Volume 11, Issue 6, June – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

Adoption of ISO/IEC 27001 in Mozambique: Challenges, Opportunities, and Implications for Information Security Governance

Julião Artur Francisco Mussa[1]

[1]Rovuma University

Publication Date: 2026/07/09

Abstract: The increasing digitalization of economic and social activities has intensified the importance of information security as a strategic component of organizational governance and digital resilience. In this context, ISO/IEC 27001 has emerged as the leading international standard for implementing Information Security Management Systems (ISMS), supporting organizations in managing cybersecurity risks, enhancing regulatory compliance, and strengthening digital trust. Despite its global relevance, limited research has examined the factors influencing ISO/IEC 27001 adoption in developing countries, particularly within the Mozambican context. This study analyzes the challenges, opportunities, and implications associated with the adoption of ISO/IEC 27001 in Mozambique. An integrative literature review and documentary analysis were conducted, drawing upon scientific publications, institutional reports, regulatory frameworks, and policy documents. The analysis was guided by the Technology–Organization–Environment (TOE) framework and the Technology Acceptance Model (TAM), enabling the examination of technological, organizational, environmental, and behavioral determinants of adoption. The findings indicate that ISO/IEC 27001 adoption is influenced by a combination of factors, including technological infrastructure, organizational capabilities, financial resources, regulatory conditions, management commitment, and stakeholders' perceptions of usefulness and implementation complexity. Key barriers include the shortage of qualified cybersecurity professionals, implementation and certification costs, infrastructural limitations, and low levels of cybersecurity maturity. Conversely, significant opportunities were identified, including enhanced digital trust, improved regulatory compliance, stronger risk management practices, increased organizational competitiveness, and greater resilience against cyber threats. The study concludes that ISO/IEC 27001 represents a strategic instrument for strengthening information security governance in Mozambique. The findings contribute to the literature on information security governance and technology adoption by integrating the TOE and TAM frameworks within a developing-country context. Practical recommendations are provided for organizations, policymakers, and regulatory institutions seeking to foster cybersecurity maturity and sustainable digital transformation.

Keywords: *ISO/IEC 27001; Information Security Governance; Information Security Management Systems (ISMS); Cybersecurity; Technology–Organization–Environment (TOE); Technology Acceptance Model (TAM); Digital Transformation; Mozambique.*

How to Cite: Julião Artur Francisco Mussa (2026) Adoption of ISO/IEC 27001 in Mozambique: Challenges, Opportunities, and Implications for Information Security Governance. *International Journal of Innovative Science and Research Technology*, 11(6), 2983-2994. https://doi.org/10.38124/ijisrt/26jun1208

I. INTRODUCTION

Digital transformation has profoundly reshaped business models, public services, and social interactions worldwide. In Mozambique, the increasing adoption of Information and Communication Technologies (ICT), coupled with the expansion of Internet access, digital financial services, e-government initiatives, and cloud computing, has contributed significantly to economic development and digital inclusion. However, this process has also increased the exposure of public and private organizations to information security threats, including cyberattacks, data breaches, electronic fraud, and disruptions to critical services.

Information security has therefore become a strategic concern for organizations that increasingly rely on digital systems to support their operations. In this context, the implementation of effective information security management mechanisms plays a fundamental role in protecting the confidentiality, integrity, and availability of information assets. Among the most widely recognized international frameworks for this purpose is the ISO/IEC 27001 standard, which establishes the requirements for implementing an Information Security Management System (ISMS) based on a systematic approach to risk management and continuous improvement.

The adoption of ISO/IEC 27001 has been widely promoted across different countries as an instrument for

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

strengthening information security governance, improving regulatory compliance, and enhancing digital trust. International studies indicate that certified organizations demonstrate a greater capacity to identify, assess, and mitigate security risks while benefiting from competitive advantages associated with increased credibility and compliance with legal and regulatory requirements. Nevertheless, the adoption of this standard is influenced by several technological, organizational, and environmental factors that vary significantly across economic and institutional contexts.

In developing countries, particularly within the African continent, the implementation of ISO/IEC 27001 faces challenges related to infrastructural limitations, shortages of qualified professionals, certification costs, and limited organizational cybersecurity maturity. Although several studies have examined the adoption of the standard in different international contexts, the scientific literature concerning its implementation in Mozambique remains limited and fragmented. This gap hinders a comprehensive understanding of the factors that influence the adoption of the standard and its potential implications for information security governance in the country.

Against this backdrop, there is a need to systematically understand the challenges and opportunities associated with the adoption of ISO/IEC 27001 in Mozambique, as well as its potential contribution to strengthening national cybersecurity capabilities and digital governance.

➢ *Accordingly, this Study Seeks to Answer the Following Research Question:*

- What are the main challenges, opportunities, and implications of adopting the ISO/IEC 27001 standard for information security governance in Mozambique?

➢ *To Address this Question, the Study Pursues the Following General Objective:*

To analyze the challenges, opportunities, and implications of ISO/IEC 27001 adoption in Mozambique, considering the technological, organizational, and environmental factors that influence its implementation.

➢ *Specifically, the Study Aims to:*

- Identify the main challenges that hinder the adoption of ISO/IEC 27001 in Mozambique;
- Analyze the opportunities arising from the implementation of the standard in public and private organizations;
- Examine the role of the legal, regulatory, and institutional framework in promoting information security;
- Assess the implications of ISO/IEC 27001 adoption for information security governance within the Mozambican context;
- Propose recommendations that may support policymakers, regulators, and organizations in implementing Information Security Management Systems (ISMS).

From a theoretical perspective, this study is grounded in the Technology–Organization–Environment (TOE) framework and the Technology Acceptance Model (TAM), both of which are widely used in the literature to explain the adoption of technologies, standards, and organizational practices. The integration of these models enables a comprehensive understanding of technological and organizational factors, as well as stakeholders' perceptions regarding the usefulness and ease of implementing the ISO/IEC 27001 standard.

The main scientific contribution of this study lies in providing a contextualized analysis of ISO/IEC 27001 adoption in Mozambique by integrating perspectives from information security governance, risk management, and digital transformation. Furthermore, the study contributes to the still limited body of knowledge on information security in Portuguese-speaking African countries, offering valuable evidence for researchers, practitioners, and public policymakers.

II. LITERATURE REVIEW

➢ *Information Security and Organizational Governance*

The growing dependence of organizations on digital technologies has positioned information security as a strategic element for business sustainability and operational continuity. Information security can be defined as the set of policies, practices, and mechanisms designed to ensure the confidentiality, integrity, and availability of information, protecting it against unauthorized access, improper modification, disclosure, and service disruption.

Over the last decade, information security has evolved from a predominantly technical concern to a strategic and organizational priority. According to Calder and Watkins (2015), an organization's ability to safeguard its information assets directly influences its reputation, competitiveness, and regulatory compliance. In this regard, information security governance has emerged as a critical mechanism for aligning security objectives with broader organizational goals.

The literature suggests that organizations with formal information security governance structures exhibit greater capabilities in risk management, incident response, and regulatory compliance. Consequently, the adoption of internationally recognized standards has become one of the most effective strategies for enhancing organizational maturity in information security management.

➢ *The ISO/IEC 27001 Standard and Information Security Management Systems*

ISO/IEC 27001 is widely recognized as the leading international standard for the implementation of Information Security Management Systems (ISMS). Developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the standard establishes requirements for the design,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

implementation, operation, monitoring, review, maintenance, and continual improvement of information security processes.

The latest version, ISO/IEC 27001:2022, reinforces the risk-based approach and introduces new controls related to cloud computing, threat intelligence, continuous monitoring, and data protection. These updates reflect the increasing complexity of digital environments and the growing need for robust mechanisms to address emerging cybersecurity threats.

Numerous studies have highlighted the benefits associated with ISO/IEC 27001 implementation, including:

- Reduction in the likelihood of security incidents;
- Improved legal and regulatory compliance;
- Increased trust among customers and business partners;
- Strengthened risk management capabilities;
- Enhanced organizational reputation and credibility.

However, the adoption of the standard is not determined solely by its technical advantages. Factors related to organizational resources, technological capabilities, regulatory environments, and stakeholder perceptions play a decisive role in the implementation process.

➢ *Challenges and Critical Factors Influencing ISO/IEC 27001 Adoption*

The international literature identifies multiple factors that influence the adoption of ISO/IEC 27001, particularly in developing economies.

Da Veiga and Eloff (2007) argue that the shortage of specialized competencies represents one of the most significant barriers to the effective implementation of Information Security Management Systems. This challenge is especially pronounced in emerging economies, where the availability of certified information security professionals remains limited.

Similarly, Heras-Saizarbitoria and Boiral (2013) identify implementation and certification costs as major obstacles to the adoption of ISO/IEC 27001, particularly among small and medium-sized enterprises (SMEs). These costs include expenditures related to specialized consultancy services, employee training, security technologies, internal process restructuring, and periodic external audits.

Other studies emphasize the influence of organizational culture on implementation outcomes. According to Humphreys (2008), resistance to change and insufficient commitment from senior management can significantly undermine the effectiveness of information security initiatives and compromise certification efforts.

Despite these challenges, several authors argue that the strategic benefits associated with ISO/IEC 27001 certification tend to outweigh the initial investment costs, particularly in organizations operating within highly regulated environments or sectors exposed to elevated cybersecurity risks.

➢ *ISO/IEC 27001 Adoption in Developing Countries*

In developing countries, the implementation of ISO/IEC 27001 is often constrained by additional structural factors, including infrastructural deficiencies, limited digital maturity, and inadequate public cybersecurity policies.

Studies conducted in Namibia, South Africa, Mauritius, and other countries within the Southern African Development Community (SADC) reveal common challenges associated with financial constraints, shortages of qualified specialists, and the absence of government incentives supporting information security certification initiatives.

- *Conversely, the Benefits Observed in these Contexts Include:*

✓ Strengthening digital trust and confidence;
✓ Enhancing international competitiveness;
✓ Improving organizational governance practices;
✓ Facilitating regulatory compliance;
✓ Attracting foreign direct investment.

Although evidence regarding the positive impacts of ISO/IEC 27001 certification has steadily increased across different African contexts, research specifically addressing Mozambique remains scarce. This gap highlights the need for context-specific studies capable of providing a deeper understanding of the factors influencing the adoption and effectiveness of information security standards within the country.

➢ *The Technology–Organization–Environment (TOE) Framework and the Technology Acceptance Model (TAM)*

The Technology–Organization–Environment (TOE) framework and the Technology Acceptance Model (TAM) are among the most widely employed theoretical frameworks for analyzing the adoption of technological innovations and information systems.

The TOE framework, proposed by Tornatzky and Fleischer (1990), examines how three contextual dimensions influence an organization's decision to adopt and implement innovations:

- *Technological Context*

Refers to both internal and external technologies relevant to the organization, including existing technological capabilities and available technological solutions within the market.

- *Organizational Context*

Encompasses organizational characteristics such as structure, size, human resources, financial capacity, managerial support, and organizational culture.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

- *Environmental Context*

Includes external factors such as competitive pressure, government support, regulatory requirements, industry characteristics, and relationships with stakeholders.

In contrast, the Technology Acceptance Model (TAM), developed by Davis (1989), focuses on individual users' perceptions regarding the adoption and use of new technologies. TAM proposes that the intention to use a technology is primarily influenced by two key constructs:

- *Perceived Usefulness (PU)*

The degree to which an individual believes that using a particular system will enhance job performance and organizational effectiveness.

- *Perceived Ease of Use (PEOU)*

The degree to which an individual believes that using a particular system will be free of effort and easy to understand and operate.

The integration of TOE and TAM provides a comprehensive analytical framework for examining the adoption of ISO/IEC 27001 by simultaneously considering contextual factors (technological, organizational, and environmental) and individual perceptions regarding the usefulness and ease of implementation of the standard.

Such an integrated approach is particularly relevant in developing-country contexts, where infrastructural conditions, institutional environments, organizational capabilities, and stakeholder perceptions may significantly influence both the acceptance and successful implementation of international information security standards. Consequently, the combined TOE–TAM perspective offers a robust theoretical foundation for understanding the determinants of ISO/IEC 27001 adoption in Mozambique and other emerging economies.

III. METHODOLOGY

➢ *Research Design*

This study adopted a qualitative research approach based on an integrative literature review and documentary analysis. This methodological strategy enables the systematic synthesis and critical evaluation of existing knowledge concerning the adoption of ISO/IEC 27001, while identifying research gaps, emerging trends, and context-specific factors relevant to Mozambique.

The integrative literature review followed the methodological framework proposed by Mendes, Silveira, and Galvão (2008), comprising the following stages:

- Identification of the research topic and formulation of the research question;
- Definition of inclusion and exclusion criteria;
- Specification of the information to be extracted from the selected studies;
- Data analysis and synthesis;
- Presentation and discussion of findings.

This approach was considered appropriate due to the limited availability of empirical studies specifically addressing ISO/IEC 27001 adoption in Mozambique and the need to integrate evidence from both academic and institutional sources.

➢ *Data Sources*

Data were collected from scientific databases and institutional documents to ensure comprehensive coverage of both academic and practical perspectives regarding information security governance and ISO/IEC 27001 adoption.

- *The Scientific Databases Consulted Included:*

✓ Google Scholar;
✓ IEEE Xplore;
✓ ScienceDirect;
✓ SpringerLink;
✓ Scopus;
✓ Web of Science;
✓ ACM Digital Library.

- *To Complement the Scientific Literature, Institutional and Policy-Related Documents were Collected from:*

✓ National Institute of Information and Communication Technologies (INTIC);
✓ National Institute for Standardization and Quality (INNOQ);
✓ International Telecommunication Union (ITU);
✓ International Organization for Standardization (ISO);
✓ World Bank;
✓ African Union.

The inclusion of institutional documents enabled a broader understanding of the Mozambican regulatory, technological, and policy environment related to information security and digital transformation.

➢ *Search Strategy*

A systematic search strategy was employed using combinations of keywords in both English and Portuguese. Boolean operators were applied to maximize the retrieval of relevant studies.

- *The Primary Search Expression was Structured as Follows:*

("ISO/IEC 27001" OR "Information Security Management System" OR "ISMS")

AND

("Mozambique" OR "SADC" OR "Developing Countries")

AND

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

("Adoption" OR "Implementation" OR "Challenges" OR "Opportunities" OR "Information Security Governance")

Additional searches were conducted using related terms to ensure comprehensive coverage of the literature.

➢ *Inclusion and Exclusion Criteria*

To ensure the quality and relevance of the reviewed literature, explicit inclusion and exclusion criteria were established.

- *Inclusion Criteria*

The following types of documents were considered eligible:

✓ Peer-reviewed journal articles;
✓ Academic theses and dissertations;
✓ Technical reports published by recognized institutions;
✓ Publications issued between 2015 and 2026;
✓ Studies addressing ISO/IEC 27001, Information Security Management Systems (ISMS), information security governance, and cybersecurity;
✓ Research focusing on developing countries, particularly within the Southern African Development Community (SADC) region.

- *Exclusion Criteria*

The following documents were excluded:

✓ Publications without full-text availability;
✓ Duplicate studies;
✓ Documents lacking direct relevance to the research objectives;
✓ Opinion papers without scientific evidence;
✓ Commercial or promotional materials.

➢ *Study Selection Process*

The study selection process followed the recommendations established by the PRISMA 2020 framework (Page et al., 2021), ensuring transparency and methodological rigor.

Initially, 184 records were identified through database searches and institutional sources. After removing duplicates, 151 records remained for screening.

The screening of titles and abstracts resulted in the identification of 79 potentially relevant studies. Subsequently, full-text assessments were conducted, leading to the final inclusion of 46 studies in the qualitative analysis.

➢ *Study Selection Summary*

Table 1 Study Selection Summary

Stage	Number of Documents
Records identified	184
Duplicates removed	33
Records screened	151
Full-text studies assessed	79
Studies excluded after full-text review	33
Studies included in the review	46

The PRISMA process contributed to improving the transparency, reproducibility, and reliability of the review.

➢ *Conceptual Research Model*

This study was theoretically grounded in the integration of two widely recognized frameworks in technology adoption research: the Technology–Organization–Environment (TOE) framework and the Technology Acceptance Model (TAM).

- *Technology–Organization–Environment (TOE)*

The TOE framework was employed to analyze factors associated with:

✓ Technological context;
✓ Organizational context;
✓ Environmental context.

This framework enables the examination of organizational adoption decisions within their broader technological and institutional environments.

- *Technology Acceptance Model (TAM)*

The TAM framework was utilized to analyze factors related to:

✓ Perceived Usefulness (PU);
✓ Perceived Ease of Use (PEOU).

The model provides insights into stakeholders' perceptions regarding the value and complexity associated with implementing ISO/IEC 27001.

The integration of TOE and TAM facilitated a multidimensional analysis of the factors influencing ISO/IEC 27001 adoption in Mozambique.

➢ *Analytical Framework*

Based on the literature review and the integrated TOE–TAM framework, an analytical framework was developed to guide data coding, categorization, and interpretation.

- *Technological Dimension*

✓ Technological Infrastructure: Availability and maturity of technological resources and information systems.
✓ Security Technologies: Existence of mechanisms for protection, monitoring, and incident detection.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

- *Organizational Dimension*

✓ Financial Resources: Organizational capacity to invest in ISO/IEC 27001 implementation.
✓ Human Resources: Availability of qualified information security professionals.
✓ Security Culture: Degree of organizational awareness and commitment to information security.
✓ Management Support: Level of involvement and commitment from senior leadership.

- *Environmental Dimension*

✓ Regulatory Environment: Information security laws, regulations, and public policies.
✓ Competitive Pressure: Market demands and partner requirements.
✓ Institutional Support: Government incentives and capacity-building initiatives.

- *TAM Constructs*

✓ Perceived Usefulness: Expected benefits associated with ISO/IEC 27001 certification.
✓ Perceived Ease of Use: Perceived complexity of implementation.

- *Outcome Variable*

✓ ISO/IEC 27001 Adoption: Organizational decision to implement the standard.

- *Impact Variable*

✓ Information Security Governance: Effects of adoption on risk management, compliance, operational resilience, and digital trust.

➢ *Data Analysis Procedures*

The collected data were analyzed using Thematic Analysis, following the methodological guidelines proposed by Braun and Clarke (2006).

- *The Analysis Involved the Following Stages:*

✓ Familiarization with the data through comprehensive reading of the selected documents;
✓ Initial coding based on predefined analytical categories;
✓ Identification and grouping of recurring themes;
✓ Review and refinement of themes;
✓ Interpretation of findings within the theoretical perspectives provided by TOE and TAM.

The thematic analysis enabled the identification of recurring patterns associated with the challenges, opportunities, and governance implications of ISO/IEC 27001 adoption in Mozambique.

The interpretation of findings focused on understanding the relationships between technological, organizational, environmental, and behavioral factors influencing implementation processes.

➢ *Scientific Rigor and Trustworthiness*

To enhance the credibility, reliability, and validity of the study, several methodological rigor strategies were adopted.

First, source triangulation was employed by combining evidence from scientific literature, institutional reports, policy documents, and regulatory frameworks. This approach reduced the risk of relying on a single source of information and strengthened the robustness of the findings.

Second, transparent inclusion and exclusion criteria were applied throughout the review process to minimize selection bias and improve reproducibility.

Third, the analytical framework derived from the TOE and TAM models provided a structured basis for data coding and interpretation, enhancing theoretical consistency.

Finally, the use of the PRISMA framework contributed to methodological transparency by documenting each stage of the study selection process.

Collectively, these measures increased the trustworthiness of the findings and strengthened the scientific rigor of the research.

IV. RESULTS AND DISCUSSION

➢ *Overview of the Findings*

The analysis of the selected studies enabled the identification of a set of factors influencing the adoption of ISO/IEC 27001 in Mozambique. Based on the analytical framework grounded in the Technology–Organization–Environment (TOE) framework and the Technology Acceptance Model (TAM), the findings were grouped into five major dimensions: technological factors, organizational factors, environmental factors, behavioral factors, and the impacts of ISO/IEC 27001 adoption on information security governance.

The results indicate that the adoption of ISO/IEC 27001 is simultaneously influenced by internal organizational conditions, characteristics of the external environment, and the perceptions of stakeholders involved in the implementation process. These findings reinforce the multidimensional nature of information security governance and highlight the importance of considering both contextual and behavioral determinants when analyzing the adoption of international security standards.

➢ *Technological Factors Influencing ISO/IEC 27001 Adoption*

- *Technological Infrastructure*

Technological infrastructure emerged as one of the primary determinants of ISO/IEC 27001 adoption. The reviewed studies indicate that many Mozambican organizations continue to face challenges related to the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

modernization of information systems, security monitoring capabilities, and technologies designed to protect digital assets.

Although significant progress has been observed in the digitalization of public and private services, infrastructural limitations remain evident, particularly outside major urban centers. These limitations directly affect organizations' capacity to implement the security controls required by ISO/IEC 27001 and to maintain an effective Information Security Management System (ISMS).

These findings support the assumptions of the TOE framework, according to which technological readiness and infrastructure availability constitute critical determinants of organizational innovation adoption.

- *Security Technologies and Risk Management Capabilities*

The analysis further revealed that organizations already employing formal risk management practices, security monitoring mechanisms, and access control systems demonstrate a greater propensity to adopt ISO/IEC 27001.

The existence of structured security processes facilitates the integration of ISMS requirements, reducing implementation complexity and increasing the likelihood of successful certification. Organizations with mature security practices tend to perceive the standard as a natural extension of their existing governance mechanisms rather than as an entirely new organizational initiative.

This finding suggests that technological preparedness plays a significant role in accelerating the implementation and institutionalization of information security standards.

➢ *Organizational Factors*

- *Shortage of Qualified Human Resources*

The lack of qualified information security professionals was the most frequently cited challenge across the reviewed literature. The findings indicate that Mozambique faces a shortage of specialists certified in ISO standards, information systems auditing, cybersecurity management, and risk governance.

This limitation affects not only the initial implementation of ISO/IEC 27001 but also the long-term maintenance and continuous improvement of Information Security Management Systems. The shortage of skilled personnel increases organizational dependence on external consultants, raising implementation costs and potentially compromising sustainability.

These findings are consistent with studies conducted in other African countries, where the cybersecurity skills gap has been identified as a major obstacle to the adoption of international information security standards.

- *Financial Resources and Certification Costs*

The costs associated with ISO/IEC 27001 implementation emerged as another critical organizational challenge. The analysis indicates that expenditures related to consultancy services, staff training, security technologies, internal audits, and certification processes represent substantial barriers for both public institutions and private enterprises.

The burden is particularly significant for small and medium-sized enterprises (SMEs), which often operate under constrained financial conditions and limited access to specialized expertise.

The findings confirm that financial capacity exerts a direct influence on adoption decisions, supporting previous research that identifies resource availability as a key predictor of technology and standards adoption.

- *Organizational Culture and Management Commitment*

Another significant factor identified was the maturity of organizational security culture. Organizations demonstrating higher levels of cybersecurity awareness and stronger engagement from senior management were more likely to pursue ISO/IEC 27001 implementation.

The findings suggest that information security is still frequently perceived as a purely technical responsibility rather than a strategic governance issue. Such perceptions limit the integration of security objectives into broader organizational decision-making processes.

These results reinforce the importance of developing governance models that actively promote executive involvement and foster a security-oriented organizational culture.

➢ *Environmental Factors*

- *Regulatory and Institutional Framework*

The results indicate that the regulatory environment significantly influences ISO/IEC 27001 adoption. Legislative developments such as the Electronic Transactions Law, the National Cybersecurity Strategy, and emerging personal data protection initiatives represent important steps toward strengthening Mozambique's digital security ecosystem.

Nevertheless, the reviewed studies reveal persistent challenges related to the effective implementation and enforcement of existing policies, as well as the absence of specific mechanisms designed to encourage information security certification.

These findings suggest that while the regulatory framework is evolving positively, further institutional support is required to facilitate broader adoption of internationally recognized security standards.

- *Competitive Pressure and Market Requirements*

The analysis demonstrates that organizations operating in highly regulated sectors—such as banking, telecommunications, and digital services—face stronger pressures to align with international security standards.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

The need to demonstrate compliance, reliability, and trustworthiness to international partners and customers has emerged as a significant driver of ISO/IEC 27001 adoption. In many cases, certification is perceived not only as a security measure but also as a strategic business requirement that enhances market credibility and competitiveness.

This finding supports the TOE framework's proposition that external environmental pressures significantly influence organizational adoption decisions.

➢ *Behavioral Factors: Insights from the Technology Acceptance Model (TAM)*

- *Perceived Usefulness*

The reviewed studies reveal a broad recognition among managers and decision-makers of the benefits associated with ISO/IEC 27001 implementation.

✓ *The Most Frequently Cited Benefits Include:*

- Improved risk management capabilities;
- Enhanced protection of information assets;
- Increased customer trust and confidence;
- Improved regulatory compliance;
- Strengthened organizational reputation.

The perception of these benefits positively influences organizational intentions to adopt the standard. Managers generally associate ISO/IEC 27001 certification with improved governance, operational resilience, and long-term organizational sustainability.

These findings are consistent with TAM, which posits that perceived usefulness is one of the strongest predictors of technology adoption and acceptance.

- *Perceived Ease of Use*

Despite recognizing the benefits of ISO/IEC 27001, many managers perceive its implementation as a complex and resource-intensive process.

The perceived complexity associated with risk assessments, documentation requirements, control implementation, internal audits, and certification procedures discourages some organizations from initiating adoption processes, particularly those with lower levels of technological and organizational maturity.

This finding confirms TAM's assumption that perceived ease of use significantly influences acceptance behavior and adoption intentions.

Organizations are more likely to embrace ISO/IEC 27001 when implementation processes are perceived as manageable and when adequate support mechanisms are available.

➢ *Implications of ISO/IEC 27001 Adoption for Information Security Governance*

The analysis indicates that ISO/IEC 27001 adoption can generate substantial improvements in information security governance within Mozambique.

- *The Principal Benefits Identified Include:*

✓ Strengthened risk management practices;
✓ Enhanced internal control mechanisms;
✓ Improved compliance with legal and regulatory requirements;
✓ Increased digital trust;
✓ Greater operational resilience and business continuity;
✓ Enhanced organizational competitiveness.

The findings suggest that ISO/IEC 27001 should not be viewed merely as a technical or compliance-oriented framework. Rather, it should be regarded as a strategic governance instrument capable of supporting organizational transformation and sustainable digital development.

Within this context, ISO/IEC 27001 emerges as a valuable mechanism for supporting Mozambique's digital transformation agenda by fostering safer, more resilient, and trustworthy digital environments.

➢ *Integrated Synthesis of Findings*

The integration of the TOE and TAM frameworks enabled a comprehensive understanding of the factors influencing ISO/IEC 27001 adoption in Mozambique.

The findings indicate that adoption decisions result from the interaction of technological readiness, organizational capabilities, environmental conditions, and stakeholder perceptions. No single factor alone is sufficient to explain adoption behavior; rather, implementation outcomes depend on the combined influence of multiple interrelated dimensions.

The study therefore demonstrates that promoting ISO/IEC 27001 adoption in Mozambique requires a systemic approach that simultaneously addresses technical capacity building, institutional incentives, regulatory development, and the cultivation of a national information security culture.

Such an integrated perspective is essential for creating sustainable conditions that support the long-term success of information security governance initiatives.

➢ *Discussion of Findings Through the TOE and TAM Perspectives*

The findings largely corroborate the core assumptions of the TOE framework by demonstrating that technological, organizational, and environmental factors significantly influence ISO/IEC 27001 adoption.

In particular, the shortage of qualified professionals and financial constraints emerged as critical barriers to the implementation of Information Security Management Systems within Mozambican organizations. These challenges

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

highlight the importance of investing in human capital development and institutional capacity-building initiatives.

Simultaneously, the findings support the assumptions of the Technology Acceptance Model by showing that perceived benefits positively influence adoption intentions. Organizations that recognize the strategic value of ISO/IEC 27001 are more inclined to pursue certification despite existing barriers.

However, perceptions of technical and organizational complexity continue to hinder adoption efforts, particularly among organizations with lower levels of digital maturity. This observation underscores the need for implementation frameworks, awareness programs, and support mechanisms capable of reducing perceived barriers and facilitating organizational readiness.

Overall, the findings are consistent with evidence reported in other developing countries and reinforce the need for integrated approaches that simultaneously address technological, organizational, institutional, and behavioral dimensions of information security governance.

- *Managerial Implications*

The findings provide valuable practical guidance for managers, information security officers, policymakers, and organizational leaders.

Successful implementation of ISO/IEC 27001 requires continuous investment in technical capacity development, the strengthening of organizational security culture, and active involvement from senior management. Furthermore, organizations should integrate information security governance into their strategic planning processes and treat ISO/IEC 27001 certification not merely as a compliance requirement but as a strategic instrument for value creation, risk reduction, and digital trust enhancement.

By adopting this perspective, organizations can transform information security from a reactive operational function into a core component of organizational governance and sustainable digital transformation.

V. CONCLUSION

The increasing digitalization of Mozambique's economy and society has significantly elevated the importance of information security as a strategic component for protecting digital assets, ensuring service continuity, and fostering trust in digital environments. In this context, ISO/IEC 27001 has emerged as one of the most widely recognized international standards for implementing Information Security Management Systems (ISMS), contributing to cyber risk mitigation and the strengthening of organizational governance.

The primary objective of this study was to analyze the challenges, opportunities, and implications associated with the adoption of ISO/IEC 27001 in Mozambique. To achieve this objective, an integrative literature review and documentary analysis were conducted, supported by the Technology–Organization–Environment (TOE) framework and the Technology Acceptance Model (TAM).

The findings demonstrate that the adoption of ISO/IEC 27001 is influenced by a complex combination of technological, organizational, environmental, and behavioral factors. Among the most significant barriers identified were the shortage of qualified information security professionals, high implementation and certification costs, infrastructural limitations, and relatively low levels of cybersecurity maturity within organizations.

Conversely, the study identified substantial opportunities associated with the implementation of the standard, including enhanced digital trust, improved regulatory compliance, increased organizational competitiveness, attraction of foreign investment, and stronger risk management capabilities.

The findings further indicate that ISO/IEC 27001 adoption can play a significant role in strengthening information security governance in Mozambique by promoting more structured approaches to risk management, data protection, compliance, and organizational resilience. However, successful implementation depends upon coordinated efforts among organizations, regulatory bodies, educational institutions, and public policymakers.

Overall, the study concludes that ISO/IEC 27001 represents a strategic instrument capable of supporting Mozambique's digital transformation agenda while contributing to the development of safer, more resilient, and trustworthy digital ecosystems.

- *Theoretical Contributions*

From a theoretical perspective, this study contributes to the literature on information security governance and the adoption of international standards by integrating the Technology–Organization–Environment (TOE) framework and the Technology Acceptance Model (TAM) within the specific context of Mozambique.

The findings demonstrate that the adoption of ISO/IEC 27001 cannot be explained solely through technological considerations. Instead, implementation outcomes emerge from the interaction between organizational capabilities, institutional conditions, environmental pressures, and stakeholders' perceptions regarding the usefulness and complexity of the standard.

Furthermore, the study contributes to addressing the limited body of knowledge concerning information security governance in Portuguese-speaking African countries. By providing context-specific evidence, the research establishes a foundation for future comparative studies across the Southern African Development Community (SADC) region and other developing economies.

The integrated TOE–TAM perspective also enriches the theoretical understanding of information security governance

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

by illustrating how contextual and behavioral dimensions jointly influence organizational decisions related to cybersecurity standards adoption.

➢ *Practical Contributions*

From a practical standpoint, the findings provide valuable insights for organizational leaders, information technology managers, cybersecurity professionals, auditors, and information security practitioners.

The evidence presented can support both public and private organizations in designing and implementing effective Information Security Management Systems. In particular, the study highlights the importance of prioritizing investments in:

- Information security training and professional development;
- Cybersecurity awareness and organizational culture;
- Risk management capabilities;
- Security governance structures;
- Continuous improvement processes.

The findings further emphasize the critical role of executive leadership in driving successful implementation initiatives. Organizations whose senior management actively supports information security programs are more likely to achieve successful certification outcomes and sustain long-term governance improvements.

Additionally, the study demonstrates that ISO/IEC 27001 certification should be regarded not merely as a compliance requirement but as a strategic mechanism for enhancing organizational value creation, competitiveness, and digital trust.

➢ *Public Policy Implications*

The findings underscore the importance of strengthening Mozambique's national cybersecurity ecosystem and digital governance framework.

To promote wider adoption of international information security standards, governmental institutions should consider implementing public policies focused on:

- Expanding education and training programs for information security professionals;
- Creating incentive mechanisms that encourage organizations to adopt internationally recognized security standards;
- Strengthening the institutional capabilities of INTIC and INNOQ;
- Promoting information security certification within critical sectors of the economy;
- Enhancing the implementation and enforcement of personal data protection and cybersecurity legislation;
- Integrating cybersecurity education into higher education curricula and professional training programs.

Such initiatives can contribute to increasing national cybersecurity maturity, strengthening digital resilience, and supporting sustainable digital transformation across the country.

Moreover, public-private collaboration should be encouraged to facilitate knowledge sharing, capacity building, and the dissemination of best practices related to information security governance.

➢ *Limitations of the Study*

Despite providing a comprehensive overview of ISO/IEC 27001 adoption in Mozambique, several limitations should be acknowledged.

First, the study relied primarily on documentary and literature-based evidence and did not include the collection of primary empirical data from Mozambican organizations. Consequently, the findings should be interpreted as theoretically and documentarily grounded rather than empirically validated within the national context.

Second, the limited availability of scientific studies specifically addressing ISO/IEC 27001 adoption in Mozambique restricted the depth of empirical analysis and required the incorporation of evidence from comparable African contexts.

Third, the qualitative nature of the research design does not permit the establishment of causal relationships between the identified factors and actual levels of ISO/IEC 27001 adoption.

Although these limitations do not undermine the relevance of the findings, they indicate the need for further empirical investigations capable of validating and expanding the conclusions presented in this study.

➢ *Future Research Agenda*

Considering the limitations identified, future studies should explore ISO/IEC 27001 adoption through empirical, quantitative, and mixed-method approaches.

- *Promising Avenues for Future Research Include:*

✓ Conducting case studies within public and private organizations in Mozambique;
✓ Applying survey-based research to empirically validate the integrated TOE–TAM framework;
✓ Performing comparative analyses of ISO/IEC 27001 adoption across SADC member countries;
✓ Investigating the impact of ISO/IEC 27001 certification on organizational performance and cybersecurity maturity;
✓ Developing information security governance maturity models tailored to the Mozambican context;
✓ Examining the relationship between personal data protection, digital transformation, and Information Security Management Systems adoption;

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

- ✓ Exploring the influence of leadership, organizational culture, and digital innovation on cybersecurity governance effectiveness.

Future empirical research in these areas will contribute to a more robust understanding of the determinants and outcomes of information security standards adoption in developing countries.

In conclusion, the adoption of ISO/IEC 27001 represents a strategic opportunity to strengthen information security, digital trust, and organizational governance in Mozambique. As digital transformation continues to reshape economic and social activities, the implementation of internationally recognized information security standards will become increasingly important for building a secure, resilient, and sustainable digital future.

REFERENCES

[1]. INTIC. (2025). *Segurança dos dados em Moçambique na transformação digital e computação em nuvem: Uma abordagem estratégica*. Disponível em: https://intic.gov.mz/seguranca-dos-dados-em-mocambique-na-transformacao-digital-e-computacao-em-nuvem-uma-abordagem-estrategica/

[2]. Barros, M. J. Z., & Van Niekerk, B. (2023). *Cybersecurity in Mozambique: Status and Challenges*. European Conference on Information Warfare and Security.

[3]. ISO. (s.d.). *ISO/IEC 27000 family - Information security management systems*. Disponível em: https://www.iso.org/isoiec-27001-information-security.html

[4]. Linford & Co. (2025). *What is ISO? Understanding International Security Standards*. Disponível em: https://linfordco.com/blog/what-is-the-iso/

[5]. Kitsios, F. (2023). *The ISO/IEC 27001 Information Security Management Standard to Ensure Compliance*. MDPI.

[6]. SGS. (s.d.). *Certificação ISO/IEC 27001 - Segurança da Informação*. Disponível em: https://www.sgs.com/pt-mz/servicos/certificacao-iso-iec-27001-seguranca-da-informacao-ciberseguranca-e-protecao-da-privacidade

[7]. ISO. (s.d.). *The impact of ISO/IEC 27001 certification on digital trade*. Disponível em: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100505.pdf

[8]. Tjirare, D. J. (2018). *Designing a national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia*. NUST Repository.

[9]. Ramtohul, A., & Soyjaudah, K. M. S. (2016). *Information security governance for e-services in southern African developing countries e-Government projects*. Journal of Science & Technology Policy Management.

[10]. Culot, G., & Nassimbeni, G. (s.d.). *The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda*. ResearchGate.

[11]. Ramadhan, N. (s.d.). *IEC 27001 Information Security Management Standard to SMEs*. DiVA Portal.

[12]. Moçambique. (2017). *Lei n.º 3/2017, de 9 de Janeiro (Lei das Transações Eletrónicas)*. Disponível em: https://www.dataguidance.com/sites/default/files/electronic_transactions_law.pdf

[13]. PLMJ. (2025). *Moçambique: Proposta de Lei de Proteção de Dados Pessoais*. Disponível em: https://www.plmj.com/pt/conhecimento/notas-informativas/Mocambique-Proposta-de-Lei-de-Protecao-de-Dados-Pessoais/34166/

[14]. INTIC. (s.d.). *Governo inicia processo de actualização da Estratégia Nacional de Segurança Cibernética 2026-2030*. Disponível em: https://intic.gov.mz/governo-inicia-processo-de-actualizacao-da-estrategia-nacional-de-seguranca-cibernetica-2026-2030/

[15]. Academia.edu. (s.d.). *SEGURANÇA CIBERNÉTICA: CAPACIDADE DE RESPOSTA À ATAQUES CIBERNÉTICOS A INFRA-ESTRUTURAS CRÍTICAS DE INFORMAÇÃO NO SECTOR DE TELEFONIA MÓVEL EM MOÇAMBIQUE*. Disponível em: https://www.academia.edu/116788231/SEGURAN%C3%87A_CIBERN%C3%89TICA_CAPACIDADE_DE_RESPOSTA_%C3%80_ATAQUES_CIBERN%C3%89TICOS_A_INFRA_ESTRUTURAS_CR%C3%8DTICAS_DE_INFORMA%C3%87%C3%83O_NO_SECTOR_DE_TELEFONIA_M%C3%93VEL_EM_MO%C3%87AMBIQUE

[16]. ITU. (s.d.). *Global Cybersecurity Index*. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[17]. ISACA. (2024). *Navigating the ISO/IEC 27001:2022 Transition: A 90-Day Challenge*. Disponível em: https://www.isaca.org/resources/isaca-journal/issues/2024/volume-3/navigating-the-iso-iec-27001-2022-transition-a-90-day-challenge

[18]. BSI Group. (s.d.). *Transition to the ISO/IEC 27001:2022 standard*. Disponível em: https://www.bsigroup.com/en-GB/insights-and-media/insights/blogs/transition-to-the-iso-iec-27001-2022-standard/

[19]. DePietro, R., Wiarda, E., & Fleischer, M. (1990). *The context for change: Organization, technology and environment*. In L. G. Tornatzky & M. Fleischer (Eds.), The processes of technological innovation (pp. 151-175). Lexington Books.

[20]. Emergent Mind. (2026). *TOE Framework: Tech, Org, Environment*. Disponível em: https://www.emergentmind.com/topics/technology-organization-environment-toe-framework

[21]. Davis, F. D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS Quarterly, 13(3), 319-340.

[22]. ScienceDirect. (s.d.). *Integrating Individual and Organizational Perspectives: A TAM-TOE Framework for ISO 27037 Adoption in Malaysian Government Digital Forensics Agencies*. Disponível em:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1208

https://www.sciencedirect.com/science/article/pii/S2199853125001301

[23]. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). *The PRISMA 2020 statement: an updated guideline for reporting systematic reviews*. BMJ, 372.