JDBIM
(Journal of Digital Business and Innovation Management)

Volume 3, Issue 1, Juni 2024, 1-20
ISSN (Online): **2962-3898**
DOI: 10.26740/jdbim.v3i1.59169
https://ejournal.unesa.ac.id/index.php/jdbim

Maturity Level Risk Assessment in Media Companies with ISO 27001 Framework

Anne Ivena Wijaya [1*], Dwi Indah Lestiani [2], Yeni Rosa Damayanti [3], Adinda Ayu Putri Sugiono [4], Sherissa Callista Huanggino [5]

[12345] Department of Digital Business, Universitas Negeri Surabaya
Ketintang, Surabaya 60231, Indonesia

Abstract

This study aims to assess the maturity level of information security in media companies using the ISO 27001 framework. With the rapid growth of the media industry and increasing cyber security risks, media companies must ensure that their information security systems meet applicable international standards so that existing data can be properly protected. This article uses the PRISMA method, which analyzes sources from articles or papers on Publish or Perish. The research focuses on article sources that discuss the application of the ISO 27001 framework in companies and the Maturity Level of media companies. The results show that applying the ISO 27001 framework in conducting Maturity Level Assessments in media companies is very important to improve information security and reduce the risk of data leakage. This research also provides an important understanding of the application of the ISO 27001 framework in the media industry and offers guidance for media companies to improve their security maturity level.

***Keywords**: ISO 27001; Information Security; Media Company*

Received: 1 April 2024; Accepted: 29 Juni 2024; Published: 30 Juni 2024

*Corresponding author
Email: anne.22076@mhs.unesa.ac.id

To cite this document:
Wijaya, Anne Ivena., Lestiani, Dwi Indah., Damayanti, Yeni Rosa., Sugiono, Adinda Ayu Putri., Huanggino, Sherissa Callista. (2024). Maturity Level Risk Assessment in Media Companies with the ISO 27001 Framework. *Journal of Digital Business and Innovation Management*, Vol. 3 No.1, pp. 1-18.

INTRODUCTION

Data Security Management is managing and protecting data from unauthorized access, modification, or loss. This includes implementing security controls such as data encryption, access monitoring, user activity tracking, and data recovery measures in emergency situations. The main purpose of Data Security Management is to ensure that data remains confidential, secure, and accessible only to authorized individuals. By implementing best practices in data security management, organizations can reduce data security risks and ensure the effectiveness of their daily operations (Albugmi et al., 2016).

Data Security Management is related to data breaches in the field of information security. Data Breach is when confidential data is found, transmitted, watched, achieved, or used by individuals who are not obliged to do so. Data breach can occur due to attacks by individuals with income or fraud purposes, criminal groups, political activities, or the state. Data that can be the purpose of a data breach includes financial data such as credit or debit account numbers, bank data, health data, personal identity data (PII), trade information, or intellectual information. Data breaches can cause direct costs (costs of recovery, testing) and indirect costs (business losses, security management for exposed victims data). Management of incidents related to information security breaches. A personal data breach can be called a data privacy incident. Many cases of data breaches are caused by the negligence of the information owner. Most information security and data privacy measures and standards require handling information security incidents or data privacy violations (Gabriel et al., 2018).

The International Organization for Standardization (ISO) is responsible for developing international standards in various fields, such as technology, industry, and management. ISO has various standards that can be used in various fields, such as quality, energy, food safety, and information security management standards. ISO standards have important functions for the company, such as improving company standards, increasing company credibility, increasing consumer trust, and minimizing errors in the production process (Calder, 2017).

ISO 27001 is an international standard governing information security management systems (ISMS). This standard provides models and guidelines for organizing, establishing, and managing information security systems in organizations. This can help organizations to identify, evaluate and manage possible information security risks. ISO 27001 also sets out the requirements for a risk-based management approach to information

security, including policies, and remedy actions in the event of a security incident. Implementing ISO 27001 helps organizations improve information security, protect sensitive data, strengthen customer trust, and comply with applicable security regulations. Many organizations worldwide, both in the public and private sectors, use ISO 27001 as a framework to effectively manage their information security (Hsu et al., 2016).

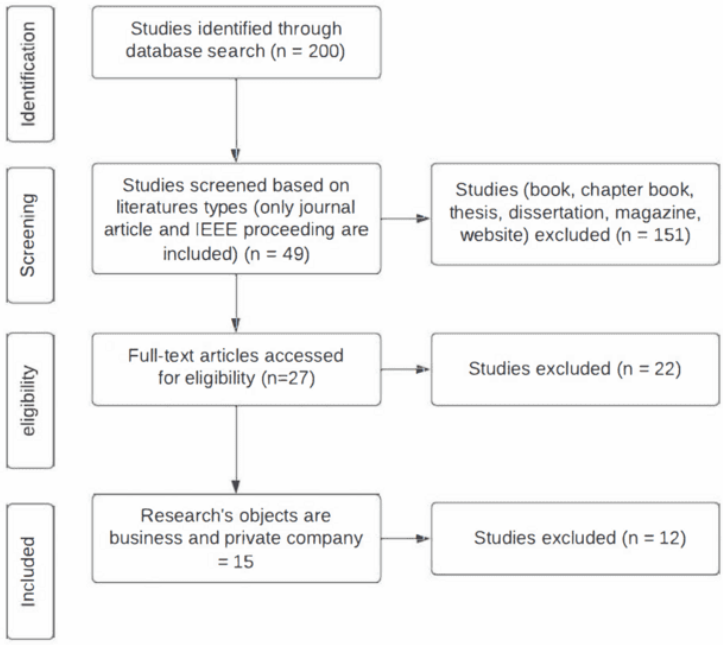
ISO/IEC 27001:2013 is an information security management system standard. Structurally, ISO 27001:2013 is divided into 2 large parts, namely: a. clause, is a requirement that must be met if the organization implements information security using the ISO 27001:2013 standard; and appendix A, is a reference document that is used as a guideline in determining security controls that must be applied to ISMS. In ISO 27001:2005, Annex A consists of 11 domain groups, 39 control objectives, and 133 controls, while in the ISO 27001:2013 amendment, Annex A consists of 14 domain groups, 35 control objectives, and 114 controls. With ISO/IEC 27001, companies can obtain their ISMS certification by third-party organizations and thus show customers evidence of their security measures (Fathurrohman & Witjaksono, 2020).

Previous research discusses maturity assessment for information security management in MSMEs (Cholez & Girard, 2014); Riadi & Prayudi (2016) discuss the framework for measuring maturity level assessment. Cholez and Girard's work is a valuable resource for SMEs looking to strengthen their information security posture through structured assessment, process improvement, and strategic management practices. It addresses SMEs' unique challenges and offers insights into achieving effective information security management despite resource limitations. Riadi and Prayudi's work likely contributes to the field of information security management by offering a structured approach to assessing and improving information security performance through a maturity-level framework. It provides organizations with a systematic method to evaluate their security practices, identify gaps, and establish a roadmap for continuous improvement in information security management. Schmitz et al., 2021 provide valuable insights into how practitioners assess and improve the maturity levels of information security controls, offering practical guidance for organizations striving to strengthen their security posture in an increasingly digital and interconnected environment. There is not much research with a systematic literature review approach that discusses the scientific development of maturity assessment level in information security management using the ISO 27001 framework. This is the novelty in this research. This research is expected to help organizations

to better understand the maturity level of their information security controls based on the ISO 27001 standard. By evaluating this maturity, organisations can identify weaknesses and strengths in their IT risk management. Maturity level assessment not only provides an overview of the current state of affairs, but also provides a basis for continuous improvement. Organisations can use assessment results to design clear action plans to improve the maturity of their information security controls over time, in line with changes in security threats and business needs.

METHOD

PRISMA is a guide to assess a systematic review and/or meta-analysis. PRISMA helps writers and researchers in compiling a quality systematic review and meta-analysis with the steps shown with the following chart:



Picture 1. Research PRISMA Chart

RESULT AND DISCUSSION

Data Analysis with Publish or Perish

The Publish or Perish application is software that can help researchers analyze and evaluate published scientific publications. The following are the search results using Publish or Perish with the keyword "data security management; data breach; ISO 27001" in the last 10 years from 2013 to 2023 and there are 200 journals that already have citation records and patents.

Analysis with *VOS viewer*

Network Visualization

Network Visualization is a network visualization of data analysis. The analysis we do is using normalization analysis with the association strength method. From our analysis, there are 3 colors: red, green, and blue. Each color represents each cluster, such as red (cluster 1), green (cluster 2), and blue (cluster 3). From the analysis, some items enter 2 clusters simultaneously, namely Information Security Management. The analysis results from 200 journals on VOS viewer contained 11 items, 3 clusters, 53 links, and a total links strength of 902 (Table 1).

Table 1. Article Keyword Clustering

Cluster	Item
Cluster 1 (7 Items)	1. Information Security Management 2. ISO 3. ISO IEC 4. Organization 5. Security Management 6. Standard 7. Study
Cluster 2 (3 Items)	1. Implementation 2. Information Security Management 3. ISMS
Cluster 3 (1 Items)	1. Data

The following is the result of the VOS viewers article from network visualization where many studies discuss Information Security Management, ISO, ISO IEC, Organization, Security Management, Standard, Study. From the analysis we did, there is still a little research that discusses Implementation, ISMS and Data.

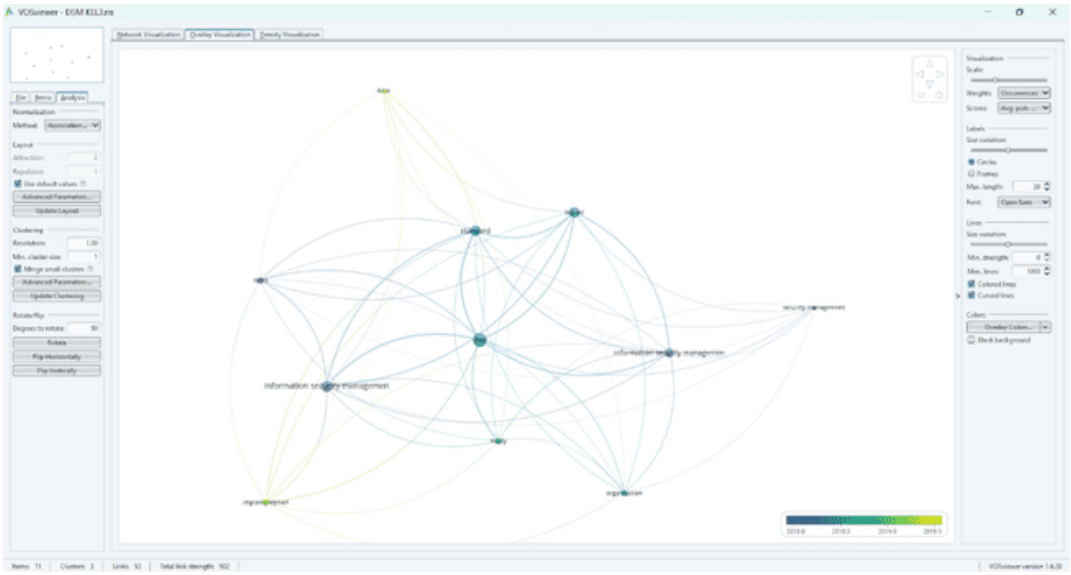


Figure 1. Network Visualization

Overlay Visualization

Overlay Visualization is a visualization of the time span of research that has been done. From the results of the analysis that we did, if the color of the item is getting to the left or the color is getting darker (close to purple) then the publication of the research has been carried out for a long time, and if the color of the item is getting to the right or the color is getting brighter, then the publication of the research is still new. In Figure 2, research on data and implementation was published in 2019 and above, then research on studies published in 2019, while research on information security management, ISO, Security Management, Standard, ISMS, ISO IEC, and Organization was published in 2018 and below.

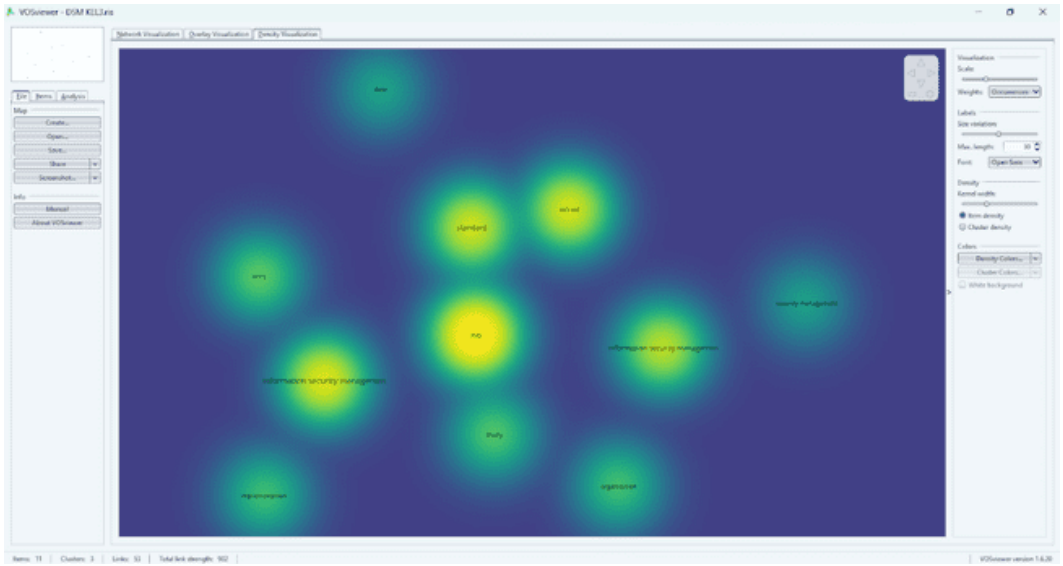


Figure 2. Overlay Visualization

Density Visualization

Density Visualization is a visualization of the density related to the number of occurrences. Density can be affected by items. The brighter the color (yellow color), the denser the data or the more often the term appears in a document. From the results of our analysis, it can be seen in the image below that the terms ISO, Information Security Management, Standard, and ISO IEC have density, or those terms often appear in a document.

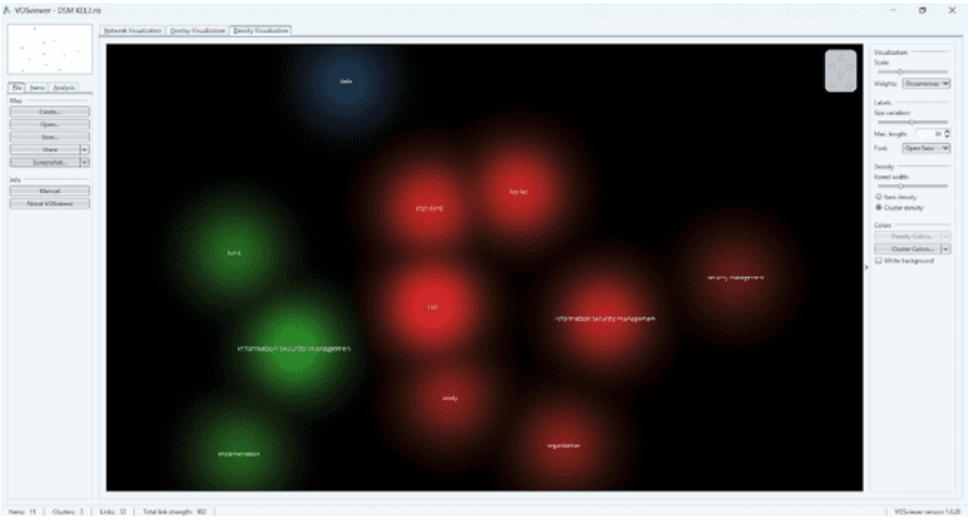


Figure 3. Density Visualization

Based on Figure 3, the cluster can affect density. The results of our analysis show in the image below that each item has been grouped by cluster. Cluster 1 consists of Information Security Management, ISO, ISO IEC, Organization, Security Management, Standards, and Study. Cluster 2 consists of Implementation, Information Security Management, and ISMS, while Cluster 3 consists of data.

Data Analysis with Excel

From the search results using Publish or Perish with the keyword "data security management; data breach; ISO 27001," in the last 10 years, from 2013 to 2023, 200 journals already have citation records and patents. Then, from the 200-journal data, we identified by filtering the type by only selecting a journal with the PDF type. After identification, 49 journal data were obtained using the PDF type.

The second stage is screening. After obtaining 49 journal data that use the pdf type, we filter the publisher by only choosing a credible publisher so that 49 journal data are published by a credible institution after the screening process.

The third stage is eligibility. After obtaining 49 journal data published by a credible institution, we filtered the appropriate journal-title and related keywords so that 15 journal data were obtained that are consistent with the topic we will analyze. The following are 15 journal data included in the topics that we will analyze, namely topics that are still related to the keyword "data security management; data breach; ISO 27001" in the last 10 years, namely from 2013 to 2023.

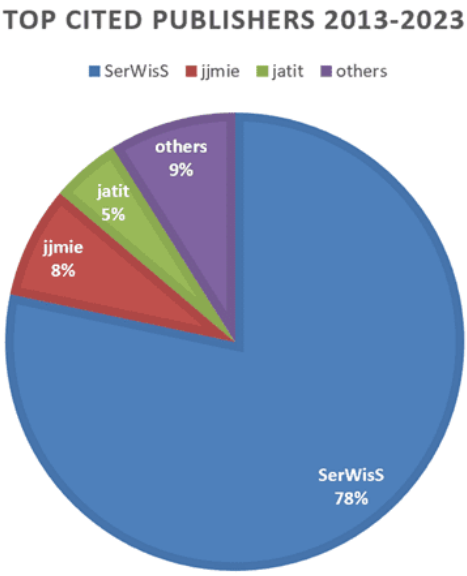


Chart 2. Top Cited Publishers on Maturity Level Assessment Information Security Management System

From the 15-journal data included, we analyzed the names of publishers and cities. The results of the analysis that we did were 14 publisher names, namely serwiss.bib.hs-hannover.de, as many as 387 cites or 78%, jjmie.hu.edu.jo as many as 39 cites or 8%, jatit.org as 24 cites or 5%, research.mitwpu.edu.in as many as 8 cites or 2%, aasmr.org as 8 or 2%, irjaes.com as much as 1 cites, losearijournals.com as 1 cites, opus.lib.uts.edu.au as 4 cites or 1%, humapub.com as much as 1 cites, iiisci.org as 6 cites or 2%, core.ac.uk as 1 cites, ceur-ws.org as 3 cites, and ijmcs.future (Chart 2).

Implementation of Information Security Management System

Today, technological advances have changed how attacks on international systems occur. In information warfare, power is measured by the information collected about the threats. As information technology evolves, it is very important to identify the potential hazards of any technological advances. This is necessary to prevent the company from experiencing

losses. Therefore, constant security system updates become very important to avoid hacker fraud since any technology can be attacked.

According to Lami (2013), developing the ISMS framework requires several actions. The main points are defining security policy, obtaining administrative support, defining ISMS scope, risk assessment, risk management, selecting appropriate/applicable controls and preparing implementation statements (SOA), preparing all policies or procedures, internal audits, and continuously updating/improving. This Standard consists of a standard requirements section (mandatory clauses 4 to 8, no exceptions, applicable to all types of organizations) and an Appendix section. The ISO 27001 ISMS appendix consists of 11 security domains (A.5 to A.15) to provide a security layer (Table 2).

Table 2. ISO 27001 ISMS Annex Domains (2005 Edition)

A5 – Security Policy
A6 – Organizing Information Security
A7 – Asset Management
A8 – Human Resources Security
A9 – Physical & Environmental Security
A10 – Communications & Operations Management
A11 – Access Control
A12 – Information Systems Acquisition, Development and Maintenance
A13 – Information Security Incident Management
A14 – Business Continuity Management (BCM)
A15 - Compliance

Source: Lami (2013)

According to Saadat & Abbasi (2021), organizational policy is a regulation that establishes permissible and not allowed behavior. Information security policies are created by senior executives and show how important it is to keep information across the company. It also describes the tasks and responsibilities related to security and what data types should be maintained. Procedures, standards, and policies help enforce those policies. Standards provide specific instructions on how to comply with policies and ensure consistency in organizational security, while guidelines support standards by establishing recommended controls. The process explains how policies, standards, and recommendations are implemented.

There are two main approaches to implementing information security policies: top-down and bottom-up. Engineers, organizational managers, and system administrators usually start a bottom-up approach. However, this method often does not work because it does not include top management planning, such as cooperation between divisions and proper allocation of funds. On the other hand, the top-down approach involves

coordinated top management planning and representatives who provide financing and propose implementation mechanisms. The top management's responsibility is to determine the necessary resources, policies, operations, and methods.

Adopting an information security program helps companies protect and avoid data misuse. Organizational data security is strongly influenced by various elements, such as education and information, supervisor support, finance, implementing information security management, and conformity with company goals. Education and awareness about information security is very important. Increasing employee awareness and providing education can help maintain organizational information security. The security awareness program refers to the knowledge and instruction provided to each organization member. Security awareness programs help members of the organization carry out their duties safely.

In addition, strong and consistent management supervision is also an important part of ensuring sustainable information security. With proper support and supervision, implementing information security policies can run smoothly and effectively by ensuring all stakeholders understand and comply with regulations.

Information Technology Management in organizations with ISO 27001

ISO/IEC 27001:2005 ISMS is one of the strictest standards for information security, ensuring the safest environment for technology-based organizations. It uses the tools and procedures necessary to ensure information systems' confidentiality, integrity, and availability to address almost all aspects that affect the organization's security experience (Itradat et al., 2014). The application of the Information Security Management System (ISMS) based on the ISO/IEC 27001:2005 standard is considered very important to eliminate the risks faced by information systems.

ISO/IEC 27001:2013 is an international standard for entities that manage information security (Zaydi & Nassereddine, 2021). This explains how a company should use the Hybrid Conceptual Approach to Information Security Governance to meet information security requirements, such as confidentiality, integrity, and availability of its information assets, and include them in ISMS. This standard outlines the necessary measures for establishing, implementing, operating, and managing information security systems. This standard generally applies to all types of organizations. Introducing a cyclical pattern called the 'Plan-Do-Check-Act' Model or PDCA, this standard aims to create, implement,

oversee, and improve the organization's Information Security Management System (ISMS).

ISO 27001 certification is valid for 3 years and requires continuous compliance with standard requirements. ISO 27001 can assist companies in obtaining Information Security Management System (ISMS) certification by third-party organizations, show evidence of security measures that have been implemented, and reduce the risks and losses that companies may face related to information security. Organizations can implement appropriate risk management measures to ensure that their Information Security Management System (ISMS) operates, is monitored, and improved in accordance with the ISO/IEC 27001:2005 standard. This enables organizations to ensure that their information security systems operate, are monitored, and maintained in accordance with standard requirements so as to ensure that they remain secure.

ISO/IEC 27001:2013 is an international standard for entities that manage information security (Zaydi & Nassereddine, 2021). This explains how a company should use the Hybrid Conceptual Approach to Information Security Governance to meet information security requirements, such as confidentiality, integrity, and availability of its information assets, and include them in ISMS. This standard sets out the necessary measures for the establishment, implementation, operation, and management of information security systems. This standard generally applies to all types of organizations. Introducing a cyclical pattern called the 'Plan-Do-Check-Act' Model or PDCA, this standard aims to create, implement, oversee, and improve the organization's Information Security Management System (ISMS).

According to Zaydi & Nassereddine (2021), the Introduction (object, reference, and glossary) begins in the first clause, and clauses 6–10 are important in this standard. To build a successful ISMS, these five clauses must be applied. Clause 4-Organizational Context: understand the organizational context, the needs and expectations of interested parties, and define the scope of the SMM. This clause clearly states that the organization must establish, implement, maintain and continue to improve ISMS based on PDCA quality methods. Clause 5-Leadership: indicates that management must show commitment and provide all. Clause 6-Planning: Building the ISMS Phase shows that routine internal audits are essential to ensure the implementation of ISMS is effective and meets the goals that have been set. ISMS processes and procedures must comply with ISO 27001 standards and applicable laws or regulations. Clause 7-Supption: stipulates that ISMS must be adequate, appropriate, and effective through

review, which must be done at least once a year. During this review, the results of the ISMS internal audit were evaluated, and strategies for fixing and preventing problems were established. In Clause 8 on the operation, implementation, and exploitation of ISMS, organizations can ensure that the actions are always successful. Audits, event analysis, reviews, and corrective and preventive actions are used to achieve this. Clause 9-Performance Evaluation: Monitoring and reviewing the ISMS Phase: Evaluate and assess process performance following ISMS policies, objectives, and practical elements, and report the results to management for evaluation. Clause 10-Improvement: Maintenance and Improvement of the ISMS Phase: Take corrective and preventive action based on the results of internal ISMS audits and management reviews or other relevant information to improve ISMS.

Application of Standards and Risk Assessment in the ISO 27001 Framework

The ISO 27001 standard only provides general risk analysis and risk management plans that can be applied to all types of businesses. They do not specify, mention, or recommend any control method for any particular risk scenario. Although standardization and regulation play an important role in attracting budgets and the attention of C-level executives in information security, there are growing challenges to balancing actual information security risks with compliance requirements. As a result, the perception of vulnerability and a sense of security is increasing. Organizations can meet compliance requirements without feeling threatened in today's fast-moving threat world.

In the field of risk management, many experts and associations agree that failure can be caused by information ambiguity derived from different risk assessments from different points of view (McCuaig, 2008, p. 3; Ernst, 2009, p. 4). The maturity level of the information technology security system is determined using the checklist from Annex A ISO 27001, which contains 11 domains and 39 control objectives, to conduct an asset information technology risk assessment and provide risk level control recommendations.

ISO/IEC 27001 was issued in October 2005 to replace the BS7792-2 standard. The Indonesian version of ISO/IEC 27001 contains several clauses explaining the specifications or requirements to be met when building an Information Security Management System (ISMS). This standard must be independent of information technology products, requires a risk-based management approach, and is designed to ensure

that information security controls can protect information assets that provide security trust (Communication, 2011, p. 10).

Many clauses in the ISO Standard list important requirements that must be met. These include (1) information security management system; (2) management obligations; (3) ISMS internal audit; (4) management review of ISMS; and (5) continuous improvement. In addition to the important requirements contained in this standard, it is necessary to set goals, control, and control information security. It covers eleven areas of the security domain, namely: (1) information security policy; (2) information security organization; (3) asset management; (4) information security human resources; (5) physical and environmental security; (6) communication and operations management; (7) access control; (8) procurement/acquisition; and (9) data protection and sensitive data.

ISO/IEC 27001 establishes rules for developing and operating ISMS, including some controls to control and reduce risks associated with information assets that the organization wants to protect through the implementation of ISMS. The ISO/IEC 27001 Standard sets out the following steps to implement the ISMS standard: (1) Defining ISMS policies (2) The scope of ISMS (3) Making a Risk Assessment (4) Based on a risk assessment and determining the selection of risk controls to be applied (5) Making a Statement of Application.

The ISO 27001 and information security audits also ensure three important components of information security. First is confidentiality, which means that information can only be accessed by authorized persons and distributed to them, so unauthorized persons cannot access or transmit data. Second is the availability of criteria, which means the process runs quickly and the authorized person is not rejected. Third is integrity, which means the credibility of data resources, which ensures that the data is not accidentally altered.

Integrated ISO 27701 and GDPR-based Information Privacy Compliance Requirements Model

In a time when information can be obtained easily, awareness regarding the importance of data security and privacy is increasing. This increase in awareness then leads to developing various models or standards that are useful to ensure compliance with regulations. So that each individual and organization is required to be able to comply with regulations related to data security and privacy. In this case, the commonly used standards for information privacy compliance are ISO 27701 and the

General Data Protection Regulation (GDPR). ISO 27701 is an extension of ISO 27001, which includes privacy-specific matters as part of ISO 27701.

According to the research results conducted by Anwar & Gill (2020), ISO/IEC 27701:2019 and GDPR have overlapping requirements. This is because the approach suggested by the ISO 27701 standard is different from the GDPR approach. ISO 27701 uses a risk-based approach to ensure the privacy of personal information, while GDPR uses a rights-based approach to address broader risks to the rights and freedoms of data subjects. In addition, the results in Table 2 (Anwar & Gill, 2020, p.6-7) also mention ten other gaps or differences between ISO 27701 and GDPR.

ISO 27701 is a model of information privacy compliance requirements that apply to data sets structured in IT assets or on digital media only, while GDPR also applies to unstructured data, namely on digital media and physical media. So, both ISO 27701 and GDPR are standard information privacy compliance requirements that can be used by media companies. If the media company is a physical media, then the standard used is only GDPR. However, ISO 27701 and GDPR can be integrated into information privacy compliance requirements. As can be seen in Table 3 (Anwar & Gill, 2020, p.8-9), ISO 27701 has paragraphs that provide guidance and controls, and the GDPR has articles that set out requirements for the processing of personal data.

Maturity level assessment using ISO 27001:2013 and US Index version 4.0: IDN Media

BSSN publishes guidelines for evaluating and assessing readiness for implementing information security following SNI ISO/IEC 27001. In addition, BSSN states that the WE Index is an assessment that determines the level of information security readiness owned by an organization or institution. However, it cannot be used to assess how well data security works. According to the US index, Personal Data Protection (PDP) includes Governance, Framework, Asset Management, Third Party Technology Aspects, Cloud Service Security, and Third-Party Technology Aspects. The KAMI Index version 4.0 is a tool for evaluating organizational maturity, the completeness of the implementation of ISO/IEC 27001:2013, and an overview of information security governance. The Ministry of Communication and Information Technology makes the KAMI index.

This evaluation tool is not intended to evaluate how well a security system exists. On the other hand, it is intended to give agency leaders an overview of the level of completeness and maturity of the information security framework. The following areas are included in the evaluation

conducted using KAMI Index: electronic systems categories, information security governance, information security risk management risk management information security management framework, information asset management, information technology and security, and more. IDN Media is a technology-based media and content platform company focusing on Indonesia's Millennial and Gen-Z generation. Winston Utomo and William Utomo founded IDN Media in Surabaya on June 8, 2014. In 2020, IDN Media has eleven active digital media platforms: IDN Times, Popbela.com, Popmama.com, Yummy, and GGWP.ID, Duniaku.com, IDN Creative, Event, IDN Creator Network, IDN Foundation, and IDN Programmatic OOH.

Before assessing the area coverage of our Index version 4.0 begins, the process of classifying the use of Electronic Systems (ES) is first carried out in IDN Media to find out how important the role of ES is in IDN Media. The assessment results show low and strategic importance of using electronic systems in IDN Media. The scoring score given was 39, which indicates that it falls into the strategic category.

According to this strategic assessment category, using ES in IDN Media is an integral component of all work processes in IDN Media. The value of ES is very high because it must comply with National Regulations or Standards, have more than 5000 users, associate personal data with other personal data, and have high data security. Based on the importance of using ES in IDN Media, the final value of the assessment of the coverage area of KAMI Index version 4.0 must be more than 609 to obtain a 'Readiness Status' value with a value of 'Good'.

IDN Media's information security has reached a sufficient maturity level, reaching level II of the Basic Framework Fulfillment Standard with a score of 370. Some areas assessed in our Index version 4.0 are not yet eligible and do not meet the ISO 27001 compliance standard. The radar chart shows that one area meets the ISO 27001 compliance standard, three areas meet the operational application category, and one area meets the basic framework. Because the value obtained by IDN Times only meets the importance of using, which is a strategic level with a score of 610, the score obtained is only 370. The OUR 4.0 Index has quite different maturity levels for each domain. The maturity level of the new IDN Media is currently only I-II, while the minimum requirement for ISO 27001 certification is III+

CONCLUSION

This research evaluates organizational maturity using our Index version 4.0 and the importance of using Electronic Systems (SE) in IDN Media, which is considered very important in protecting data and ensuring compliance with applicable security standards. The results showed that the IDN Media information security management system had just reached maturity level II (Application of the Basic Framework). They also have not met the minimum threshold for readiness for ISO/IEC 27001:2013 certification, which is level III+.

Applying the ISO 27001 framework in conducting maturity level assessment (Maturity Level Assessment) in media companies is very important to improve information security and reduce the risk of data leakage. By adopting these standards, companies can implement best practices in information security management, including risk identification and assessment, development of security policies and procedures, and implementation of appropriate security controls. ISO 27001 integration allows companies to strengthen compliance with privacy regulations such as GDPR, thus helping to increase customer trust and protect the company's reputation. This supports previous research on Maturity level assessment which not only provides an overview of the current state of affairs, but also provides a basis for continuous improvement. Organizations can use assessment results to design clear action plans to improve the maturity of their information security controls over time, in line with changes in security threats and business needs. The limitations of this research are the company's object in the literature study that is not analyzed per industry cluster and provides a general picture so the recommendation for further research is to be more specific to the study at the maturity level of information security management assessment in the industry with various business risk characteristics.

REFERENCES

Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016, August). Data security in cloud computing. In *2016 Fifth international conference on future generation communication technologies (FGCT)* (pp. 55-59). IEEE.

Anwar, M. J., & Gill, A. (2021, January). Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model. In Australasian Conference on Information Systems 2020.

Calder, A. (2017). *Nine steps to success: An ISO 27001 implementation overview*. IT Governance Ltd.

Cholez, H., & Girard, F. (2014). Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of Software: Evolution and Process*, *26*(5), 496-503.

Computing, C. O. P. C. (2019). Measuring Information Security And cybersecurity on private cloud computing. Journal of Theoretical and Applied Information Technology, 96(1).

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 04(02), 92-100 https://doi.org/10.4236/jis.2013.42011.

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.

Fagade, T., & Tryfonas, T. (2017, July). Hacking a bridge: An exploratory study of compliance-based information security management in banking organization. In Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017) (Vol. 2, pp. 94-99).

Gabriel, M. H., Noblin, A., Rutherford, A., Walden, A., & Cortelyou-Ward, K. (2018). Data breach locations, types, and associated characteristics among US hospitals. *Am J Manag Care*, *24*(2), 78-84.

Hsu, C., Wang, T., & Lu, A. (2016, January). The impact of ISO 27001 certification on firm performance. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*(pp. 4842-4848). IEEE.

Itradat, A., Sultan, S., Al-Junaidi, M., & Daas, F. (2014). Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. In Jordan Journal of Mechanical and Industrial Engineering (Vol. 8).

Jafri, N. O. O. R. A. I. D. A. N. I. Z. A., & Yusof, M. M. (2018). Managing data security risk in model software as a service (SAAS). Asia-Pacific J. Inf. Technol. Multimedia, 7, 99-117.

Kaban, E., & Legowo, N. (2018). Audit Information System Risk Management Using Iso 27001 Framework At Private Bank. Journal of Theoretical & Applied Information Technology, 96(1).

Lami, K. A. Y. A. (2013, July). Practical Guidelines and Major Issues in Information Security Management Systems Implementations. In 1st International Symposium on Computing in Informatics and Mathematics.

Legowo, N., & Juhartoyo, Y. (2022). Risk management; risk assessment of information technology security system at bank using ISO 27001. Journal of System and Management Sciences, 12(3), 181-199.

Nosova, E., Anisimova, L., Murovana, T., Sviatiuk, Y., & Iafinovych, O. (2021). Information Security System in Provision of the Economic Security and Risk Management of the Enterprise. In CPITS II (2) (pp. 21-31).

Phirke, A., & Ghorpade-Aher, J. (2019). Best practices of auditing in an organization using ISO 27001 standard. Int. J. Recent Technol. Eng, 8(2), 691-695.

Riadi, I., & Prayudi, Y. (2016). A maturity level framework for measurement of information security performance. *International Journal of Computer Applications*, *141*(8), 975-8887.

Saadat, M., & Abbasi, M. U. (2021). Information Security Policy Development: the Mechanism to Ensure Security Over Information Technology Systems. Global International Relations Review, IV, 22-30.

Schmitz, C., Schmid, M., Harborth, D., & Pape, S. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *Computers & Security*, *108*, 102306.

Sugiarto, P., & Suryanto, Y. (2022). Evaluation of the Readiness Level of Information System Security at the BAKAMLA Using the KAMI Index based on ISO 27001: 2013. Int. J. Mech. Eng, 7(2), 3607-3614.

Waruwu, M., & Indrati, A. (2021). IDN Media Information Security Management System Maturity Measurement Analysis Using ISO 27001: 2013 and KAMI Index Version 4.0. International Research Journal of Advanced Engineering and Science, 6(3), 36-40

Zaydi, M., & Nassereddine, B. (2021). A Conceptual Hybrid Approach for Information Security Governance. In International Journal of Mathematics and Computer Science (Vol. 16, Issue 1). http://ijmcs.future-in-tech.net