Improving Organizational Readiness for Cyber Incidents in Maritime Industry Using ISO 27002 Security Framework

Dominica Dini Afiat[1], *Hendy* Tannady[2], *Johanes* Fernandes Andry[3], *Cristiano* Ronaldo Yusup[4], *Edi* Purwanto[5], *Filscha* Nurprihatin[6]

[1.] Department of Management, Sekolah Tinggi Ilmu Ekonomi Bhakti Pembangunan, Indonesia
[2.] Department of Master of Management, Universitas Esa Unggul, Indonesia
[3,4.] Department of Information System, Universitas Bunda Mulia, Indonesia
[5.] Department of Management, Universitas Pembangunan Jaya, Indonesia
[6.] Department of Industrial Engineering, Sampoerna University, Indonesia

Abstract. The current business world requires organizations to operate dependable information systems because digital business activities need organizations to handle extensive data from business transactions. The research develops an information security and data management framework which follows ISO 27002 standards to achieve operational and data security and organizational resilience. The researchers used a qualitative case study method to assess current practices in order to identify security vulnerabilities and create a security framework which complies with global information security standards. The study identified three main problems which included divided data storage systems and missing access control systems and absent incident management systems as factors that caused operational inefficiencies and data mismatches and increased risk to business operations. The study demonstrates that international security standards enable organizations to implement digital transformation by helping them connect their technological systems with existing business processes and their workforce. The study provides a maritime industry model which other companies can use to enhance their data governance practices and operational sustainability through effective information security management.

1 Introduction

Digitalization has transformed business operations which require organizations to implement information systems because this change affects their operations [1]. Shipping companies create digital platforms which connect all their systems that they require to manage customer data and monitor ship operations and execute their financial and security processes [2]. Organizations lack essential security protections because their security management system functions incorrectly and their access control system fails to operate properly and their incident response team lacks sufficient operational resources [3]. The case study demonstrates that an IT administrator deleted vital operational data which caused service interruptions that resulted in lost customer trust because of unregulated data management procedures. Cyber attacks which include ransomware attacks create outages which last multiple days because they disable both logistics and accounting systems resulting in complete business shutdown and major financial damages [4]. Organizations need to create effective information security management systems which should comply with international standards to achieve better system stability and operational reliability and digital performance throughout their existing challenges [5].

The marine sector is one of the most important infrastructures supporting the global commerce [1]. The rising reliance on digital technology in vessel control, cargo monitoring, logistical coordination and financial transactions has greatly enlarged the cyber-attack surface [5]. Thus, the marine enterprises need proper cybersecurity frameworks that can deal with not only technology but also organizational risks [7].

Due to the high reliance on networked digital technology, the maritime sector has become one of the main targets for cyberattacks. Ransomware, data breaches and operational technology disruptions have increased dramatically in recent years among marine events, the European Union Agency for Cybersecurity (ENISA) warned, with ports and shipping businesses constituting an increasing percentage of critical infrastructure assaults [8]. High-profile cases like the 2017 NotPetya ransomware attack on Maersk, which resulted in losses estimated at USD 300 million and stopped global shipping for weeks, show the serious consequences of insufficient cybersecurity preparedness in the maritime industry. In addition to the economic losses, such events threaten the continuity of supply chains, the safety of cargo and the stability of national economies, thereby underlining the necessity for comprehensive and regulated security governance in the organizations of the maritime sector [9].

The researchers selected the ISO 27002 Security Framework because it provides comprehensive guidelines for developing security controls which safeguard information through its established

procedures that include both security monitoring and incident response frameworks [6]. The research applies ISO 27002 standards for monitoring and information security incident management to set requirements for developing an Incident Response Team which will operate at the shipping company [3]. ISO 27002 security frameworks require organizations to create security procedures which combine their operational protocols with methods for continuous risk assessment to measure their security performance against international standards [10][11]. The research shows how maritime companies use ISO 27002 principles to create operational systems which connect their technological assets with their employees and their organizational regulations through literature study and practical fieldwork. The ISO 27002 standard serves as an appropriate method to transform chaotic security processes into a unified information security system that operates across the entire organization [12].

The cybersecurity implementation and information security governance in different businesses have been studied extensively in previous research. However, there are few studies that have explicitly studied the use of ISO 27002 as an operational framework to increase organizational responsiveness to cyber event in the marine sector. Previous research has tended to concentrate on technical security measures and not the integration of security governance, incident response readiness and organizational capacity building in a single framework [11][12].

The current research fills this gap by making three main additions to the existing body of information. First, it evaluates the security vulnerabilities of a maritime corporation in Indonesia empirically, providing insights applicable to the setting of emerging economies, which are under-represented in the literature on information security governance. Secondly, it introduces an operational cybersecurity preparedness architecture based on ISO 27002, adapted to the operational features of maritime enterprises, combining monitoring systems, incident categorization and response procedures in a single governance structure. Third, it shows the role of ISO 27002 as a transformation tool to bridge the gap between fragmented, ad hoc, security practices and a cohesive organization-wide information security management system. The results aim to provide practical advice to marine enterprises who are interested in improving their cyber resilience, using globally accepted criteria.

The research project develops a system that watches over the organization through its information security incident response plan which meets ISO 27002 requirements to enhance both operational capabilities and business performance. The study needs to find security weaknesses because current protection methods require assessment to create standard security controls which will boost data protection and better handle security incidents while reducing future security breaches. The research results will enable the organization to develop more effective security protocols which will reduce operational risks and safeguard critical business data. The study needs to find security weaknesses in current protection methods while creating standard control systems which will deliver practical solutions for better data security and improved incident response and reduced security breach occurrence.

2 Research methodology

The researchers developed a security monitoring system which used ISO 27002 Security Framework procedures to handle incident management based on their case study investigation. The researchers conducted qualitative research to study organizational operations during security vulnerability periods so they could develop specific security recommendations. The research progressed through multiple stages that occurred in sequential order. The first stage involved problem identification, where preliminary observations revealed weaknesses in data protection, lack of structured monitoring, and the absence of a formal incident response mechanism. The findings demonstrated the requirement for an official security framework which would decrease operational risks while maintaining business operations.

The researchers gathered data during the second study phase which used multiple research methods to validate its results through triangulation. The research team used three methods for their study which included observing IT operational activities and conducting semi-structured interviews with system administrators and operational personnel and examining internal documents that contained system usage guidelines and access control procedures and incident documentation.

Data collection took place over a period of roughly eight weeks and included on-site observations, semi-structured interviews and internal document inspections by the study team. During the observation phase the research team directly observed day-to-day activities of IT operations in three functional areas, the IT administration unit, the operations division and the finance department. This direct observation permitted the researchers to see first-hand how data was kept, accessed and handled under the current procedures of the company, and to spot security-relevant behaviors that may not have been divulged during formal interviews.

For the interview phase, seven informants were recruited using purposive sampling so that the respondents had firsthand knowledge of the organization's information systems and security processes. The informants included two IT system administrators, two operational staff members responsible for entering cargo and logistics data, a finance officer who maintained the records of transactions, a department head who oversaw IT governance, and a senior manager who made overall operational decisions. All interviews were conducted individually, lasted between 45 and 75 minutes, and were designed to reduce the social desirability bias. Interview questions were designed around four themes: data management practices, perceived security concerns, incident handling processes and understanding of information security rules. All sessions

were recorded with the participants' agreement and then transcribed for theme analysis.

During the document review phase, a total of nine internal documents were reviewed. They included the organization's current IT usage policies, system access logs, incident logs for the previous 12 months, internal audit reports, data storage procedures, employee job descriptions, vendor contracts for IT services, backup and recovery documentation, and the organization's general operations manual. These papers were evaluated to identify formal or informal security procedures that were already in existence before the introduction of the ISO 27002 framework, to cross-validate the conclusions based on observations and interviews. Triangulation of the three data sources enhanced the internal validity of the findings of the gap assessment and provided a thorough empirical foundation for the suggested cybersecurity preparedness framework.

The third stage required a gap assessment together with risk assessment because both processes needed evaluation of current organizational practices under ISO 27002 control standards. The benchmarking process discovered deficiencies in the monitoring system and access control systems and it identified problems with the incident reporting procedures and documentation practices. The researchers evaluated each gap according to its operational effects and its likelihood of occurrence and its business impact. The study's fourth stage developed a security management framework which covered all monitoring system components and incident classification systems and response protocols and the development of an Incident Response Team (IRT).

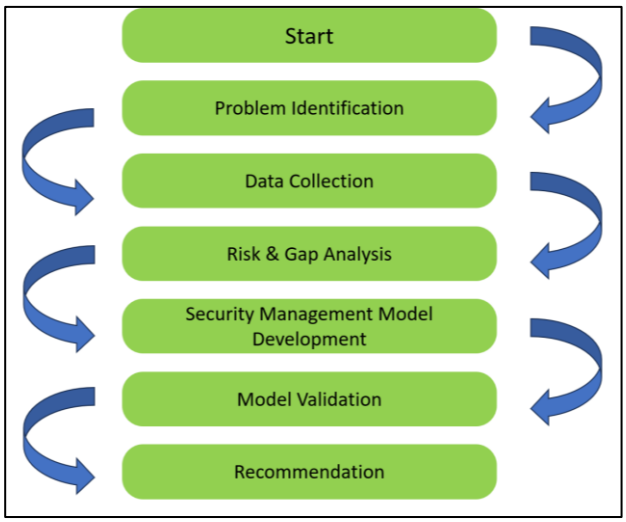

Fig. 1. Research Methodology.

The project reached its conclusion when the final testing stage evaluated the proposed model to determine its compliance with both organizational requirements and actual real-world usage. The organization developed an operational execution strategy which meets ISO 27002 standards because the process developed an operational execution strategy to help the organization transition from reactive problem handling to proactive implementation of information security measures.

3 Result and discussion

The organization achieved better operational results and improved its data management processes through the implementation of an ISO 27002-based information security framework according to the study results. The company used manual methods and unconnected software systems before implementing the new system because these methods led to wrong recordkeeping and made it hard to track inventory and created delays in reporting. The company stored operational data which included sales transactions and stock levels and supplier information in multiple files that lacked a common validation system which resulted in inventory data mismatches. The management team lost system connectivity which stopped them from monitoring company activity through continuous data retrieval, leading decision-makers to rely on draft estimates instead of actual data. The study detected major access control flaws and monitoring process breakdowns and incident response shortcomings which organizations used to build their ISO 27002 security framework.

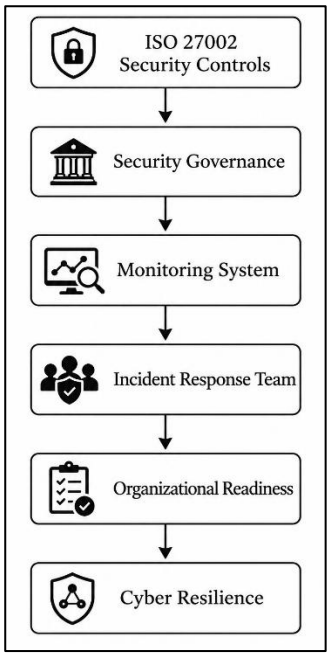

Fig. 2. ISO 27002-Based Cybersecurity Readiness Framework

Based on the results of this study, the proposed ISO 27002-Based Cybersecurity Readiness Framework is shown in Figure 2. The concept illustrates how ISO 27002 security controls might be embedded in corporate governance structures, monitoring activities and incident response capabilities. Factoring in these elements might improve companies' readiness to react to cyber incidents and elevate their overall cyber resilience.

The organization established its primary data management targets through the development of a unified system which tracked all data-related activities across the organization. The system enabled automatic inventory tracking which allowed employees to track inventory changes and work activities across the organization. The new system enabled organizations to

maintain their optimal inventory levels because it generated reports that contained precise inventory information. The system implementation reduced manual data entry mistakes by creating validation systems and standard operating documentation methods. The organization achieved better business outcomes through administrative work reduction which enabled employees to concentrate on more valuable activities. The reliable data enabled management to identify sales patterns and study customer behavior while assessing supplier performance which supported their data-driven decision-making process.

The study produced two main outcomes which included creating improved systems for operational monitoring and emergency response. The organization used informal methods to handle operational disruptions because they failed to create documented procedures which would provide systematic evaluations of incidents. The company established structured logging and reporting systems which followed ISO 27002 principles to determine who would manage data-related incidents. The organization established these structures to boost accountability which helped management to handle operational disturbances in a better way. The establishment of backup systems together with secure data storage facilities improved information accessibility while reducing the likelihood of data loss from hardware failures or human errors. The system brings together hardware devices software applications cloud computing resources and expert personnel to create a single system which enables technological protections to function together with organizational management systems.

The research proved that organizations require both technological investments and employee security knowledge and security culture development to succeed with their information security programs. The organization established training programs together with role definitions which enabled employees to understand their duties for maintaining data protection and system security because information security became an organization-wide responsibility. The employees who learned to use the new system discovered that it functioned as a tool to simplify their work processes instead of creating additional work duties. The framework maintained its effectiveness throughout the entire time because organizations had to enforce their existing procedures which were needed for compliance during the cultural transformation period.

The research results show that implementing ISO 27002 serves as a risk management tool which also enables organizations to implement operational changes. The organization established a secure data management system which replaced its existing manual and decentralized operations to achieve improved efficiency and transparency and strategic capability. The research shows that organizations need to implement structured information security governance systems because these systems protect their assets and improve interdepartmental collaboration and enable data-informed decision making and enhance their capacity to withstand digital threats. Organizations can use internationally recognized security standards as a practical method to enhance their cybersecurity defenses and business performance according to the results which show how organizations operate in today's data-driven business environment.

Table 1. Operational Impact After Implementation of ISO 27002-Based Framework

Operational Aspect	Condition Before Implementation	Condition After Implementation	Organizational Impact
Inventory Management	Frequent discrepancies between physical and recorded stock	Real-time synchronized inventory tracking	Increased accuracy and reduced stock errors
Decision-Making Process	Based on estimations and fragmented reports	Data-driven analysis supported by integrated information	Improved strategic planning and responsiveness
Reporting Efficiency	Manual and time-consuming reporting	Automated and standardized reporting system	Faster report generation and reduced administrative workload
Data Security	Vulnerable to accidental deletion and unauthorized modification	Controlled access, audit trails, and backup protection	Enhanced data integrity and accountability
Incident Handling	Reactive and undocumented problem resolution	Structured monitoring and incident response workflow	Faster recovery and prevention of recurring issues
Cross-Department Coordination	Isolated operational processes	Integrated system connecting sales, inventory, and finance	Improved organizational collaboration
Employee Role Awareness	Limited understanding of data responsibility	Defined roles supported by training and governance	Stronger security culture and compliance

Source: Data Processing by the Authors (2026)

Table 1 illustrates how organizations improved their performance and governance standards after they adopted the ISO 27002-based framework. The centralized data management system allowed businesses to monitor their inventory movements while showing their current stock levels because it provided complete tracking capabilities. The organization established automated systems which replaced its slow manual reporting procedures because these systems could produce correct reports within brief periods, thus increasing operational efficiency while decreasing work demands. Management used integrated data to replace their previous intuition-based decision-making process with evidence-based strategies which relied on dependable analytical tools.

The results of this study align with earlier studies that emphasize the strategic significance of information security governance in enhancing organizational performance and resilience. The use of centralized data management, specified monitoring techniques and coordinated procedures for incident response reinforces the results of previous studies and improves the consistency of information and decreases operational

vulnerabilities [10]. Similarly, the increased capacity to identify and mitigate security flaws aligns with the results of previous studies, who argued that successful cybersecurity management involves not just technological controls but also organizational readiness and response skills [13]. Besides, the results of previous studies underlined the critical contribution of information security culture to employee compliance and overall security effectiveness [14]. The initiation of staff training programs and well-defined security responsibilities explain these findings. The implications of this study's findings are that ISO 27002 should be considered as a comprehensive governance framework and not a technical security standard that covers technology, processes and human resources to improve an organization's readiness to deal with cyber incidents while providing operational efficiency and sustainability of the business in the long run.

The implementation of controlled access systems together with audit trails and backup systems, enabled substantial security advancements which protected data integrity while decreasing possibilities of accidental loss or unauthorized data changes. The organization established organized monitoring systems together with incident response procedures which improved its capacity to find and solve operational issues because they enabled immediate detection of problems, which changed the organization from solving issues after they occurred to solving problems before they happened.

4 Conclusion

ISO 27002 information security frameworks provide organizations multiple advantages because these frameworks enable better data management and increased efficiency in their business operations. The evaluation revealed that unstructured controls created disorganized information storage systems together with disorganized work processes which created higher security risks and business operational risks. The organization used ISO 27002 standards to find important access management deficiencies and testing deficiencies and incident management weaknesses which served as the basis for developing a more secure integrated data system. The proposed framework required organizations to operate their security systems through three elements which included their technological systems and their established operational methods and their personnel educational programs. The organization achieved better data precision while their reporting times decreased and their data processes became more transparent and their organization could make decisions based on digital evidence. The implementation showed that organizations can achieve better security results through structured governance systems which reduce risks and drive their operational advancements while they pursue digital transformation goals. The framework will undergo enhancement in future research through the integration of quantitative performance metrics and testing of its effectiveness across multiple business sectors to confirm its value in helping organizations achieve resilience.

The findings of this study have major practical implications for maritime businesses, as it suggests that the adoption of security measures based on ISO 27002 might enhance data governance, raise incident response capabilities, and improve the responsiveness of organizations to cyber threats. We urge management establish formalized monitoring procedures, specialized Incident Response Teams, and ongoing security education initiatives to support sustainable cybersecurity practices. Theoretical implications This research contributes to the literature on information security governance by expanding the scope of ISO 27002 from a technical compliance to a broader framework for building organizational cyber resilience through the integration of technology, processes and human resources. This research, however, is limited to a single example in the marine business and it is qualitative in nature. Therefore, it is advised that future study experimentally evaluate the proposed paradigm across multiple sectors and organizational contexts utilizing quantitative approaches and integrating observable measures of cybersecurity performance to increase the generalizability and robustness of the results.

References

1. F. Zeng, A. Chen, S. Xu, H. K. Chan, Y. Li, Digitalization in the Maritime Logistics Industry: A Systematic Literature Review of Enablers and Barriers, J. Mar. Sci. Eng. 13, 797 (2025). https://doi.org/10.3390/jmse13040797
2. M. Fruth, F. Teuteberg, Digitization in maritime logistics—What is there and what is missing?, Cogent Bus. Manag. 4, 1411066 (2017). https://doi.org/10.1080/23311975.2017.1411066
3. A. Ahmad, S. Maynard, S. Park, Information security strategies: Towards an organizational multi-strategy perspective, J. Intell. Manuf. 25, 357–370 (2014). https://doi.org/10.1007/s10845-12-0683-0
4. Klumpp, M., & Loske, D., Sustainability and resilience revisited: Impact of information technology disruptions on empirical retail logistics efficiency. *Sustainability, 13*(10), 5650 (2012). https://doi.org/10.3390/su13105650
5. Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M., The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76–105 (2021). https://doi.org/10.1108/TQM-09-2020-0202
6. Kamil, Y., Lund, S., & Islam, M. S., Information security objectives and the output legitimacy of ISO/IEC 27001: Stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and e-Business Management, 21*(4), 699–722 (2023). https://doi.org/10.1007/s10257-023-00646-y
7. Martínez, F., Sánchez, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E., Maritime

cybersecurity: Protecting digital seas. *International Journal of Information Security, 23*, 1429–1457 (2024). https://doi.org/10.1007/s10207-023-00800-0

8. European Union Agency for Cybersecurity (ENISA), *Port cybersecurity: Good practices for cybersecurity in the maritime sector*. Publications Office of the European Union, (2019). https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
9. Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
10. J. Mamani Idme, J. L. Valenzuela García, S. A. Huaraz Morales, L. Andrade-Arenas, Implementation of information security controls based on ISO/IEC 27002 in organizational systems, Int. J. Adv. Sci. Eng. Inf. Technol. 11, 2275–2282 (2021). https://doi.org/10.18517/ijaseit.12.1.13914
11. H. Taherdoost, Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview, Electronics, 11, 14 (2022). https://doi.org/10.3390/electronics11142181
12. International Organization for Standardization, *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection—Information security controls*. ISO, (2022). https://www.iso.org/standard/75652.html
13. Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., Sushil, & Dwivedi, Y. K., Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change, 170*, 120872 (2021). https://doi.org/10.1016/j.techfore.2021.120872
14. Tolah, A., Furnell, S. M., & Papadaki, M., An empirical analysis of the information security culture key factors framework. *Computers & Security, 108*, 102354 (2021). https://doi.org/10.1016/j.cose.2021.102354