DecisionTech Review
Vol. 3, 2023, 1-6. DOI: 10.47909/dtr.05

ORIGINAL RESEARCH

Pro-Metrics

Risk management model for information security

Jhon Arista Alarcon

Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional de San Martín – Tarapoto, Peru.
Email: jaristaa @alumno.unsm.edu.pe
ORCID: 0000-0003-3137-9087

ABSTRACT
This study emphasizes the significance of risk management models in bolstering information security within organizations. As information systems increasingly become integral to business operations, materializing business risks without adequate risk management has become exceedingly costly. The paper investigates the elements and activities crucial for developing frameworks that manage risks in information security. By conducting a literature review, this research identifies common processes across various risk management models, such as asset identification, risk analysis, and the establishment of controls. It highlights adopting standards like ISO 31000 and ISO 27005 and methodologies such as Magerit and COSO, advocating for a personalized approach to risk management. This tailored approach aids organizations in identifying information assets and understanding the inherent risks, thereby enabling the establishment of quantitative metrics for risk assessment and the implementation of protective controls. The study underscores the necessity of a risk management model in achieving an organization's objectives and mitigating information security risks, advocating for models that adapt to specific organizational needs rather than directly copying existing standards. The findings suggest that technological innovations and predictive analytics, through Big Data and machine learning, are future directions for enhancing risk management and information security levels. This research provides a foundational insight for future studies exploring risk management frameworks in diverse organizational contexts.
Keywords: risk management; information security; information management; risk analysis.

1. INTRODUCTION

As information systems are increasing in business, risk materialization has become increasingly costly, even more so if adequate risk management is not carried out (Sasidharan *et al.,* 2022). For example, a study by the Organization of American States (OAS) and the Inter-American Development Bank (IDB) indicates that in 2016, a loss of $575 billion was estimated worldwide due to information security incidents. Meanwhile, in the Caribbean and South America, a loss was estimated between $90 and 180 billion (Turk *et al.,* 2022).

The development of the organization's own operations, processes, and procedures occurs in this context, in which the aim is to promote digital transformation initiatives and promote the use of emerging technologies,

Received: 09-02-2023. **Accepted:** 09-05-2023. **Published:** 16-05-2023

How to cite: Alarcon , J. A. (2023). Risk management model for information security. *DecisionTech Review, 3,* 1-6. https://doi.org/10.47909/dtr.05

DecisionTech Review
Vol. 3, 2023, 1-6. DOI: 10.47909/dtr.05

whose adoption collides with manual and mechanical processes that are current (which are of value to the organization), and others that have strong roots in the organizational culture, presenting resistance to change.

This situation becomes more complex when considering that the operators of the organization's processes do not always have fully identified all the information assets they manage, not knowing their value or appropriate treatment. Rodrigo Yashir, as cited in (Preidys & Ramanauskait, 2021), in turn, states that: "with respect to the responsibilities of matters about the security of information assets, there is a lack of understanding in organizations," especially those in the public sector, manifesting itself at the leadership level, which usually It is the responsibility of the technological areas, without the support of senior management, having an orientation towards computer security, without fully considering comprehensive aspects of security-oriented to information assets, whether physical or digital; thereby increasing the risks to which the organization is exposed.

In another study by Digiware, it was estimated that the economic impact was high in Peru, $4 billion, so risk management should be considered a more serious issue within companies. In a 2015 Ernst & Young study, 100% of respondents indicated that their current information security scheme does not fully cover the needs of their organization. In this study, 41% of companies consider they have minimal probability of detecting a sophisticated attack. They admitted that the main reason hindering information security effectiveness is 100% due to budgetary constraints and 89% due to the lack of specialized resources, respectively (Sasidharan *et al.*, 2022).

In this scenario, using models that contribute to the adequate management of these risks can reduce the negative impacts of risks inherent to the information assets that the organization has, applying analytical techniques that allow knowing the level of dangerous events to evaluate the impact, probability, and consequences that they could generate, contributing to the analysis, identification, and treatment of said risks.

This research focuses on reviewing the literature referring to risk management models, to identify the elements and activities to be considered while developing frameworks that allow managing risks pertaining to information security.

2. SOURCE

2.1. Risk management model

A risk management model contributes to the organization in identifying its information assets, as well as knowing the risks inherent to them. In addition, it allows establishing metrics that allow the value of the risk to be quantitatively measured, knowing the vulnerabilities, establishing necessary controls that protect said assets from attacks or security threats and establishing controls that allow facing the risks that arise.

The development of personalized risk management models is supported by standards and/or management methodologies, such as ISO 31000, ISO 27005, Magerit, COSO, etc. The risk management models analyzed are characterized by having some common processes, such as:

— Establishment of the context.
— Definition of scope.
— Identification of assets.
— Identification, analysis, and evaluation of risks.
— Declaration of Applicability.
— Risk treatment.
— Compliance review.
— Measurement (Measure effectiveness of controls)
— Corrective actions.
— Registration and report.
— Monitoring, follow-up, and review.
— Communication and consultation.

Adequate risk management is used as a baseline for determining and defining the organization's objectives (Preidys & Ramanauskait, 2021). Therefore, the basic criteria for fulfilling these objectives are defined in this phase. It is necessary to consider that risk management must be able to integrate with the organization's context, both internal

and external. This entails defining the internal and external conditions to establish the risk management framework. At the internal level, it is considered:

— The organizational culture.
— Organization resources.
— Organizational processes and objectives.

2.2. Information security

It contemplates the protection of data or assets that store information that is essential for an organization. The management of said assets may or may not involve the use of technology (Ma, 2022). A proactive process or planning is essential to protect information, which guarantees efficient use in processing information (Li, 2022). To this end, organizations must consider measures that increase the related aspects.

3. MATERIALS AND METHODS

According to the reviewed literature, various elements, processes, and common activities are identified while developing risk management models as a reference guide in their development, having an orientation towards the security of the risk information management model. That is why we ask ourselves: How important are risk management models in information security for organizations?

To answer this question, it was carried out based on a systematic review, which requires a sequence of locating, analyzing, ordering, counting, and evaluating a bibliography from defined sources over some time. The advantages are that the process is replicable, scientific, and transparent (Tranfield; Denyer; Smart, 2003). This article proposes to review the concepts associated with risk management models in organizations based on a protocol that allows the specific criteria and parameters of the information search and analysis process to be defined in advance. It specified the process that would be followed during the search, the filters to select the information, and the flow it would follow until it was appropriately structured. The above is summarized in three major phases:

1. The choice of the information source and sample data selection.
2. The transformation of data through the use of bibliometric techniques.
3. The report of the results.

The literature review was carried out using mixed methods, that is, content analysis and statistical analysis (Lu *et al.,* 2014), for which not only publication trends, main authors, and journals were identified, but also They managed, compiled, and analyzed the various elements or data of the documents with the support of the Maxqda qualitative data analysis software, which allowed structured data to be analyzed. The systematic review report was constructed and, at the same time, updated throughout the research.

The review started from an exploratory search, through which the expression information security risk management was identified as a term equivalent to risk management in information security. The databases of the Institute of Electrical and Electronics Engineers (IEEE), ScienceDirect, and Web of Science were selected, considering that it is an international reference for its content of quality articles together with the Scopus database.

The search equation used was:

TS: ("information security")

This equation was intended to be broad and have the maximum possible coverage while still having a manageable size of the results, which is why using logical operators, search strings, and restrictions in specific security areas was avoided to have complete information for subsequent bibliometric and qualitative analyses. We consulted for publications indexed between January 1, 2019, and September 30, 2022 (date of last data update). Documents considered gray literature and those over four years old with the dates above were excluded, resulting in 33 articles.

The titles of the articles based on theoretical and empirical research were examined, referring to:

1. Good practices in information security;
2. The frameworks or methodologies for developing a risk management model.
3. Information security policies and controls to manage risks.
4. Risk management within companies.

DecisionTech Review
Vol. 3, 2023, 1-6. DOI: 10.47909/dtr.05

This article is proposed as a starting point for future research that considers delving into each proposed organizational category and studying other work frameworks in various organizational contexts.

4. RESULTS AND DISCUSSION

Several articles mention the use of the ISO/IEC 27000, ISO/IEC 31000, and COBIT standards, which are known as a best practices guide, presented as a framework, and consider the philosophy that IT resources need to be managed by a set of processes naturally grouped to provide the relevant and reliable information that an organization requires to achieve its objectives, and finally allows an evaluation of the processes involved in the organization. The following table shows the results of the investigations regarding risk management considering the different factors.

Authors	Good practices	Policies	Risk management	Information and network systems	Security incidents
(Hamdi *et al.*, 2019)	Balanced scorecard	Information Security policies	Asset classification	Cloud computing	Computer crime
(García & Moreta, 2019)	Best practices	Information security policy	Asset identification	Computer networks	Data security
(Antunes *et al.*, 2022)	Business practice	IS security policies	Business information risk	ICT security tools	Downtime loss
(Cordero, 2021)	Certification	National information security policy	Controls	ICT	Event studies
(Denker, 2021)	Conformity assessment procedure	Policy	Information assets	Information systems	Insider trading
(Gonzalez-Granadillo *et al.*, 2021)	Information security certification	Power and politics	Information security risk analysis	Information systems security	Nonmalicious security violation
(Sai Manoj *et al.*, 2019)	Information security compliance	Security policy	Information security risk management	Information systems security management	Organizational effectiveness
(Walkowski *et al.*, 2020)	Information security management system	Security policy adoption	Information security threats	Information systems services	Security breaches
(Zhu *et al.*, 2021)	Information security requirements	Security policy implementation	Information security vulnerabilities	Information technology capabilities	Security shocks
(Roponen *et al.*, 2020)	Information systems security standards	Technology policy	Information systems risk	Information technology security	Information leakage

Table 1. Research related to the systematic review of risk management. Source: prepared by the author.

Organizations contemplate managing information security with greater precision regarding existing risks or those that may materialize at some point (Oh *et al.,* 2021). As the review of the articles demonstrates, many factors must be considered. Although many of these organizations choose to implement an information security management system (ISMS) directly, they fail to mitigate security risks or incidents (César, 2021) because it is not formulated a model that allows you to solve your needs regarding risk management

and information security, as evidenced in Table 1. This alludes to the importance of a risk management model for an organization that gives a starting point at which each aspect is considered, allowing it to achieve its objectives and goals (Ekström *et al.,* 2021).

For Zhao *et al.,* (2019), organizations are currently choosing to consider personalized models for risk management based on the calculation by risk groups, in the same way (Johnson *et al.,* 2021) mentions that the analysis probabilistic risk analysis (PRA), which allows analyzing the performance of the system when an interruption occurs, will enable organizations to anticipate this situation, which the model should contemplate or integrate.

5. CONCLUSIONS

Implementing risk management models aligned to an organization's particular requirements contributes to the reduction of costs and makes the processes of an organization more predictable. This helps senior management to make better decisions to communicate and resolve their risks more effectively. An existing standard should not be copied, applied, and used as a standard practice since its adaptability to the organization must be considered and applicable to specific situations. Organizations face different types of risks and must take different approaches to eliminate or control them.

A risk management model contemplates exploring the organizational factors and risk management practices that affect the achievement of the objectives they consider strategic. The purpose of managing risks is to develop a detailed analysis of the organization, its operations, assets, processes, and existing interrelationships to establish a complete list of risks, which involves identifying, analyzing, and providing risk treatment alternatives.

The trend for risk management is towards a decrease in human interventions; this will increase as regulations become more complex and compliance controls tend to be more demanding. To reduce error levels, Those that cannot be automated will require a higher level of control, monitoring, and follow-up. Technological innovations will contribute to decision-making in risk management; they will allow the use of large amounts of information such as Big Data and "machine learning," to develop tools that provide predictive information and increasingly precise using the identification of behavioral patterns from data sets without human intervention in the data learning process, which will increase information security levels.

Conflict of interest

The author declares that there is no conflict of interest.

Statement of data consent

The data generated during the development of this study has been included in the manuscript. ■

REFERENCES

Antunes, M., Maximiano, M., & Gomes, R. (2022). A Client-Centered Information Security and Cybersecurity Auditing Framework. *Applied Sciences (Switzerland), 12*(9). https://doi.org/10.3390/app12094102

César, R. G. (2021). *Propuesta de Implementación de un Sistema de Gestión de Seguridad de la Información aplicando la Norma ISO 27001:2013 para una Institución del Estado en la Provincia Constitucional de Callao-2021*.

Cordero, J. V. (2021). ISO/IEC standards as mechanisms of proactive responsibility in the General Data Protection Regulation. *Revista de Internet, Derecho y Politica, 33*(33), 1-12. https://doi.org/10.7238/IDP.V0I33.376366

Denker, A. (2021). Protection of privacy and personal data in the big data environment of smart cities. International Archives of the Photogrammetry, *Remote Sensing and Spatial Information Sciences - ISPRS Archives, 46*(4/W5-2021), 181-186. https://doi.org/10.5194/isprs-Archives-XLVI-4-W5-2021-181-2021

Ekström, T., Sundling, R., Burke, S., & Harderup, L.-E. (2021). Probabilistic risk analysis and building performance simulations

– Building design optimisation and quantifying stakeholder consequences. Energy and Buildings, 252, 111434. https://doi.org/10.1016/j.enbuild.2021.111434

García, F. Y. H., & Moreta, L. M. L. (2019). Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI; Focused on Shipping Companies. *Applications in Software Engineering - Proceedings of the 7th International Conference on Software Process Improvement, CIMPS 2018,* 29-39. https://doi.org/10.1109/CIMPS.2018.8625848

Gonzalez-Granadillo, G., Menesidou, S. A., Papamartzivanos, D., Romeu, R., Navarro-Llobet, D., Okoh, C., Nifakos, S., Xenakis, C., & Panaousis, E. (2021). Automated cyber and privacy risk management toolkit. *Sensors, 21*(16), 1-28. https://doi.org/10.3390/s21165493

Hamdi, Z., Anir Norman, A., Nuha Abdul Molok, N., & Hassandoust, F. (2019). A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors. *Journal of Physics: Conference Series, 1339*(1). https://doi.org/10.1088/1742-6596/1339/1/012103

Johnson, C. A., Flage, R., & Guikema, S. D. (2021). Feasibility study of PRA for critical infrastructure risk analysis. *Reliability Engineering and System Safety, 212,* 107643. https://doi.org/10.1016/j.ress.2021.107643

Li, Y. (2022). Security and Risk Analysis of Financial Industry Based on the Internet of Things. *Wireless Communications and Mobile Computing, 2022*. https://doi.org/10.1155/2022/6343468

Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing and Management, 59*(1), 102744. https://doi.org/10.1016/j.ipm.2021.102744

Oh, R., Lee, Y., Zhu, D., & Ahn, J. Y. (2021). Predictive risk analysis using a collective risk model: Choosing between past frequency and aggregate severity information. *Insurance: Mathematics and Economics, 96,* 127-139. https://doi.org/10.1016/j.insmatheco.2020.11.002

Preidys, S., & Ramanauskait, S. (2021). *Applied Sciences Educational Organization's Security Level Estimation Model.*

Roponen, J., Ríos Insua, D., & Salo, A. (2020). Adversarial risk analysis under partial information. *European Journal of Operational Research, 287*(1), 306-316. https://doi.org/10.1016/j.ejor.2020.04.037

Sai Manoj, K., Mrudula, K., & Phani Srinivas, K. (2019). Risk factors and security issues in various cloud storage operations. *International Journal of Innovative Technology and Exploring Engineering, 8*(12), 311-320. https://doi.org/10.35940/ijitee.K1815.1081219

Sasidharan, M., Burrow, M. P. N., Ghataora, G. S., & Marathu, R. (2022). A risk-informed decision support tool for the strategic asset management of railway track infrastructure. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 236(2), 183-197. https://doi.org/10.1177/09544097211038373

Turk, Ž., Sonkor, M. S., & Klinc, R. (2022). Cybersecurity assessment of bim/cde design environment using cyber assessment framework. *Journal of Civil Engineering and Management, 28*(5), 349-364. https://doi.org/10.3846/jcem.2022.16682

Walkowski, M., Krakowiak, M., Oko, J., & Sujecki, S. (2020). Efficient algorithm for providing live vulnerability assessment in corporate network environment. *Applied Sciences (Switzerland), 10*(21), 1-16. https://doi.org/10.3390/app10217926

Zhao, X., Chen, Q., Xue, J., Zhang, Y., & Zhao, J. (2019). A method for calculating network system security risk based on a lie group. *IEEE Access, 7,* 70610-70623. https://doi.org/10.1109/ACCESS.2019.2919141

Zhu, T., Haugen, S., & Liu, Y. (2021). Risk information in decision-making: definitions, requirements and various functions. *Journal of Loss Prevention in the Process Industries, 72,* 104572. https://doi.org/10.1016/j.jlp.2021.104572