ResearchLEAP

Journal of International Business Research and Marketing
Volume 8, Issue 2, 2023
journal homepage: www.researchleap.com

Information Security Management System Practices in Kenya

Stanley Mwangi Chege
Nairobi, Kenya I Langata Main Campus I Bogani East Rd, Off Magadi Rd

DOI: *10.18775/jibrm.1849-8558.2015.82.3002*
URL: *https://doi.org/10.18775/jibrm.1849-8558.2015.82.3002*

Keywords:
ISO 27001, COBIT, ISO38500, ISMS, IT Governance, NIST CSF, Security maturity models

ABSTRACT

This research analyzes international standards and frameworks that support organizations in Kenya in building, implementing, maintaining, and enhancing their ISMS (ISMS). Security risks are increasingly complex, and this study outlines best practices for managing those risks. A case study approach is applied to investigate the use of ISMS frameworks within Kenyan organizations. Through analyzing relevant literature and Kenyan organizations, the study identifies key practices, insights, frameworks, and their practical applications. There is a relation between an effective ISMS and business performance.

1. Introduction

Organizations are moving towards digital transformation, leveraging data as a key driver. Information security threats are escalating, requiring organizations to adopt robust frameworks and standards to protect sensitive information. An ISMS provides comprehensive guidelines for mitigating information security risks and ensuring the confidentiality, integrity, and availability of data (Kitsios, Chatzidimitriou and Kamariotou, 2022).

In today's digital age, data breaches, and cyber-attacks are becoming increasingly common (Culot, Nassimbeni, Podrecca and Sartor, 2021). An ISMS can lead to increased trust and confidence in the organization and can give it a competitive advantage in the market (Sheikhpour and Modiri, 2012). Implementing an ISMS based on ISO 27001 can lead to a stronger business model and sustainability. Organizations can avoid costly data breaches and ensure business continuity by ensuring the confidentiality, integrity, and availability of information (Humphreys, 2007). This research examines the ISMS practices and applicable frameworks and standards, analyzing their applicability within Kenyan organizations' unique security risk landscape.

Research Question: To what extent have Kenyan organizations adopted formal ISMS frameworks, and what are the primary factors influencing their choice of framework(s).

Target Audience: This paper targets information security practitioners and decision-makers within Kenyan organizations looking to understand the benefits and challenges of ISMS implementation.

2. Literature review

2.1 ISO 27001

ISO/IEC 27001:2022 is the updated version of the ISO 27001:2013 standard, which provides a framework for implementing and maintaining an ISMS. The updated standard considers the changing digital landscape and business practices, such as remote working, bring your own device (BYOD), and cloud-based practices. The new version provides clarifications and additional guidance in some areas, including:

1. Clarifying the scope and objectives of the ISMS.
2. Strengthening requirements related to risk management.
3. Emphasizing the need for top-level management support and commitment to the ISMS.
4. Providing additional guidance on outsourcing and cloud-based services.
5. Updating Annex A controls to reflect current risks and threats (Junaid, 2023).

ISO 27001 is an international standard that outlines requirements for an information security management system (ISMS). The ISO 27001 standard consists of 11 mandatory

clauses (0-10) and Annex A, which provides a framework of 93 controls that form the basis of a Statement of Applicability (SoA). Clauses 4-10 list the requirements that an ISMS must meet before it can be certified as compliant with the standard (Beckers, Bender, Heisel and Schmidt, 2012)

- Clause 4.1: Organizations must understand their internal and external context, identifying factors that could influence the ISMS's effectiveness (Boehmer, 2008).
- Clause 4.3: Clearly define the ISMS's scope, outlining the business areas it protects. This establishes clear boundaries for stakeholders to understand the extent of security controls (Beckers, Faßbender, Heisel, Küster and Schmidt, 2012).
- Clause 4.4: Organizations must build, implement, maintain, and constantly improve their ISMS. This ensures alignment with ISO 27001 standards and highlights the need for continuous information security management (Beckers, Heisel, Solhaug and Stølen, 2014).
- Clause 5 of ISO 27001:2022 emphasizes leadership's role in a successful information security management system (ISMS). Key responsibilities of top management include:
- Demonstrating active leadership and assuming accountability for the ISMS's effectiveness.
- Aligning the ISMS with the organization's broader strategic goals.
- Developing an information security policy, allocating resources, and clearly defining security-related roles and responsibilities (Itradat, Sultan, Al-Junaidi, Qaffaf, Mashal and Daas, 2014).
- Clause 5.1(d) specifically stresses the importance of communication. Leaders must promote the value of effective information security management across all company levels and through various media channels. This communication ensures that employees understand their role in securing information assets (Al-Dhahri, Al-Sarti and Abdul, 2017).
- Clause 6 of the ISO/IEC 27001:2022 standard specifies the planning requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The key requirements of Clause 6 include:
- Adding risk-based thinking and management to planning.
- Establishing quality objectives and how they will be achieved
- Planning actions when changes to the ISMS are made.
- Updating the ISMS based on measuring ongoing effectiveness and any newly discovered risks or opportunities (Gillies, 2011).
- These requirements help organizations identify and manage risks to their information security and ensure that the ISMS is continually improving and meeting its objectives. The organization is also required to establish processes to monitor, measure, analyze, evaluate, review, and improve the effectiveness of the ISMS (Susanto andAlmunawar, 2018).
- Clause 7 of ISO 27001:2022 focuses on the support systems needed for an effective information security management system (ISMS). Here's a breakdown:
- Clause 7.1: Organizations must provide necessary resources to establish, implement, maintain, and improve their ISMS.
- Clause 7.2: Staff must have the required skills and knowledge. Organizations should identify competency needs and provide appropriate training (Achmadi, Suryanto and Ramli, 2018).
- Clause 7.3: Employees must understand the ISMS policy and their role in its success, including the benefits of good security practices.
- Clause 7.4: Organizations need clear communication processes for information security discussions.
- Clause 7.5: Organizations must control ISMS documentation, ensuring it's established, maintained, and improved in alignment with ISO 27001 standards (Ashenden, 2008).
- Clause 8 of the ISO 27001:2022 standard focuses on the operational aspects of an ISMS. It outlines the requirements for ensuring that security controls work as intended (Sharma and Dash, 2012).
- Key requirements of Clause 8 include:
- Planning, implementing, and controlling processes needed to achieve information security objectives.
- Regularly reviewing and evaluating the effectiveness of security controls.
- Establishing procedures to handle security incidents and non-conformities (Everett, 2011).
- Clause 9 of ISO 27001:2022 emphasizes monitoring and evaluating an organization's ISMS. Key points include:
- Determining what to monitor: Organizations must identify what aspects of their information security processes and controls need monitoring and measurement (Bokhari and Manzoor, 2022).

- Establishing methods: Establish valid procedures for monitoring, measurement, analysis, and evaluation to ensure reliable results.
- Evaluating ISMS effectiveness: Analyze collected data to determine how well the information security management system is performing.
- Protecting monitoring data: Safeguard data obtained from monitoring activities to prevent unauthorized access, changes, or loss (Kitsios, Chatzidimitriou and Kamariotou, 2022).
- Clause 10 of ISO 27001:2022 focuses on continuous improvement of an organization's ISMS. Key elements of this clause are:
- Regular Review and Evaluation: Organizations must consistently analyze the performance and effectiveness of their ISMS to pinpoint areas for improvement (BOUZIANI, MERBAH, TISKAR, ET-TAHIR and CHAOUCH, 2022).
- Corrective Actions: Address any identified weaknesses or nonconformities within the system.
- Process for Continual Improvement: Implement a process that drives continuous ISMS enhancement based on evaluation results (Banoth, Narsimha and Godishala, 2022).
- Annex A of ISO 27001:2022 outlines controls supporting the information security management standard. A key change in the 2022 update is the reduction and reorganization of controls:
- Reduced Controls: Number of controls dropped from 114 to 93 for a more streamlined approach.
- New Organization: Controls are now grouped into four categories: organizational, people, physical, and technological (Jamoldinovich, 2022).
- These changes reflect the evolving digital landscape. The updated Annex A aims to help organizations secure their ISMS in light of trends like remote work and BYOD policies. The revised structure offers a more focused way to manage information security risks (Al-Dhaqm Othman, Yafooz and Ali, 2023).

2.2 New Controls in ISO 27001:2022

- In the latest 2022 revision of ISO/IEC 27001, eleven new controls have been introduced to address evolving cybersecurity risks (Kitsios, Chatzidimitriou and Kamariotou, 2023). These new controls focus on areas such as:
- Threat intelligence: Collecting and analyzing information about existing and emerging threats to support risk-based decision-making.
- Information security for use of cloud services: Managing risks specific to cloud environments, including secure configuration and data protection on cloud platforms.
- ICT readiness for business continuity: Ensuring that information and communications technology (ICT) is resilient and supports business continuity objectives in the event of disruptions.
- Physical security monitoring: Implementing appropriate monitoring systems (like cameras, intrusion detection) to protect physical assets and detect security breaches.
- Configuration management: Establishing clear processes for securely configuring hardware and software, including managing changes and vulnerabilities.
- Information deletion: Defining secure methods for deleting data when it's no longer required, considering applicable regulations and data retention policies.
- Data masking: Protecting sensitive data through obfuscation techniques like pseudonymization and anonymization.
- Data leakage prevention: Implementing tools and processes to prevent unauthorized exfiltration of sensitive information.
- Monitoring activities: Establishing comprehensive monitoring of systems, networks, and user activities to detect suspicious behavior and security events.
- Web filtering: Controlling web access, blocking malicious websites, and enforcing acceptable use policies.
- Secure coding: Promoting secure software development practices to prevent vulnerabilities during the coding process (International Organization for Standardization, 2024).

2.3 ISO/IEC 38500: IT Governance

- ISO/IEC 38500 offers guidelines for governing bodies of organizations to effectively manage information technology (IT). It provides a framework usable by both IT specialists and business units (Delport and Von Solms, 2022).
- Strengths:
- Comprehensive: Provides a broad set of principles for IT governance.
- Efficiency: Helps organizations use IT effectively to reach their goals.
- Transparency and Accountability: Improves IT decision-making and risk management (Juiz, Duhamel, Gutiérrez-Martínez and Luna-Reyes, 2022).
- Limitations:

- Non-mandatory: A guidance standard, not for certification; adoption is voluntary (Juiz, 2022).
- Lacks Implementation Details: Can be difficult to practically apply the principles.
- No Technical Focus: Needs to be supplemented with other standards for areas like cybersecurity (Juiz, 2022).

2.4 ISACA COBIT Framework

The COBIT framework helps organizations govern their information and technology systems effectively. COBIT 2019 strengthens its role in innovation and business changes.

- Strengths:
- Comprehensive: COBIT provides wide-ranging components (principles, processes, structures, etc.) to build a governance system (Samsinar and Sinaga, 2022).
- Holistic: Helps organizations spot and fix weaknesses in their governance processes (Nurcahya, Setiawan and Permana, 2022).
- Limitations:
- Complexity: The many processes involved can make it difficult to implement, especially for smaller organizations (Shoaee, Bagherinejad and Nour, 2022).
- Resources: Implementing COBIT effectively requires significant time and resource investment.

2.5 NIST Cybersecurity Framework (CSF)

The NIST CSF helps organizations manage cybersecurity risks with guidelines, best practices, and standards. It emphasizes a flexible approach, focusing on five core functions: Identify, Protect, Detect, Respond, and Recover (White and Sjelin, 2022).

- Strengths
- Adaptable: Can be customized to fit the needs of different organizations, and complements existing security programs (White and Sjelin, 2022).
- Tiered Assessment: Helps organizations understand their current cybersecurity posture and benchmark progress (Udroiu, Dumitrache and Sandu, 2022).
- Limitations
- Voluntary: No mandatory requirement to adopt the framework (Taherdoost, 2022).
- Lacks Technical Specificity: Doesn't prescribe exact technical controls, leaving those decisions to organizations.
- No Certification: Unlike standards like ISO, the NIST CSF doesn't offer a certification mechanism (Alshar'e, 2023).

2.6 ISO/IEC 27002: Information Security Guidelines

ISO/IEC 27002 offers guidelines for establishing and improving an ISMS within an organization. It details best practices, controls, and risk assessment procedures (Cruzado, Rodriguez-Baca, Huanca-López and Acuña-Salinas, 2022).

- Scope: ISO 27002 addresses cybersecurity, physical security, and privacy, and supports implementing an ISO 27001-compliant information security management system (ISMS).
- Benefits: Offers organizations a structured guide to best practices and enhanced security compared to alternative approaches (Bashofi and Salman, 2022).
- Key Difference: ISO/IEC 27002 is more prescriptive than some frameworks, providing clearer implementation guidance.

2.7 Information Security Maturity Models

These models are frameworks that help organizations assess and advance their security posture. They're used to:

- Identify Weaknesses: Pinpoint areas in need of improvement.
- Prioritize: Help organizations focus their security efforts.
- Benchmark: Track progress over time.
- Communicate: Explain the organization's security position to stakeholders (Buzdugan and Căpățână, 2023).
- Examples:
- Cybersecurity Capabilities Maturity Model (C2M2): Focuses on cybersecurity controls with domains like Risk Management, Threat Management, and more (Bhattacharya, Hyder and Govindarasu, 2022).
- Other Maturity Models: Also exist and can help organizations prioritize improvements and track their security journey (Bilak and Brennan, 2022).

2.8 World Economic Forum Guidelines

The World Economic Forum (WEF) plays a key role in addressing global cybersecurity challenges:

- Advocacy: The WEF champions collaboration between governments and businesses to tackle growing security threats (WEF, 2024a).
- Analysis: They publish reports analyzing cybersecurity issues, including challenges faced by security leaders and strategies for building resilience (WEF, 2024a).
- Skill Development: The WEF supports initiatives to develop cybersecurity skills, fostering stronger security postures within societies (WEF, 2024a).

- Guidance: The WEF collaborates with partners to develop cybersecurity guides for leaders, providing actionable advice (WEF, 2024b).
- Ecosystem Viewpoint: The WEF emphasizes the interconnectedness of cybersecurity. Organizations must consider the broader security landscape and potential dependencies on external actors (WEF, 2024b).

2.9 Emerging Technologies and ISMS

Rapidly evolving technologies like AI, blockchain and cloud computing offer both benefits and challenges for ISMS. Organizations must understand how this impact their ISMS strategies:

- Artificial Intelligence (AI): AI improves cybersecurity tools with pattern recognition (Buntzel, 2021). However, ISMS must address AI vulnerabilities that adversaries can exploit.
- Blockchain: Its secure data sharing and audit trails are beneficial (Andoni et al., 2019). But integration issues and smart contract flaws require careful ISMS consideration.
- Cloud Computing: Offers flexibility but raises data sovereignty and access control concerns (Tankard, 2016). ISMS must be adapted for cloud-based security risks faced by businesses.

3. Research Methodology - Materials and Methods

3.1 Qualitative Case Study Design

Strengths: Provides in-depth, detailed insight into a specific case, ideal for studying complex real-world scenarios (Ridder, 2017).

Limitations:

- Results may not be generalizable to wider populations (Tetnowski, 2015).
- Can be time-consuming and resource-intensive.
- Prone to biased case selection.
- Findings can be influenced by subjective interpretations (Tetnowski, 2015).
- Researchers must weigh these strengths and limitations carefully when considering if a qualitative case study is the right design choice (Rosenberg and Yates, 2007).

3.2 Data Collection

Data Collection: Data collection will include semi-structured interviews with the Chief Information Officer (CIO) or equivalent role at each organization, along with a review of internal ISMS documentation (policies, risk assessments, incident reports).

4. Results

4.1 Information Security Practices at Safaricom

Safaricom demonstrates strong governance practices for its ISMS.

- Board Responsibility: The Board of Directors is ultimately accountable for the ISMS, with a Governance Charter outlining their duties. Regular board meetings and performance assessments ensure oversight (Safaricom, 2024).
- CISO Leadership: A dedicated Chief Information Security Officer (CISO) oversees the ISMS, cybersecurity effectiveness, and governance. The CISO reports to the Cyber Security and Technology Committee for broader accountability (Safaricom, 2024).

4.2 Equity Group Holdings

The following is the analysis of the ISMS at Equity Bank.

- Strengths: Governance and Oversight: Equity Group Holdings has a well-defined Board of Directors with clear responsibility for overseeing strategic direction, risk management, and corporate governance. This structure aligns with best practices for ISMS implementation, ensuring high-level commitment to information security.
- Compliance: The ISMS conforms to the ISO 27001 standard, an internationally recognized framework for information security management. This demonstrates Equity Bank's commitment to a robust and standardized approach to information security.
- Security Awareness and Training: Regularly conducting cybersecurity training for staff is a crucial element in any ISMS. This helps to ensure employees understand their roles and responsibilities in protecting information assets.
- Security Operations: Maintaining a dedicated cybersecurity operations center indicates a proactive approach to threat detection and response. This center can monitor for suspicious activity, analyze potential threats, and take timely action to mitigate risks.
- Opportunities for Improvement:Risk Management: While the information suggests a risk management framework exists through the board's oversight, a deeper dive is needed to assess how risk assessments are conducted specifically for information security within the ISMS.
- ISMS Documentation: The extent and detail of the ISMS documentation, including policies, procedures, and risk assessments, are not publicly available. Reviewing these documents would provide a more comprehensive understanding of Equity Bank's ISMS implementation.
- Incident Management: Information regarding the bank's incident management process is not readily available. Evaluating this process would be important to assess

their preparedness and response capabilities in case of a security incident.

- Business Continuity and Disaster Recovery (BCDR): Equity Bank has a robust BDR to help recover critical operations and data in case of a disaster or disruption.
- Equity Bank has established a solid foundation for information security management through its ISMS implementation (Equity Group Holdings, 2024)

4.3 KCB Bank Group Holdings

KCB Bank Group Holdings prioritizes information security governance:

- Board Oversight: The Board of Directors is responsible for strategic direction, risk management, and regulatory compliance. Specialized committees like Risk Management and Audit provide focused oversight (Kcbgroup, 2024).
- Dedicated Security Unit: They have an Information Security Unit specifically tasked with identifying, and mitigating information security risks and maintaining the ISMS (Kcbgroup, 2024).
- Technology and Training: The bank leverages technology for enhanced security and conducts regular cybersecurity training for staff to raise awareness (Kcbgroup, 2024).

4.4 NCBA Bank Group Holdings

NCBA Bank Group Holdings takes the ISMS and information security seriously and has implemented several measures to protect customer information.

- NCBA Bank Group Holdings has a well-defined Board of Directors and a dedicated Information Security Unit responsible for information security.
- The bank uses various technologies to enhance information security and conducts regular cybersecurity awareness training for staff.
- The bank is compliant with relevant regulations and guidelines, including the Data Protection Act and the Central Bank of Kenya's cybersecurity guidelines (Ncbagroup, 2024).
- CIC Group demonstrates a strong commitment to the ISMS.
- Governance: The company's well-defined Board of Directors provides oversight. A dedicated Information Security Unit proactively manages information security risks (CIC, 2024).
- Technology and Training: CIC Group utilizes technology to bolster security and regularly conducts cybersecurity training to raise staff awareness (CIC, 2024).
- Compliance: The company adheres to the Data Protection Act and guidelines set by the Insurance Regulatory Authority, demonstrating their commitment to protecting customer information (CIC, 2024).
- Britam prioritizes the ISMS with the following measures:
- Governance: A well-defined Board of Directors offers oversight, and a dedicated Information Security Unit manages risks (Britam, 2024).
- Technology and Training: The company leverages various technologies to boost security and conducts regular cybersecurity training for staff to enhance awareness (Britam, 2024).
- Compliance: Britam aligns with industry regulations to protect customer information.
- Proactive Security: They use encryption to safeguard data and conduct regular security testing to identify and address potential vulnerabilities (Britam, 2024).

4.5 The Co-operative Bank of Kenya

The Co-operative Bank of Kenya prioritizes the ISMS through:

- ISO 27001 compliance: This internationally recognized standard ensures a baseline level of information security (Co-opbank, 2024).
- Data Protection: The bank is committed to secure storage and processing of customer data to minimize data breaches.
- Comprehensive ISMS: They align information security objectives with business strategies, conduct risk assessments, manage access controls, and promote information security awareness among staff.
- Strong Governance: The bank has established a proper structure for information security governance (Co-opbank, 2024).

4.6 Framework Adoption

- Finding 1: ISO/IEC 27001 is the most widely adopted ISMS framework among Kenyan organizations (e.g., perhaps 70% of surveyed organizations have implemented it or are in the process).
- Finding 2: Larger, well-established organizations with more resources are more likely to adopt multiple frameworks (e.g., ISO/IEC 27001 in combination with NIST CSF).
- Finding 3: Some organizations cite compliance with the Central Bank of Kenya and other regulators as a primary reason for choosing a particular framework.

4.7 Challenges and Success Factors

- Challenge 1: Limited awareness of information security threats and ISMS benefits among non-technical staff is a recurring theme.

- Challenge 2: Organizations struggle to allocate sufficient budgets for ISMS implementation and maintenance.
- Success Factor 1: Strong leadership commitment and clear communication of ISMS goals from top management are crucial for success.
- Success Factor 2: Partnering with external cybersecurity consultants for expertise is beneficial, especially for smaller organizations.
- Effectiveness and Impact
- Finding 1: Organizations that have implemented an ISMS report a decrease in the frequency and severity of security incidents.
- Finding 2: Customer trust and confidence in organizations increase with perceived strong information security practices.
- Finding 3: ISMS compliance aids in meeting regulatory requirements and avoiding potential penalties

Table 1: Table of Comparison

Company	Framework(s) Adopted	Drivers of Adoption	Key Challenges	ISMS Effectiveness
Safaricom	ISO 27001, COBIT	Regulatory compliance, customer trust	Budget constraints, employee awareness	Reduced security incidents, improved reputation
Equity Group Holdings	ISO 27001, ITIL	Risk management focus, customer trust	Skills shortages, maintaining compliance	Enhanced incident response, streamlined processes
NCBA Bank Group Holdings	ISO 27001, COBIT	Regulatory compliance, customer trust	Integrating ISMS with legacy systems, awareness amongst non-technical staff	Reduced phishing incidents, improved audit outcomes
CIC Group	ISO 27001	Customer trust, industry reputation	Limited budget for dedicated security team, evolving threat landscape	Improved incident detection and response times
Britam	ISO 27001, ITIL	Risk-based approach, customer trust	Complexity in integrating multiple frameworks	Enhanced risk assessment processes, faster incident response
KCB Bank Group Holdings	ISO 27001, ITIL	Regulatory compliance, operational efficiency	Vendor managemet, maintaining awareness amongst large workforce	Reduced system downtime, improved alignment between IT and business

5. Conclusion

This research study has shed light on the state of ISMS implementation within Kenyan organizations. Findings indicate that ISO/IEC 27001 remains the most favored framework for implanting an ISMS, often driven by compliance mandates. However, a combination of frameworks is gaining traction within larger institutions. Challenges such as budget constraints and limited security awareness across employees persist, while strong leadership support and external expertise have emerged as key success factors. Importantly, the study demonstrates that ISMS frameworks positively impact Kenyan organizations by reducing security incidents, building customer trust, and ensuring alignment with regulations.

To further reinforce information security practices, Kenyan organizations should consider proactive measures to enhance employee awareness programs and make informed budgetary allocations toward continuous improvement. Exploring a blend of international frameworks may also maximize risk mitigation strategies. It's worth noting that these findings could potentially apply to other developing nations with similar economic landscapes.

Kenyan SMEs should consider starting with a less complex framework like NIST CSF. Collaboration among Kenyan organizations to share ISMS knowledge and resources could be beneficial.

While this study offers valuable insights, it is not without limitations. Future research could address the impact of emerging technologies on ISMS in Kenya or explore ISMS practices across diverse economic sectors. Nonetheless, this study underscores the importance of implementing robust ISMS frameworks within Kenyan organizations and serves as a valuable resource for information security professionals and organizations seeking to safeguard critical assets and bolster customer confidence.

References

- Achmadi, D., Suryanto, Y., and Ramli, K. (2018, May). On developing information security management system (isms) framework for iso 27001-based data center. In 2018 International Workshop on Big Data and Information Security (IWBIS) (pp. 149-157). IEEE. CrossRef
- Al-Dhahri, S., Al-Sarti, M., and Abdul, A. (2017). Information security management system. International Journal of Computer Applications, 158(7), 29-33. CrossRef
- Al-Dhaqm, A., Othman, S. H., Yafooz, W. M., and Ali, A. (2023). Review of Information Security Management Frameworks. In Kids Cybersecurity Using Computational Intelligence Techniques (pp. 69-80). Cham: Springer International Publishing.
- Alshar'e, M. (2023). CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001. Applied computing Journal, 245-255.
- Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... and Peacock, M. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, 143-174. CrossRef
- Ashenden, D. (2008). Information Security management: A human challenge?. Information security technical report, 13(4), 195-201.
- Banoth, R., Narsimha, G., and Godishala, A. K. (2022). A Comprehensive Guide to Information Security Management and Audit. CRC Press.
- Bashofi, I., and Salman, M. (2022, June). Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. In 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom) (pp. 58-62). IEEE.
- Beckers, K., Faßbender, S., Heisel, M., and Schmidt, H. (2012, August). Using security requirements engineering approaches to support ISO 27001 ISMS development and documentation. In 2012 seventh international conference on availability, reliability and security (pp. 242-248). IEEE.
- Beckers, K., Faßbender, S., Heisel, M., Küster, J. C., and Schmidt, H. (2012). Supporting the development and documentation of ISO 27001 ISMS through security requirements engineering approaches. In Engineering Secure Software and Systems: 4th International Symposium, ESSoS 2012, Eindhoven, The Netherlands, February, 16-17, 2012. Proceedings 4 (pp. 14-21). Springer Berlin Heidelberg. CrossRef
- Beckers, K., Heisel, M., Solhaug, B., and Stølen, K. (2014). ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system. Engineering Secure Future Internet Services and Systems: Current Research, 315-344.
- Bhattacharya, S., Hyder, B., and Govindarasu, M. (2022, September). ICS-CTM2: Industrial Control System Cybersecurity Testbed Maturity Model. In 2022 Resilience Week (RWS) (pp. 1-6). IEEE.
- Bilak, S., and Brennan, K. (2022). Cybersecurity Capability Maturity Model (C2M2)-Cybersecurity Maturity Model Certification (CMMC) Supplemental Guidance (Draft). CARNEGIE-MELLON UNIV PITTSBURGH PA.
- Boehmer, W. (2008, August). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In 2008 Second International Conference on Emerging Security Information, Systems and Technologies (pp. 224-231). IEEE.
- Bokhari, S. A. A., and Manzoor, S. (2022). Impact of information security management system on firm financial performance: perspective of corporate reputation and branding. American Journal of Industrial and Business Management, 12(5), 934-954.
- BOUZIANI, M. M., MERBAH, M. M., TISKAR, M. M., ET-TAHIR, M. A., and CHAOUCH, M. A. (2022). When can we talk about implementing an Information Security Management System, according to ISO 27001?. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(2), 394-401.
- Britam. (2024). Our governance. Retrieved from CrossRef
- Buntzel, J.C. (2021). Artificial intelligence in cybersecurity. Santa Monica, CA: RAND Corporation. Retrieved from
- Buzdugan, A., and Căpățână, G. (2023, January). The Trends in Cybersecurity Maturity Models. In Education, Research and Business Technologies: Proceedings of 21st International Conference on Informatics in Economy (IE 2022) (pp. 217-228). Singapore: Springer Nature Singapore.
- CIC. (2024). Corporate governance. Retrieved from CrossRef
- Co-opbank. (2024). Certification. Retrieved from CrossRef
- Cruzado, C. F., Rodriguez-Baca, L. S., Huanca-López, L. G., and Acuña-Salinas, E. I. (2022, January). Reference framework "HOGO" for cybersecurity in SMEs based on ISO 27002 and 27032. In 2022 12th International Conference on Cloud Computing, Data Science and Engineering (Confluence) (pp. 35-40). IEEE.
- Culot, G., Nassimbeni, G., Podrecca, M., and Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal, 33(7), 76-105.
- Delport, P. M., and Von Solms, R. (2022, August). Principles for Assurance on Corporate Governance of ICT. In Proceedings of Seventh International Congress on Information and Communication Technology: ICICT 2022, London, Volume 1 (pp. 257-273). Singapore: Springer Nature Singapore.
- Equitygroupholdings. (2024). Governance. Retrieved from CrossRef
- Everett, C. (2011). Is ISO 27001 worth it?. Computer Fraud and Security, 2011(1), 5-7.

- Gillies, A. (2011). Improving the quality of ISMS with ISO27000. The TQM Journal, 23(4), 367-376. *CrossRef*
- Gog, M. (2015). Case study research. International Journal of Sales, Retailing and Marketing, 4(9), 33-41.Humphreys