 1–5. https://doi.org/10.47363/JMCA/2023(2)E137

Celestin, M., & Vanitha, N. (2019). The rise of remote auditing: Challenges, opportunities, and best practices. *International Journal of Computational Research and Development*, *4*(2), 13-20.

Deloitte NASCIO Cybersecurity Study. (2024). https://www.deloitte.com/us/en/ Insights/industry/government-public-sector-services/2024-deloitte-nascio-cybersecurity-study.html

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews*, *24*(1), 2582–2595. https://doi.org/10.30574/wjarr.2024.24.1.3169

Ilori, O., Lawal, C. I., Friday, S. C., Isibor, N. J., & Eke, E. C. C.-. (2022). Cybersecurity Auditing in the Digital Age: A Review of Methodologies and Regulatory Implications. *Journal of Frontiers in Multidisciplinary Research*, *3*(1), 174–187. https://doi.org/10.54660/.ijfmr.2022.3.1.174-187

Klint, R. (2023). Cybersecurity in Home-Office Environments. *DiVA Portal*, 53. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1779054&dswid=-4035

Nyarko, D. A., & Fong, R. C.-W. (2023). Cyber security compliance among remote workers. Em *Advanced Sciences and Technologies for Security Applications* (pp. 343–369). Springer International Publishing.

Rakha, N. A. (2023). Ensuring cyber-security in remote workforce: legal implications and international best practices. *International Journal of Law and Policy*, *1*(3), 1-19.

Silva Atencio, G. (2025). Effective Cybersecurity Strategies for Mitigating Remote Work and IoT Risks in Enterprises. *FinTech and Sustainable Innovation*. https://doi.org/10.47852/bonviewfsi52025962

Treacy, S., Sabu, A., Bond, T., O'Sullivan, J., Sullivan, J., & Sylvester, P. (2023, February). Organizational cybersecurity post the pandemic: an exploration of remote working risks and mitigation strategies. In *International Conference on Cyber Warfare and Security* (Vol. 18, No. 1, pp. 394-401). Academic Conferences International Limited.