Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14448
e-ISSN : 2541-2019
p-ISSN : 2541-044X

ISO 27001 as Information Security Solution in Society 5.0 Era: Systematic Literature Review

Nurbojatmiko[1)*], Muhammad Sharhan Khatami[2)], Nur Muhammad Asnadi[3)], Rifka Anisyah[4)]
[1,2,3)]Universitas Islam Negeri Syarif Hidayatullah Jakarta
[1)] nurbojatmiko@uinjkt.ac.id, [2)] sharhan.khatami21@mhs.uinjkt.ac.id,
[3)] nm.asnadi21@mhs.uinjkt.ac.id, [4)] rifka.anisyah21@mhs.uinjkt.ac.id

Submitted :Jan 8, 2025 | **Accepted** : Jan 23, 2025 | **Published** : Feb 9, 2025

Abstract: Information security is crucial in the Society 5.0 era, characterized by the increasing use of big data, artificial intelligence (AI), and the Internet of Things (IoT). ISO 27001 serves as a globally recognized standard framework for managing information security, providing a systematic approach to identifying, evaluating, and controlling security threats to ensure the availability, confidentiality, and integrity of data within organizations. This research evaluates the implementation of ISO 27001 as an information security solution through a systematic literature review (SLR), analyzing relevant literature to identify benefits, challenges, and recommendations for its use in an interconnected technological landscape. The findings indicate that adopting ISO 27001 significantly enhances organizational information security by employing a PDCA (Plan-Do-Check-Act) approach that integrates security policies into business processes, strengthens risk management, and improves technology infrastructure and human resource competencies. Ultimately, implementing ISO 27001 not only bolsters information security but also supports operational efficiency and organizational sustainability amid rapid technological advancements. The novelty of this study lies in developing a framework that aligns ISO 27001 principles with the specific needs of Society 5.0, providing a valuable guide for organizations facing new information security challenges.

Keywords: Era Society 5.0, ISO 27001, Information Security, Organization, Systematic Literature Review

INTRODUCTION

Digital technology's quick progress has altered many facets of people's lives worldwide. The use of technologies like cloud computing, big data, artificial intelligence (AI), and the Internet of Things (IoT) is growing across a number of industries, including government, education, healthcare, and finance. This transformation marks the presence of the Society 5.0 era, where technology not only focuses on industrial efficiency, but also improves people's welfare through the integration between the digital world and human life.

The physical and digital worlds are becoming increasingly integrated in the Society 5.0 age. One of the main forces behind the development of creative answers to societal problems is AI technology. With more advanced analytics and data processing capabilities, AI enables process automation, accurate predictions, and more informed decision-making. In addition, AI is also applied to support more personalized interactions between humans and machines, such as through virtual assistant technology, robotics, and adaptive learning platforms (Sugiarto et al., 2023). However, behind the various benefits offered by AI and other digital technologies, these developments also bring new challenges that cannot be ignored, especially in terms of cybersecurity and ethical use of technology. The reliance on digital systems makes the integration of technology in every aspect of human life create new risks, such as the misuse of personal data and the threat of cyberattacks.

Information security is of paramount importance in the digital age, as information has great value and plays an important role in everyday life. Starting in 2024, companies need to make digital, technological and cyber risk prevention measures (involving information) a top priority to maintain their security and business continuity (Yuwono et al., 2022). Information security is not just about protecting or safeguarding information from unauthorized access. Preventing unauthorized access, use, disclosure, interruption, alteration, inspection, recording, or destruction of information is the overall goal of information security. This data may exist in digital or physical form. (Arini, 2019).

In December 2022, there were around 10.54 million Internet of Things (IoT) assaults worldwide. However, the number of IoT assaults recorded fell to over six million in the same month of 2021. With almost 13 million attacks

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14448
e-ISSN : 2541-2019
p-ISSN : 2541-044X

each month, June 2022 saw the highest amount of attacks (Statista, 2022). In 2023, a survey showed an 85% increase in cyber-attacks powered by generative artificial intelligence. This technology is being used by attackers to create more sophisticated and difficult-to-detect attacks, such as automated phishing and deepfake-based attacks, which pose a major threat to the security of organizations around the world (Z.Adam, 2023).

Existing research has extensively examined the benefits of digital transformation but has provided limited insights into addressing the unique cybersecurity challenges of Society 5.0. While various studies have explored aspects of information security, there remains a significant gap in understanding the role of ISO 27001 as a comprehensive solution for managing these challenges. This study offers novelty in the application of ISO 27001 as an information security solution in the Society 5.0 era. Specifically, it explores the relevance of ISO 27001 in an increasingly connected and data-driven environment, characterized by technological advances such as the Internet of Things (IoT), artificial intelligence (AI), and big data.

This research seeks to address the existing gap by analyzing the application of ISO 27001 in enhancing data protection, managing cyber risks, and ensuring compliance in an era where technological integration is paramount. By identifying implementation strategies, challenges, and effectiveness, this study provides a deeper understanding of ISO 27001's contribution to organizational security in Society 5.0.

LITERATURE REVIEW

Cyber Security

Cyber security is the process of defending against malicious attacks on computers, servers, mobile devices, electronic systems, networks, and data. The increasing use of computers, including desktops, laptops, smartphones, servers, and IoT (internet of things) devices, as well as computer networks such as the internet, in people's daily lives, has led to increased interest in cybersecurity. In Indonesia, Cyber Security is becoming increasingly worrisome. According to BSSN (Badan Siber dan Sandi Negara), Between January and August 2020, Indonesia experienced around 190 million attempted cyberattacks, more than four times the number of attempts in the same period in 2019, when there were only around 39 million attacks. In 2021, some have also concluded that there is little indication that cyberattacks are changing. Therefore, in the current Society 5.0 era, Indonesia urgently requires a national cyber security plan. If security is defined as freedom from threat or harm, then one of the most important factors in managing cyber security is understanding the threats that exist in cyberspace and developing effective solutions. Without proper cyber security efforts, it is likely that these threats will continue to increase, jeopardizing national digital security and the digital ecosystem as a whole.

ISO/IEC 27001

ISO/IEC 27001 is an international standard that helps organizations manage information security. This standard is important because it provides guidance for protecting data from threats such as theft, leakage, or unauthorized access. By implementing ISO 27001, companies can ensure that they meet legal regulations, increase customer confidence, and manage security risks effectively (Bakri & Irmayana, 2017). More than just data protection, ISO 27001 encourages strong collaboration between parts of the organization, including clear management responsibilities, internal audits, and corrective and preventive actions to ensure an optimal information security management system (Sama et al., 2021).

Era Society 5.0

The idea of Society 5.0 combines human values with the technology innovations of the Industrial Revolution 4.0 to establish a society that is focused on peopleIn 2019, the Japanese government unveiled Society 5.0, which uses cutting-edge technology including robotics, artificial intelligence (AI), the Internet of Things (IoT), and big data to address social issues, enhance quality of life, and lessen socioeconomic inequalities. Although this period presents obstacles for education, like unequal access to technology, limited digital literacy, and the possibility of less social connection, it also presents excellent chances to cultivate 21st century abilities like communication, cooperation, creativity, and critical thinking. With an approach that combines technology and human values, Society 5.0 aims to create a society that is inclusive, sustainable and able to face global challenges holistically (Budi et al., 2021).

METHOD

The Systematic Literature Review (SLR) method, which is a technique for locating, assessing, and interpreting all research resources, including papers pertaining to pertinent research problems and subjects, was utilized to perform this study. (Mu'izz et al., 2023).

The first step in this research is to search for journals using the Publish or Perish application, which is very useful for finding relevant journals to review. This research process can be more clearly seen in Figure 1.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14448
e-ISSN : 2541-2019
p-ISSN : 2541-044X

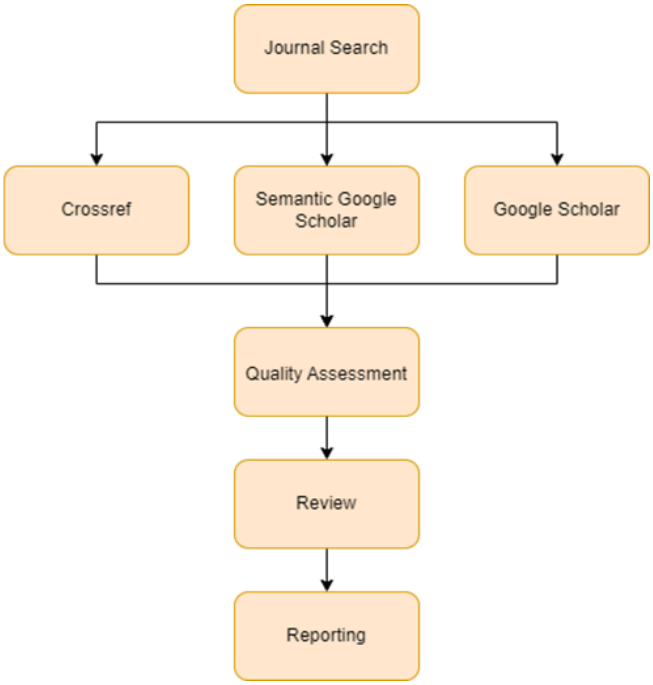

Fig. 1 Research Process

This search produced a number of journal articles that were potentially relevant to the research topic at hand. After the search process is complete, the next step is to select suitable articles, by filtering out duplicate articles, those that do not fall within a predetermined time range, and those that are not related to the topic discussed. This process is called Quality Assessment (QA).

After QA is done, the next step is to review the journal article. This stage is to find information related to the implementation of ISO 27001 in the era of society 5.0, starting from finding the problems faced, the method of solving them to the results obtained from the research process carried out.

After reviewing, the final stage is to make a conclusion or also report related to the information that has been obtained from reviewing journal articles in the previous stage.

To achieve the objectives of this study, researchers formulated research questions or can also be called research questions which will be discussed in depth at the stage of data presentation, results, and discussion.

a. RQ1: How is ISO 27001 implemented in improving information security in the Society 5.0 era?
b. RQ2: What are the main challenges in implementing ISO 27001 for information security in organizations operating in the Society 5.0 era?

RESULT

Journal Article Search Results

Based on the search results, 50 journal articles relevant to this research topic were found through the Publish or Perish application. Of these, 30 articles were selected that were published between 2019 and 2024, and all were full papers. Table 1 contains the titles of the journal articles used in this study.

Table 1Systematic Literature Review Articles

No	Source	Author	Finding	Method
1	(Ryanto & Tundjungsari, 2024)	Kamil Ryanto, Vitri Tundjungsari	Bank Victoria is still improving cybersecurity with special structures and anti-cybercrime applications, but its official policy is not yet explicit.	Descriptive analysis ISO 27001:2022
2	(Soesanto et al., 2023)	Edy Susanto, Fadila Kurniasih, Putri Mutiara, Salsabila Taqwaning Afifi	PT Jasa Marga has adequate information security but needs improvement in data access, cyber-physical security, and ISO 27001 certification.	ISO/IEC 27001 and 27002 based ISMS approach
3	(Jelita et al., 2024)	Lucia Devlina Adventia Jelita, Moh	Based on OUR Index, the system scored 19 (high), with a "Good	OUR Index 5.0 analysis, and ISO

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14448
e-ISSN : 2541-2019
p-ISSN : 2541-044X

		Noor Al Azam, Aryo Nugroho	Enough" evaluation (674) and ISO/IEC 27001 implementation at levels II-IV.	27001:2022 evaluation
4	(Budi et al., 2021)	Eko Budi, Dwi Wira, Ardian Infantono	Covid-19 fueled cyberattacks, causing breaches on Tokopedia, Bhinneka, and global threats like ransomware and malware.	Qualitative, analytical descriptive, literature study, documentation
5	(Lee & Hwang, 2021)	Woo Jin Lee dan Inho Hwang	IS voice behavior is shaped by work barriers, organizational identification, and justice, with personal security influenced by justice sensitivity.	Questionnaire survey, SEM (Structural Equation Modeling) analysis, and empirical approach
6	(Kitsios et al., 2023)	Fotis Kitsios, Elpiniki Chatzidimitriou, dan Maria Kamariotou	Companies must ensure data security; ISO 27001 boosts resilience but faces implementation challenges.	ISO 27001 implementation, risk analysis, and information security evaluation
7	(Sinaga & Taan, 2024)	Frangky, dan Rudolf Sinaga	ISO/IEC 27001:2022 enhances information security by integrating policies, procedures, and controls, improving risk management and regulatory compliance.	Qualitative-quantitative approach, interviews, surveys, and data analysis
8	(Kamal et al., 2024)	Mustafa Kamal, Muhamad Nasrullah, Yupit Sudianto, Rully Rosadi, Muhammad Arkan Fauzan, Yuvens Anggito, Wahid Yasin, Hendrik Hermawan	Evaluation results show strong scores in risk management (2.727) and access control (2.796), but compliance (2.381) and incident management (2.53) need improvement.	ISO 27001-based IT audit, survey, quantitative
9	(Fachrur Rozi et al., 2024)	Nurwan Reza Fachrur Rozi, Andri Agustav Wirabudi, Seandy Arandiant Rozano	The study developed security objectives, risk documents, and SOPs, covering policies, instructions, and records, aligned with chosen controls for risk management.	OCTAVE, risk analysis, ISO 27001-based SOPs
10	(Culot et al., 2021)	Giovanna Culot, Guido Nassimbeni, Matteo Podrecca, Marco Sartor	The study highlights five key areas: links to other standards, implementation motivation, challenges, outcomes, and contextual factors in ISO/IEC 27001 adoption.	ISO/IEC 27001 systematic literature review
11	(Mirtsch et al., 2021)	Mirtsch, Jan Kinne, Knut Blind	In Germany, ISO/IEC 27001 certification is driven by large, innovative firms, with nearly half from the ICT sector, emphasizing its role in trust and risk management.	ISO 27001 implementation, risk analysis, information security evaluation
12	(Fattah Ys et al., 2024)	Moh. Abdul Fattah Ys, Bita Parga Zen	The study reveals the National Library of Indonesia faces unaddressed risks, including fire threats and cyberattacks, lacking early detection and adequate server backups.	Literature study, interviews, observations, risk analysis based on ISO 27001
13	(Alexei, 2021)	Arina Alexei	ISO 27001 adoption in Moldova's public sector is low; establishing	ISO 27001 gap analysis,

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14448
e-ISSN : 2541-2019
p-ISSN : 2541-044X

			ISMS is vital for security resilience and trust.	information security standards review
14	(Monev, 2020)	Veselin Monev	ISMS maturity assessment with ISO 27001/27002 evaluates security controls, scores them, and suggests improvements for better effectiveness.	ISMS maturity evaluation based on ISO 27001 and ISO 27002
15	(Muhamad Bisri Mustofa et al., 2022)	Muhamad Bisri Mustofa, Evin Luthfiah Dwiandrini, Indriani Agustin, M. Afief Esyarito, Mutiara Anggraeni, Siti Wuryan	Communication media drives Smart Society 5.0 but faces challenges like blurred reality, hoaxes, and the need for a strong cybercrime mindset.	Explanatory based literature study
16	(Troisi et al., 2023)	Orlando Troisi, Anna Visvizi, Mara Grimaldi	Distributed computing and IoE drive Industry 4.0 to 5.0, with models measuring costs and enterprise architecture boosting efficiency.	SLR, content analysis, and the Society 5.0 paradigm-based approach
17	(Fathurohman & Witjaksono, 2020)	Adrian Fathurohman, R. Wahjoe Witjaksono	The study found security gaps in Bandung's Diskominfo and recommended policies, SOPs, and McAfee per ISO 27001:2013.	GAP assessment, risk analysis, ISO 27001, ISMS design
18	(Carayannis & Morawska-Jancelewicz, 2022)	Elias G. Carayannis, Joanna Morawska-Jancelewicz	Distributed computing and IoE drive Industry 5.0 with cost models and efficient architecture.	Literature study, Society 5.0 approach, Q2HM evaluation
19	(Tutik et al., 2022)	Tutik, Nurul Mutiah, Ibnur Rusi	This study identifies 23 information security assets at Sambas Diskominfo. FMEA analysis shows 1 high, 4 medium, 7 low, and 11 very low risks.	FMEA, ISO 27001, risk analysis
20	(Haikal et al., 2019)	Hikam Haikal Radya Hans Ananza, Irfan Darmawan, Rahmat Mulyana	SPBE security at West Bandung Diskominfo lacks ISO 27001:2013 compliance with low adherence and unmitigated risks.	ISO 27001, gap analysis, risk mapping
21	(Sugianto et al., 2020)	Anindya Dwi Lestari Sugianto, Febriliyan Samopa, dan Hanim Maria Astuti	The study lists major risks and management guidelines for DPTSI ITS, focusing on service, network, and device issues.	Interviews, asset analysis, threats, vulnerabilities, ISO 27001/27002.
22	(Sari & Hindarto, 2023)	Ratih Titi Komala Sari, Djarot Hindarto	EA improves food industry performance via efficiency, decisions, and adaptability, supported by management, users, and resources.	Case study, TOGAF, IT planning.
23	(Phirke & Ghorpade-Aher, 2019)	Amogh Phirke, Jay Ghorpade-Aher	The implementation of ISO 27001 enhances information security, productivity, and organizational efficiency while reducing risks and costs.	ISO/IEC 27001 for information security through ISMS
24	(Justyna & Abbas, 2021)	Żywiołek Justyna, Ali Abdul Hassan Abbas	Society 5.0 companies excel in security but face issues with procedures, conflicts, and management.	Pearson analysis, information security, Society 5.0.
25	(Fauzia Anis Sekar Ningrum et al., 2024)	Fauzia Anis Sekar Ningrum, Yudha Riwanto, et.al	University A scores 713 ("Fair") in information security, ready for ISO/IEC 27001, while University	OUR Index 5.0 questionnaire, interviews, maturity score

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14448
e-ISSN : 2541-2019
p-ISSN : 2541-044X

			B scores 321 ("Inadequate") and needs major improvements.	analysis, ISO 27001.
26	(Amirinnisa & Bisma, 2023)	Medina Amirinnisa, Rahadian Bisma	The study proposes 35 effective, 1 revised, and 22 new SOPs for Madiun Diskominfo, addressing risks from very low to high.	Qualitative-quantitative, ISO 27001/27005, FMEA, SOP
27	(Ramos Mamami et al., 2023)	Roy Guiller Ramos Mamami, Rogelio Cahuaya Ancco, Roberto René Llanqui Argollo	ISO 27001 helps companies meet legal requirements and avoid security compliance violations.	ISO 27001 Standard
28	(Kapoyos et al., 2023)	Jeremiah Marvin Kapoyos, Dimas Abimanyu Prasetyo, et.al	Cybersecurity in Society 5.0 demands awareness, collaboration, and strong policies to counter rising threats.	Qualitative descriptive method
29	(Sundari & Wella, 2021)	Piski Sundari, Wella Wella	Pusdatin is at level I+ ("Needs Improvement") and not ready for ISO 27001:2013 external audit.	PDCA (Plan-Do-Check-Act) using the WE index and ISO 27001
30	(Yahya et al., 2023)	Harun Yahya, Mahzura Aznur, Nadila Agnestesia, Ali Ikhwan	Physical data security in the Information Systems program still has vulnerabilities posing potential risks.	Qualitative with the ISO 27001 standard

RESULT

RQ1: How is ISO 27001 implemented in improving information security in the Society 5.0 era?

The implementation of ISO 27001 has proven to play a significant role in improving organizational information security in the Society 5.0 era. The main contributions are:

a. Integration of Security Policies and Procedures

The implementation of ISO 27001 integrates security policies and procedures into the organization's business processes, as was the case in Frangky & Sinaga's research (2024). This helps ensure regulatory compliance and effectively manage information security risks.

b. Improving IT Infrastructure Security

Evaluations using the ISO 27001 framework in several studies show improvements in IT infrastructure security. For example, the implementation of risk controls in government organizations and universities successfully improved the confidentiality, integrity, and availability of information systems.

c. More Systematic Risk Management

The ISO 27001 standard provides a structured PDCA (Plan-Do-Check-Act) approach in managing information security risks, so that organizations can mitigate risks on an ongoing basis.

d. Digital Transformation Support

In the era of Society 5.0, technologies such as IoT and AI dominate daily life, making data security crucial. The implementation of ISO 27001 helps organizations adapt to information security challenges in the digital era.

e. Increased Employee Awareness and Governance

Research shows that the implementation of ISO 27001 also increases employee awareness of information security, both in public and private organizations.

RQ2: What are the main challenges in implementing ISO 27001 for information security in organizations operating in the Society 5.0 era?

Some of the main challenges in implementing ISO 27001 in the Society 5.0 era found in the results of the literature review are:

a. Resistance to Organizational Culture Change

Many organizations face internal resistance to changes in work culture and adaptation of new information security policies.

b. Limited Resources and Technical Competence

Studies point to a lack of technical competence and limited resources (both financial and human) as major barriers to ISO 27001 implementation, especially in the public sector and SMEs.

c. Compliance with Complex Regulations and Frameworks

The process of implementing ISO 27001 requires compliance with various complex clauses, so organizations often struggle to achieve full compliance.

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

d. Lack of Top Management Support

Top management support is crucial in the implementation of ISO 27001. Without strong commitment, implementation is often hampered, as revealed in the case study of an expedition company.

e. Suboptimal Risk Management

Although ISO 27001 provides guidelines for risk management, the study found that there are still weaknesses in the implementation of risk assessment and mitigation, such as the lack of adequate documentation.

f. Dynamic Cyber Security Threats

In the Society 5.0 era, cyber threats such as ransomware attacks, phishing, and data leaks are on the rise. Organizations must constantly update their policies and technology to keep up with new threat developments.

DISCUSSIONS

The findings of this study underscore the pivotal role of ISO 27001 in strengthening organizational information security, particularly in the context of Society 5.0. The integration of security policies into business processes, as facilitated by ISO 27001, has been shown to enhance compliance with regulations and improve risk management. This research aligns with previous studies (e.g., Sinaga & Taan, 2024) that highlight the importance of ISO 27001 in integrating security frameworks with organizational operations. Moreover, the PDCA (Plan-Do-Check-Act) cycle employed by ISO 27001 ensures a continuous improvement process in mitigating cyber risks.

When compared to similar research, such as studies by Kitsios et al. (2023) and Kamal et al. (2024), this study further emphasizes the effectiveness of ISO 27001 in addressing security challenges brought about by emerging technologies like IoT and AI. While prior research has primarily focused on technical implementation and compliance, this study broadens the perspective by exploring the socio-organizational aspects, such as employee awareness and governance, in addition to technical infrastructure enhancements.

However, this study is not without limitations. First, the reliance on a systematic literature review limits the ability to validate findings through empirical methods, such as case studies or field surveys. Second, the variability in the scope and depth of the reviewed studies may introduce inconsistencies in drawing conclusions. Lastly, the rapidly evolving nature of cyber threats in Society 5.0 presents a challenge to the generalizability of the findings, as new vulnerabilities may emerge that were not addressed in the analyzed studies. Future research should consider empirical validation, sector-specific analysis, and adaptive frameworks to address these limitations effectively.

The results of this study indicate that the implementation of ISO 27001 in the Society 5.0 era is not only relevant but also crucial to face new information security challenges. The novelty of this study lies in the development of a framework that integrates the principles of ISO 27001 with the specific needs of Society 5.0, which can be a guide for organizations.

CONCLUSION

The implementation of ISO 27001 in the Society 5.0 era has proven to be very helpful in improving organizational information security. The standard enables the integration of security policies into business processes, strengthens IT infrastructure, better manages risks, and supports the use of digital technologies such as IoT and AI. In addition, ISO 27001 also increases employee awareness about the importance of maintaining information security.

In implementation, however, there are several challenges faced, such as lack of resources, resistance to change, complex regulations, and evolving cyber threats. To overcome these challenges, organizations need to involve management, increase training, update policies regularly, and collaborate with other parties. With a good strategy, ISO 27001 can help organizations face security challenges in the modern technological era.

The results of this study indicate that the implementation of ISO 27001 in the Society 5.0 era is not only relevant but also crucial to face new information security challenges. The novelty of this study lies in the development of a framework that integrates the principles of ISO 27001 with the specific needs of Society 5.0, which can be a guide for organizations.

REFERENCES

Alexei, A. (2021). Ensuring Information Security in Public Organizations in the Republic of Moldova Through the Iso 27001 Standard. *Journal of Social Sciences*, *IV(1)*(March). https://doi.org/10.52326/jss.utm.2021.4(1).11

Amirinnisa, M., & Bisma, R. (2023). Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun. *Jeisbi*, *04*(04), 47–58.

Arini, A. (2019). Pendeteksian Dini Tingkat Kemanan Informasi Berbasis Iso 27001 : 2013 Menggunakan Metode Ahp (Analytical Hierarchy Process). *Cyber Security Dan Forensik Digital*, *2*(2), 57–64. https://doi.org/10.14421/csecurity.2019.2.2.1480

Bakri, M., & Irmayana, N. (2017). Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar Iso 27001. *Jurnal Tekno Kompak*, *11*(2), 41. https://doi.org/10.33365/jtk.v11i2.162

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(December 2021), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Carayannis, E. G., & Morawska-Jancelewicz, J. (2022). The Futures of Europe: Society 5.0 and Industry 5.0 as Driving Forces of Future Universities. *Journal of the Knowledge Economy*, *13*(4), 3445–3471. https://doi.org/10.1007/s13132-021-00854-2

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Fachrur Rozi, N. R., Agustav Wirabudi, A., & Arandiant Rozano, S. (2024). Chance Evaluation and Improvement of Get to Control Data Security Administration Based On ISO/IEC 27001 at Telkom University Jakarta Campus. *International Journal of Science Education and Cultural Studies*, *3*(2), 1–26. https://doi.org/10.58291/ijsecs.v3i2.246

Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, *1*(1), 1–11. https://doi.org/10.25008/bcsee.v1i1.2

Fattah Ys, M. A., Parga Zen, B., & Wasitarini, D. E. (2024). Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi. *Cyber Security Dan Forensik Digital*, *6*(2), 76–82. https://doi.org/10.14421/csecurity.2023.6.2.4190

Fauzia Anis Sekar Ningrum, Yudha Riwanto, Inggrid Yanuar Risca Pratiwi, & Muhammad Ainul Fikri. (2024). Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI. *Jurnal Informatika Polinema*, *10*(3), 437–444. https://doi.org/10.33795/jip.v10i3.5154

Haikal, H., Ananza, R. H., Darmawan, I., & Mulyana, R. (2019). Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (Spbe) Menggunakan Standar Iso 27001:2013 (Studi Kasus: Diskominfotik Kabupaten Bandung Barat) Design of Information Security Governance for E-Government Using Iso 27001:20. *Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (Spbe) Menggunakan Standar Iso 27001:2013 (Studi Kasus: Diskominfotik Kabupaten Bandung Barat)*, *6*(No.2), 8368–8374.

Jelita, L. D. A., Al Azam, M. N., & Nugroho, A. (2024). Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022. *Jurnal SAINTEKOM*, *14*(1), 84–94. https://doi.org/10.33020/saintekom.v14i1.623

Justyna, Ż., & Abbas, A. A. (2021). Information Security in Information Systems Among Employees of Industrial Enterprises As Societies 5.0. *System Safety: Human - Technical Facility - Environment*, *3*(1), 64–70. https://doi.org/10.2478/czoto-2021-0007

Kamal, M., Muhamad, M., Sudianto, Y., Fauzan, M. A., Anggito, Y., Yasin, W., & Hermawan, H. (2024). Information Technology Security Audit at the YDSF National Zakat Institution Using the ISO 27001 Framework. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *13*(1), 98–103. https://doi.org/10.32736/sisfokom.v13i1.1987

Kapoyos, J. M., Prasetyo, D. A., Gusnaldi, M. R., & Sinlae, F. (2023). Pentingnya Cybersecurity di Era Society 5.0. *Pentingnya Cybersecuritydi Era Society 5.0*, *vol 1*(5), 1344–1351. https://jurnal.intekom.id/index.php/njms/article/view/229/199

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability (Switzerland)*, *15*(7). https://doi.org/10.3390/su15075828

Lee, W. J., & Hwang, I. (2021). Sustainable information security behavior management: An empirical approach for the causes of employees' voice behavior. *Sustainability (Switzerland)*, *13*(11), 1–23. https://doi.org/10.3390/su13116077

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engineering Management*, *68*(1), 87–100. https://doi.org/10.1109/TEM.2020.2977815

Monev, V. (2020). Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. *2020 34th International Conference on Information Technologies, InfoTech 2020 - Proceedings*, *September*, 17–18. https://doi.org/10.1109/InfoTech49733.2020.9211066

Mu'izz, D. F. A., Kurniawan, P. M., Durunnafis, A., Yaqin, M. A., & Fauzan, A. C. (2023). Survei Pengukuran Usability Software Menggunakan Metode Systematic Literature Review. *ILKOMNIKA: Journal of Computer Science and Applied Informatics*, *5*(3), 223–243. https://doi.org/10.28926/ilkomnika.v5i3.444

Muhamad Bisri Mustofa, Evin Luthfiah Dwiandrini, Indriani Agustin, M. Afief Esyarito, Mutiara Anggraeni, & Siti Wuryan. (2022). MEDIA MASSA DAN CYBER CRIME DI ERA SOCIETY 5.0 (Tinjauan Multidisipliner). *Jurnal Prodi Komunikasi Dan Penyiaran Islam*, *13*(1), 77–98.

*name of corresponding author

Phirke, A., & Ghorpade-Aher, J. (2019). Best practices of auditing in an organization using ISO 27001 standard. *International Journal of Recent Technology and Engineering*, *8*(2 Special Issue 3), 691–695. https://doi.org/10.35940/ijrte.B1128.0782S319

Ramos Mamami, R. G., Cahuaya Ancco, R., & Llanqui Argollo, R. R. (2023). IT policy and information security management based on ISO 27001. *Innovación y Software*, *4*(1), 96–106. https://doi.org/10.48168/innosoft.s11.a57

Ryanto, K., & Tundjungsari, V. (2024). Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 Framework. *Journal La Multiapp*, *5*(4), 344–354. https://doi.org/10.37899/journallamultiapp.v5i4.1399

Sama, H., Licen, L., Saragi, J. S. D., Erline, M., Kelvin, K., Hartanto, Y., Winata, J., & Devalia, M. (2021). Studi Komparasi Framework Nist Dan Iso 27001 Sebagai Standar Audit Dengan Metode Deskriptif Studi Pustaka. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *6*(2), 116–121. https://doi.org/10.36341/rabit.v6i2.1752

Sari, R. T. K., & Hindarto, D. (2023). Implementation of Cyber-Security Enterprise Architecture Food Industry in Society 5.0 Era. *SinkrOn*, *8*(2), 1074–1084. https://doi.org/10.33395/sinkron.v8i2.12377

Sinaga, R., & Taan, F. (2024). Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala. *Nuansa Informatika*, *18*(2), 46–54. https://doi.org/10.25134/ilkom.v18i2.205

Soesanto, E., Kurniasih, F., Mutiara, P., & Afifi, S. T. (2023). Analisis Sistem manajemen keamanan informasi dengan standar ISO/IEC 27001 dan ISO/ICE 27002 pada PT Jasa Marga. *Co-Creation : Jurnal Ilmiah Ekonomi Manajemen Akuntansi Dan Bisnis*, *1*(4), 155–164. https://doi.org/10.55904/cocreation.v1i4.700

Statista. (2022). *Worldwide Internet of Things (IoT) Attacks*. https://www.statista.com/statistics/1322216/worldwide-internet-of-things-attacks/ (accessed Sep. 28, 2024).

Sugianto, A. D. L., Samopa, F., & Astuti, H. M. (2020). Penilaian Dan Kontrol Risiko Terhadap Infrastruktur Dan Keamanan Informasi Berdasarkan Standar Iso/Iec 27001:2013 (Studi Kasus: Institut Teknologi Sepuluh Nopember). *Sebatik*, *24*(1), 96–101. https://doi.org/10.46984/sebatik.v24i1.910

Sugiarto, I., Hasnah, S., Annas, A. N., Sundari, S., & Dhaniswara, E. (2023). Inovasi Pembelajaran Berbasis Teknologi Artificial Intelligences (AI) Pada Sekolah Kedinasan Di Era Revolusi Industri 4.0 Dan Society 5.O. *Journal Of Social Science Research*, *3*(5), 10546–10555.

Sundari, P., & Wella, W. (2021). SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR). *Ultima InfoSys : Jurnal Ilmu Sistem Informasi*, *12*(1), 35–42. https://doi.org/10.31937/si.v12i1.1701

Troisi, O., Visvizi, A., & Grimaldi, M. (2023). Rethinking innovation through industry and society 5.0 paradigms: a multileveled approach for management and policy-making. *European Journal of Innovation Management*, *27*(9), 22–51. https://doi.org/10.1108/EJIM-08-2023-0659

Tutik, T., Mutiah, N., & Rusi, I. (2022). ANALISIS DAN MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE FAILURE MODE AND EFFECTS ANALYSIS (FMEA) DAN KONTROL ISO/IEC 27001:2013 (Studi Kasus : Dinas Komunikasi dan Informatika Kabupaten Sambas). *Coding Jurnal Komputer Dan Aplikasi*, *10*(02), 249. https://doi.org/10.26418/coding.v10i02.55082

Yahya, H., Aznur, M., Agnestesia, N., & Ikhwan, A. (2023). Analisis Keamanan Fisik Data Prodi Sistem Informasi UIN Sumatera Utara Medan Menggunakan Standar ISO 27001. *Jurnal Penelitian Dan Pengkajian Ilmiah Eksakta*, *2*(1), 39–44. https://doi.org/10.47233/jppie.v2i1.675

Yuwono, S. T., Pratama, N., & Afifah, V. (2022). Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001: 2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK. *Jurnal IKRAITH-Informatika*, *6*(2), 21–28. https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/download/1570/1285

Z.Adam. (2023). *85% of Cybersecurity Leaders Say Recent Attacks Powered by AI: Weekly Stat*. CFO. https://www.cfo.com/news/cybersecurity-attacks-generative-ai-security-ransom/692176/ (accessed Sep. 28, 2024).

*name of corresponding author