Journal of Information Technology and Cyber Security 4(1) January 2026: 41-53 EISSN 2987-386X | PISSN 2987-3878
DOI:10.30996/jitcs.132669

A Data Driven Approach for Information Technology Risk Modelling and Visualization: Integrating ISO 31000 and Monte Carlo Simulation

Rahmania Kumalasari [1], Lutfiyah Dwi Setia [2,*], Tri Septianto [3]

[1,2,3] Department of Information Technology, Politeknik Negeri Madiun, Indonesia
* Corresponding author: lutfiyah17@pnm.ac.id

Received: 17 October 2025
Accepted: 05 January 2026
Revised: 05 January 2026
Available online: 04 February 2026

To cite this article: Kumalasari, R., Setia, L. D., & Septianto, T. (2026). A Data Driven Approach for Information Technology Risk Modelling and Visualization: Integrating ISO 31000 and Monte Carlo Simulation. *Journal of Information Technology and Cyber Security, 4*(1), 41-53. https://doi.org/10.30996/jitcs.132669

Abstract

Information technology (IT) plays a critical role in enhancing organizational efficiency, accelerating decision-making, and strengthening competitiveness. However, as a core infrastructure, IT also introduces various risks that must be managed effectively to ensure business continuity. This study examines IT risk management at Company XYZ by integrating the ISO 31000 framework with the Monte Carlo Simulation method to quantify potential losses from 18 identified risk categories, including system failure, human error, cyberattacks, and natural disasters. To improve the interpretation and communication of risk outcomes, the research employs interactive data visualization using the Shiny dashboard (R). The simulation results show an average expected annual loss of IDR 478 million, with major risks originating from data corruption, backup failures, and cybercrime, while external factors such as earthquakes and fires also have significant impacts. This integrative approach demonstrates how ISO 31000, Monte Carlo Simulation, and interactive visualization can strengthen data-driven and transparent IT risk management for informed organizational decision-making. However, this study is limited to a single organizational case and simulated data assumptions, which may affect the generalizability of the findings.

Keywords: business and cybersecurity continuity, information technology risk management, ISO 31000, Monte Carlo Simulation, quantitative risk analysis, shiny dashboard.

1. Introduction

Information Technology is widely perceived as a crucial component of organizational advancement due to its role in improving operational efficiency, accelerating decision-making processes, and providing a competitive advantage to organizations. These advantages can be achieved by optimizing business process, reducing costs and time, and solving problems from both internal and external perspectives (Ariyandi & Purwanti, 2025). However, the use of information technology must be properly managed as to ensure security and efficiency of of the IT systems and infrastructure (Abdillah, et al., 2020). Therefore, effective information technology management is required to systematically address potential risks, protect organizational assets, enhance productivity, and reduce potential losses arising from organizational uncertainty (Anita, et al., 2023).

This study focuses on the information technology division at the company of XYZ, which focuses on technology development. This company relies heavily on information technology to support most business processes, where any disruption in IT operations may result in significant operational challenges. The IT division plays a critical role in ensuring the availability of network infrastructure and data security. However, the division is exposed to a high level of vulnerability, including server failures, cyberattacks, human error, infrastructure damage, and natural disasters. These conditions highlight the importance of implementing risk management based on international standards (ISO) to ensure the continuity of organizational operations.

While several mitigations and defensive actions have been conducted, the system remains

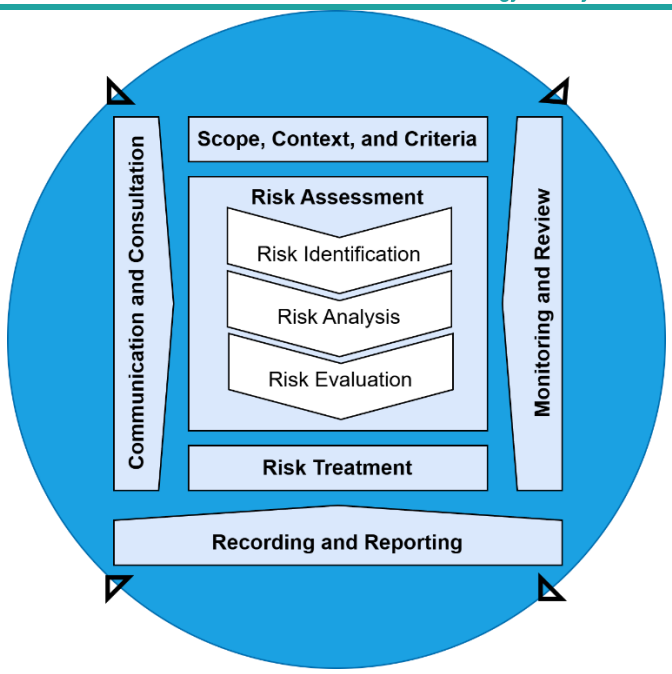


Fig. 1. Risk management process based on ISO 31000 (Institute of Risk Management, 2018).

vulnerable. Frequent issues include server disruptions and cyberattacks, unavailability of real-time monitoring system or structured risk management framework, including the absence of early warning mechanisms or simulations of potential losses.

This situation provides a strong rationale for implementing risk analysis based on the ISO 31000 standard, particularly to identify and prioritize risk treatment strategies. Risk management defined as a coordinated effort to direct and control organizational activities, aims to reduce potential losses and can also serve as a basis for establishing standardized operational procedures within the organization (Wibowo, 2022). The role of risk management is crucial in ensuring the achievement of organizational objectives and providing assurance to stakeholders (Kramarz & Korpysa, 2023).

From a practical perspective, this study offers a foundation for management to formulate more proactive and efficient risk mitigation strategies, supported by the development of a simple interactive dashboard using a Shiny App.

This study contributes to the literature on information technology risk management by extending the application of the ISO 31000 framework beyond descriptive and qualitative assessments. Unlike prior studies (Wibowo, 2022; Miftakhatun, 2020), which primarily relied on qualitative risk identification and descriptive evaluation, this research integrates Monte Carlo Simulation to quantitatively analyze 18 categories of IT risks, encompassing natural risks (e.g., floods and earthquakes), human-related risks (e.g., human error and cybercrime), and infrastructure-related risks (e.g., server downtime, data corruption, and backup failure).

The simulation results provide quantitative loss metrics, including mean annual loss, Value at Risk (VaR), and Conditional Value at Risk (CVaR), revealing that the average potential annual loss may reach approximately IDR 478 million. The findings further identify Data Corruption, Backup Failure, and Cybercrime as the highest-priority risks, while external risks such as earthquakes and fires also exhibit potentially significant impacts. This quantitative insight enables objective risk prioritization, which has not been sufficiently addressed in earlier ISO 31000-based studies (Fig. 1).

From a methodological perspective, this research advances prior work by strengthening the risk analysis and evaluation stages of ISO 31000 through stochastic modelling. While previous research has demonstrated that ISO 31000 effectively supports the identification and management of internal and external risk (Miftakhatun, 2020; Orellano & Gourc, 2025; Muryanti & Hartomo, 2021), such studies largely stopped at qualitative or semi-quantitative outcomes. In contrast, this study transforms ISO 31000 into a data-driven and measurable decision-support framework, thereby enhancing its practical applicability in IT divisions with high operational vulnerability.

Another key contribution lies in the integration of interactive visualization using Shiny App. The proposed approach not only delivers quantitative risk metrics but also presents them through an interactive

dashboard that supports what-if analysis, recurring risk monitoring, and real-time reporting. Implemented using the R programming language, the model ensures reproducibility, automation, and transparency, which are rarely addressed in prior ISO 31000 implementations.

Overall, this research introduces a threefold contribution: 1) the structured governance foundation of ISO 31000; 2) Monte Carlo Simulation for quantitative risk measurement and prioritization; and 3) interactive visualization via Shiny App for continuous monitoring and managerial decision support.

By combining international risk governance standards with advanced analytical and visualization techniques, this study offers a novel, integrated, and evidence-based approach to IT risk management. The findings provide valuable contributions to practitioners and researchers in information systems, data science, and risk analytics, particularly in developing transparent, adaptive, and data-driven risk management systems to support effective managerial decision-making.

2. Literature Review

This study employs multiple approaches and methods, with the analysis focused on three main components: the ISO 31000 risk management framework, Monte Carlo Simulation as a quantitative approach for analyzing uncertainty, and Shiny Apps as a platform for interactive visualization of the analytical results.

2.1. ISO 31000: Risk Management

ISO 31000 provides principles and guidelines applicable to various types of organizations (Glette-Iversen, Flage, & Aven, 2023; Zagoto & Sitokdana, 2021). The framework emphasizes that risk management should be an integral part of organizational decision-making rather than merely an administrative activity (Tanamaah & Berliana, 2021). The elements of the ISO 31000 framework enable organizations to systematically identify and manage diverse risks, including data security threats, system failures, and digital service disruptions.

Most existing studies on the implementation of ISO 31000 have been conducted in large industrial sectors at developed countries. Meanwhile, this study aims to integrate ISO 31000 with quantitative simulation to strengthen organizational IT governance, security, and complex cyber security problems. A study conducted by (Saputra & Hasanudin, 2025) demonstrates that ISO 31000–based risk management, management control systems, and leadership styles can significantly influence corporate financial performance under conditions of environmental uncertainty driven by policy changes. Building on this insight, the present study seeks to address the existing research gap by combining ISO 31000 principles with Monte Carlo Simulation to establish a more adaptive and data-driven risk decision-making framework suited to the contemporary digital environment.

2.2. Monte Carlo

Monte Carlo Simulation is a computational technique used to model and analyze uncertainty in strategic decision-making processes (Ningsih & Arsal, 2022). This technique generates a probabilistic distribution of possible results by performing repeated random experiments to estimate the outcomes of complex processes. In the context of risk management, Monte Carlo Simulation is employed to estimate potential losses, determine risk values, support risk prioritization, and enhance decision-making quality (Hojjati & Noudehi, 2015).

Although Monte Carlo Simulation has been widely applied in sectors such as finance, energy, and manufacturing, this study adopts Monte Carlo Simulation as a quantitative approach to calculate and identify risks within the ISO 31000 risk management framework. This integration enables a more systematic, measurable, and data-driven assessment of information technology risks.

2.3. Shiny Apps (R Programmming)

The visualization of simulation modelling in this study is implemented through a simple interactive web-based dashboard using Shiny, an R programming package which enable rapid and efficient development of interactive applications (Rhamadhani & Iswari, 2022). The Shiny application consists of two main components: a user interface (UI) that provides interactive visual displays and a server component that manages data processing and application logic (Khedr & Hilal, 2021).

In risk management research, Shiny applications are commonly used to present Monte Carlo Simulation results and key risk indicators (KRIs) to facilitate transparent, communicative, and easily interpretable data visualization (Jak, Jorgensen, Verdam, Oort, & Elffers, 2021). Shiny applications are widely used in data analysis research as a communication tool for presenting risk management evaluation results to enhances transparency and interactive risk decision-making by integrating Monte Carlo Simulation with the ISO 31000 framework through Shiny-based visualization.

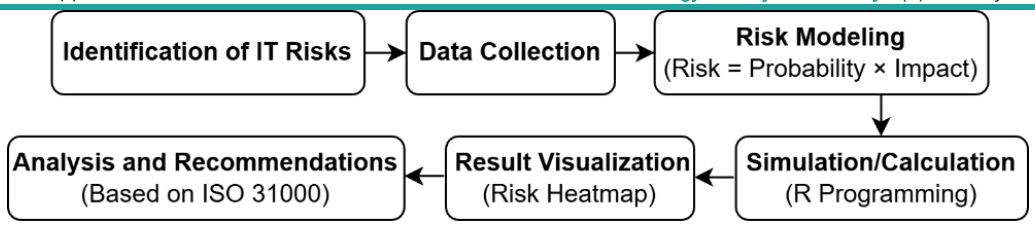


Fig. 2. Research methods.

Algorithm 1. Monte Carlo Risk Simulation with continuous variables.

Input:
n: number of Monte Carlo Simulations
μ_p, σ_p: mean and standard deviation of risk probability
μ_i, σ_i: mean and standard deviation of risk impact

Output:
$Expected\_Risk$, $Risk\_Std$, $P90\_Risk$

Initialize number of simulations n
Generate probability values $P \sim N(\mu_p, \sigma_p)$
Constrain P to the interval [0,1]
Generate impact values $I \sim N(\mu_i, \sigma_i)$
for $k = 1$ to n do
    $Risk(k) \leftarrow P(k) \times I(k)$
end for
$Expected\_Risk \leftarrow mean(Risk)$
$Risk\_Std \leftarrow standard\_deviation(Risk)$
$P90\_Risk \leftarrow 90th\_percentile(Risk)$
Return $Expected\_Risk$, $Risk\_Std$, $P90\_Risk$

$$EL = \frac{1}{n}\sum_{i=1}^{n} R_i \quad (1)$$

3. Methods

This research methodology employs a computerized simulation approach using Monte Carlo Simulation implemented in the R programming language. The methodology is designed to analyse information technology risks in the IT Division of PT XYZ, with reference to the ISO 31000 risk management framework. As illustrated in Fig. 2, the figure outlines the research process undertaken in this study.

The initial stage of this study involved identifying information technology (IT) risks within the IT Division of PT XYZ, covering environmental, human-related, and infrastructure system risk categories. This identification process was guided by the principles of the ISO 31000 framework, which emphasize potential threats that may disrupt organizational operations.

Data collection was conducted through interviews, incident history and system log analysis, as well as secondary data sources to estimate the probability and impact of identified risks. These data were subsequently used as inputs for risk modelling using a probabilistic simulation approach. All data utilized in this study underwent an anonymization process by removing specific identifiers related to the organization and involved individuals, while adhering to ethical standards in information technology research. Findings that could potentially reveal sensitive IT system details are not disclosed directly. Through these ethical constraints and controlled data access, the study maintains a balance between scientific validity and the protection of organizational privacy and information security.

Risk modelling was performed using quantitative analysis techniques based on fundamental risk calculation principles, in which risk is defined as the product of event probability and impact severity. Higher probability or impact values result in greater risk levels. In addition to deterministic risk calculations based on historical conditions, Monte Carlo Simulation was employed to capture variability and uncertainty in probability and impact estimates. This method was selected due to its ability to generate risk distributions that reflect the underlying characteristics and proportions of risks within PT XYZ, thereby representing the overall population more accurately.

The Monte Carlo algorithm applied in this study involves defining risk variables (Algorithm 1), assigning appropriate probability distributions, executing simulations over n iterations, and generating loss values and risk percentiles. The simulation results are then visualized using histograms and heatmaps. The

implementation was carried out using the R programming language with Monte Carlo Simulation procedures.

The Monte Carlo simulation produces several key indicators for measuring and evaluating information technology risk in the IT Division of PT XYZ. The primary indicator is the Expected Loss (EL), as presented in Eq. (1), which reflects the estimated annual loss calculated from the full set of simulation outcomes. In this formulation, n denotes the total number of simulation iterations, and R_i represents the risk value obtained in the i-th iteration.

Next, the Standard Deviation (σ) is used to measure the degree of risk variability and uncertainty, where the higher σ value indicates greater risk fluctuation and, consequently, higher uncertainty regarding potential losses. The next indicators are Percentile Risk (P90 and P95), which represent extreme risk levels (high-end risk) that occur only in the worst 10% or 5% of simulated scenarios. These indicators assist management in anticipating maximum risk conditions that may arise.

Besides quantitative indicators, the simulation results are visualized using a Risk Heatmap, which represents the combination of probability and impact for each risk category and supports the prioritization of mitigation actions based on urgency. Meanwhile, the Histogram of Loss Distribution illustrates the distribution of simulated loss values, providing insight into the risk pattern, whether the distribution is symmetric, skewed, or multimodal. symmetric, skewed, or multimodal. Collectively, these indicators provide a comprehensive understanding of IT risk characteristics and serve as a data-driven foundation for strategic decision-making.

The simulations were executed using the R programming language by processing thousands of random numbers according to predefined probability inputs. The risk modelling process involved iterative simulations to generate varying risk values that reflect multiple possible scenarios. The simulation outputs were subsequently visualized through data analysis techniques and graphical representations in R. Risk heatmaps display risk levels as combinations of probability and impact, while histograms depict the distribution of simulated losses (Liu, Xu, Zhou, & Fan, 2019).

Furthermore, the risk heatmap and other simulation outputs were visualized using a Shiny App, which provides an interactive and informative interface for presenting Monte Carlo Simulation results. The Shiny application allows users to adjust the number of iterations and select specific risk scenarios, generating outputs in the form of dynamic graphs and tables. Beyond serving as an analytical tool, the Shiny App functions as a visualization medium that facilitates a deeper understanding of the organization's risk profile.

The final stage involves analysing the simulation results in conjunction with the ISO 31000 framework to determine risk mitigation priorities based on urgency levels. Mitigation strategies are formulated as recommendations that organizations can adopt to reduce both the likelihood and impact of identified risks. Overall, this methodological process provides a comprehensive, objective, and quantitative assessment of IT risks, supporting managerial decision-making in accordance with international standards, particularly ISO 31000.

4. Results and Discussion

The IT division of PT XYZ focuses on the development of website application. The organization operates as a branch office in East Java which provides a wide range IT solutions to State-Owned Enterprises (BUMN). Risk management efforts discussed in this study is essential to support informed managerial decision-making.

Data preprocessing is conducted to ensure data quality and consistency prior to analysis using Monte Carlo Simulation and Shiny dashboard visualization. The process starts by collecting qualitative data and transforming those data into numerical data and normalization. Historical data and expert judgements from internal IT professionals were then used as the primary inputs for the Monte Carlo Simulation. Finally, the results were visualized to produce more measurable, realistic, and domain-relevant insights for IT risk management.

4.1. Risk Identification using ISO 31000

This process starts by identifying potential risks using assumption analysis method. This method identifies potential risks by assessing various assumptions from several risk categories, including nature, man, system, and infrastructure. This method organized potential risks and clustered them based on their category. In this study, we identify 18 potential risks, potential actions, and impacts that may occur if the risk appeared. Table 1 demonstrate the detail information of risk identification in this study.

4.2. Data Collection and Risk Simulation

Prior to conducting simulation modelling using the R programming language, a risk mapping process

Table 1
Risk identification.

ID	Risk	Event Description	Impact
R001	Flood	Work activities are disrupted	Facility damage and operational shutdown
R002	Earthquake	Damage to facilities and infrastructure	Operational disruption
R003	Lightning	Infrastructure damage	Power outage and system disturbance
R004	Fire	Infrastructure damage	Work activities halted
R005	Human error	Process errors occur	Project disruption
R006	Misuse of access rights	Unauthorized system access	Data interception or misuse
R007	Unintuitive user interface	Application usability issues	Users experience operational difficulties
R008	Data or device theft	Loss of data or devices	Operational and financial losses
R009	Cybercrime	Cyberattack incidents	Data leakage or database breach
R010	Hacking	System security breached	Operational disruption
R011	Web server failure	Server malfunction	Application inaccessible
R012	Network connection issues	Application access disrupted	Activity delays
R013	Hardware damage	Hardware reconfiguration required	Business activities disrupted
R014	Overheating	Hardware performance degradation	System performance issues and troubleshooting
R015	Power outage	Work processes interrupted	Project disruption
R016	Data corruption	Invalid or unusable data	Operational data cannot be used
R017	Server downtime	Application and database inaccessible	Business activities stopped
R018	Backup failure	Data not successfully backed up	Potential data loss

Table 2
Risk categories.

Risk Category	Probability	Impact Level	Mean Impact (IDR)	Distribution (Lognormal)
Low	0.05	Low	20 million	rlnorm(meanlog = log(20), sdlog = 0.5)
Medium	0.15	Medium	60 million	rlnorm(meanlog = log(60), sdlog = 0.6)
High	0.30	High	150 million	rlnorm(meanlog = log(150), sdlog = 0.7)
Severe	0.60	Severe	400 million	rlnorm(meanlog = log(400), sdlog = 0.8)

was performed based on the results of risk identification. As presented in Table 1, each risk is defined by its category, risk ID, likelihood, and impact, which serve as the initial inputs for the Monte Carlo Simulation implemented in R. Qualitative data presented in Table 2 were converted into quantitative values, including probability estimates and impact distributions, to enable simulation.

This study covers 18 identified risks across environmental, human, system, and infrastructure categories. Data integration for the R-based simulation involved parameterizing risk probabilities and estimating impacts. Qualitative likelihood assessments were converted into mean probability values (p_mean) ranging from 0.02 to 0.60, representing the likelihood of occurrence for each risk. Probability levels were defined as low (0.05), medium (0.15), and high (0.30).

Risk impacts were qualitatively classified into four levels and then converted into mean impact values expressed in million Indonesian Rupiah. A lognormal distribution was used to represent financial losses more realistically. The impact levels were defined as low (IDR 20 million), medium (IDR 60 million), high (IDR 150 million), and severe (IDR 400 million). This classification reflects the two fundamental dimensions of risk, namely likelihood and impact, which serve as the foundation for quantitative risk simulation and analysis.

4.3. Risk Modelling

After data mapping, a Monte Carlo Simulation model was developed to transform IT risk assessment into quantitative measures. The simulation was implemented using the R programming language and executed over 10,000 iterations for 18 identified risks to capture estimation uncertainty. Risk probabilities were used as input parameters, while risk impacts were modelled using a lognormal distribution. For each iteration, the potential loss was calculated as the product of probability and impact.

The simulation process in R began with loading the tidy verse, Shiny, and ggplot2 libraries for data transformation and visualization. Representative risks used to illustrate the model include R001 (flood risk)

Table 3
Risk conversion.

ID	Risk	Mean Probability	Symbol	Quantity	. Distribution (Gaussian and CGS–EMU Conversion to SI Units[a])
R001	Flood	0.05 (Low)	Beta(2.5, 47.5)	400 (Severe)	Lognormal(μ = 5.99, σ = 1.0)
R009	Cybercrime	0.15 (Medium)	Beta(7.5, 42.5)	150 (High)	Lognormal(μ = 5.01, σ = 0.8)
R017	Server Down	0.30 (High)	Beta(15, 35)	60 (Medium)	Lognormal(μ = 4.09, σ = 0.6)

Table 4
Iteration results.

ID	Likelihood	Impact	Loss
R006	Medium	High	22.5
R008	Medium	High	22.5
R009	Medium	High	22.5
R010	Medium	High	22.5
R016	Medium	High	22.5
R018	Medium	High	22.5
R005	High	Medium	18
R011	High	Medium	18
R012	High	Medium	18
R017	High	Medium	18
R013	Medium	Medium	9
R014	Medium	Medium	9
R002	Very Low	Severe	8
R001	Low	High	7.5
R004	Low	High	7.5
R015	Low	High	7.5
R007	Medium	Low	3
R003	Very Low	Low	0.4

Table 5
Top 5 results of the Monte Carlo method.

Risk	Probability	Expected Loss
Server downtime	0.15	41.31
Cybercrime	0.09	24.29
Hacking	0.10	21.72
Earthquake	0.03	17.99
Fire	0.06	16.53

with low probability and severe impact, R009 (cybercrime) with medium probability and high impact, and R017 (server downtime) with high probability and medium impact. Selected simulation outputs are presented in Table 3. The simulation was repeated across all iterations to observe the distribution of potential losses and assess overall risk exposure.

The selection of Beta and Lognormal distributions in the Monte Carlo Simulation is used to model appropriate probability risk likelihood, where the values are ranged between 0 and 1. This distribution is highly flexible and capable of representing various density of probability, including symmetric and skewed, through the parameter settings α (alpha) and β (beta), which were determined based on expert judgement and historical risk occurrence frequencies.

On the other hand, Lognormal distribution is utilized to model financial impact, as loss values are non-negative and likely exhibit right-skewed behaviour. This characteristic reflects real-world conditions in which most risks result in small to moderate losses, while a limited number of events may lead to extreme financial impacts.

The Monte Carlo Simulation was executed over 10,000 iterations to observe the distribution of potential losses. Simulation outputs for the 18 identified risks include likelihood, impact, and loss values, with selected results presented in Table 4.

Table 5 shows the top five risks, which exhibit the highest average probability, impact, and Expected Loss. The results were obtained from Monte Carlo Simulations implemented in the R programming language and executed over 10,000 iterations. In the simulation, risk probabilities were modelled using the Beta (α, β) distribution, while financial impacts were represented using the Lognormal (μ, σ) distribution.

This study employs several statistical indicators, including Expected Loss (EL), standard deviation

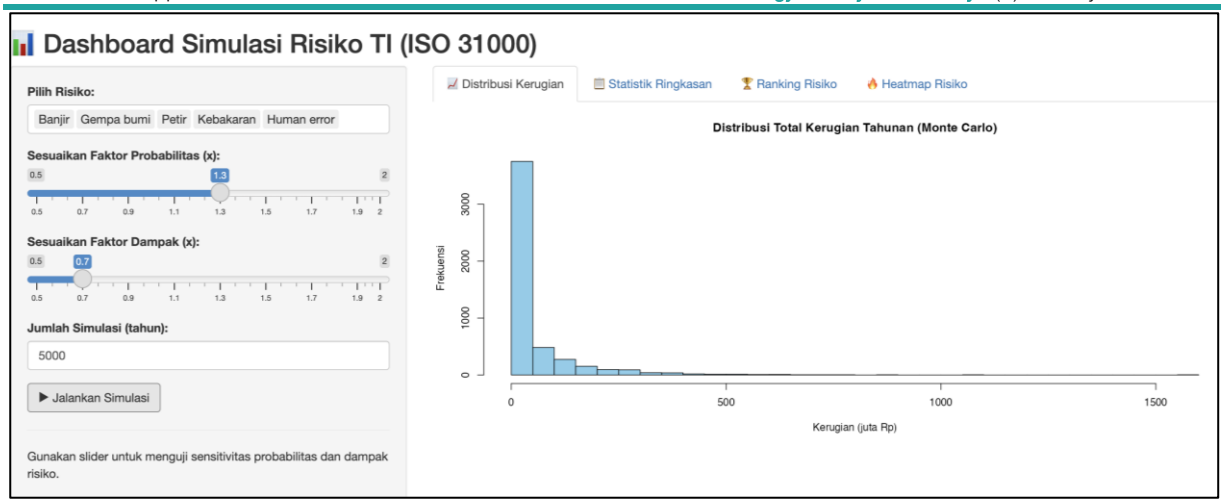


Fig. 3. Simulation dashboard.

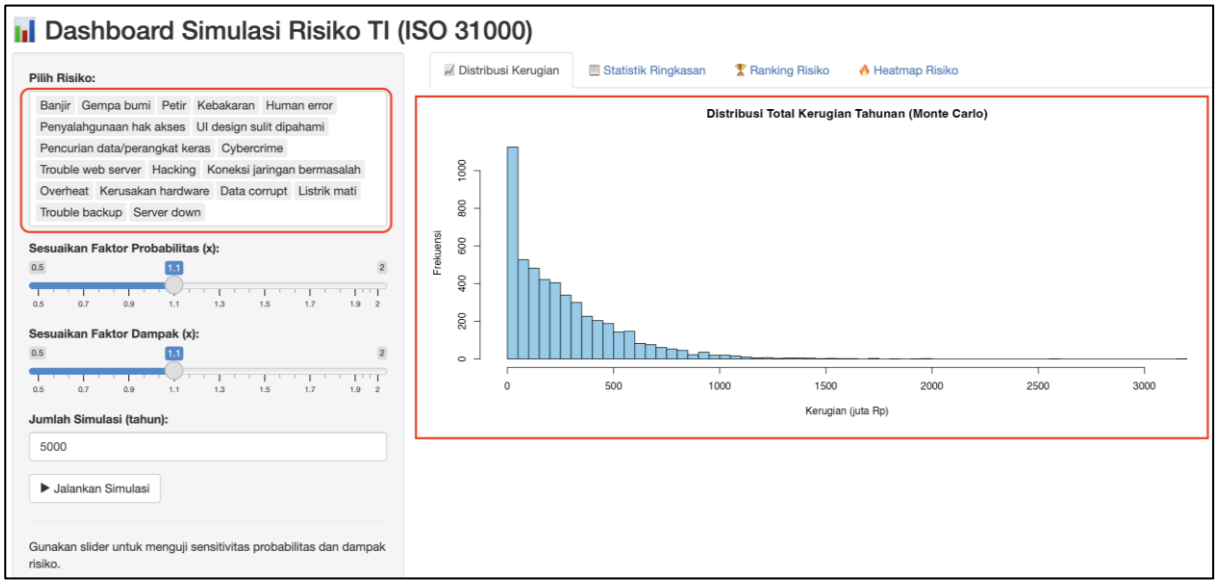


Fig. 4. Visualization of loss distribution.

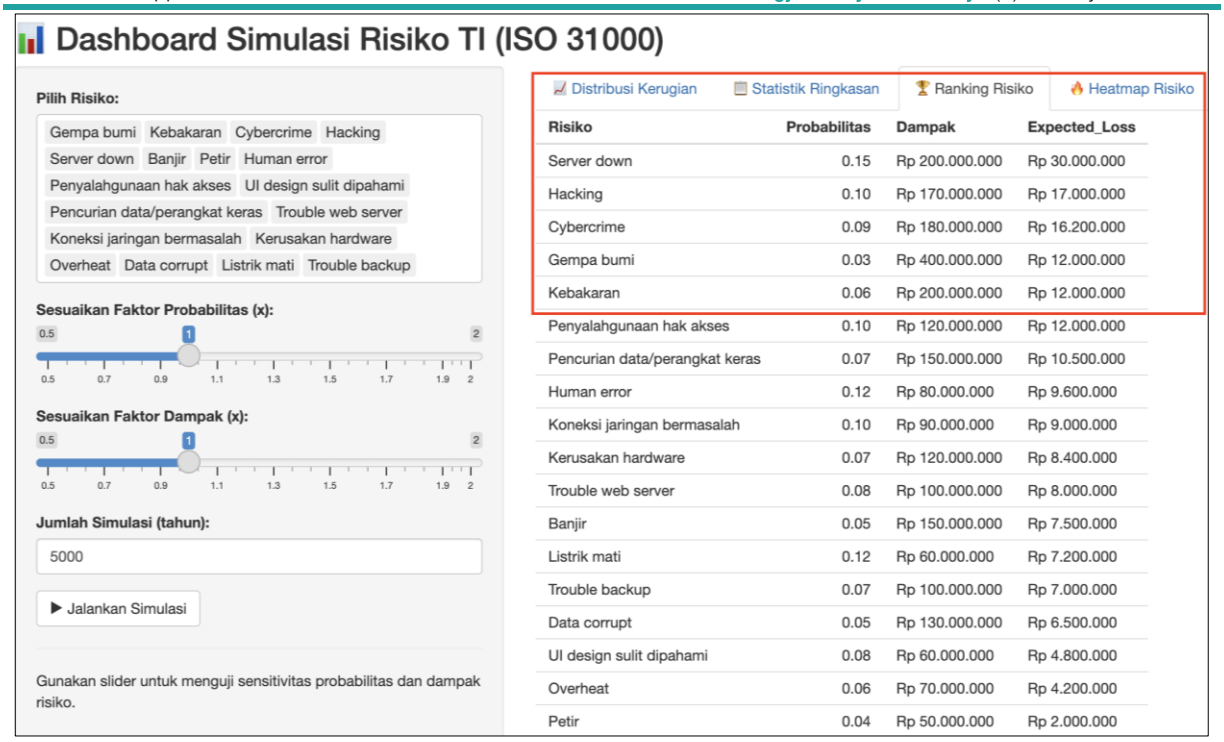
(σ), Percentile Risk (P90 and P95), Value at Risk (VaR), and Conditional Value at Risk (CVaR), to quantitatively measure, analyze, and interpret the outcomes of the risk simulations.

4.4. Risk Visualization

The risk visualization are presented through an interactive Shiny App dashboard developed using the R programming language. The dashboard enables real-time interaction, allowing users to execute simulations and immediately view visualization outputs without re-running the entire simulation process. As shown in Fig. 3, the Shiny App displays Monte Carlo–based risk simulation results aligned with the ISO 31000 framework, including a loss distribution histogram and a risk heatmap highlighting the highest-impact risks. Graphs and statistical indicators are dynamically updated in response to changes in simulation parameters, providing an interactive and responsive decision-support tool.

4.4.1. Results of Monte Carlo Simulation

The results of the Monte Carlo simulation method, referring to Algorithm 1, are illustrated in Fig. 4 in the form of a histogram visualizing the annual total loss (in million Indonesian Rupiah). The simulation was conducted using more than 10,000 Monte Carlo iterations to evaluate 18 identified risks at PT XYZ. After the simulation was executed, the histogram on the right-hand side presents the magnitude of potential losses expressed in million Rupiah. The observed pattern exhibits the characteristics of a right-skewed distribution, which is commonly found in information technology operational risks. Most losses are concentrated at a low to moderate level; however, these losses still indicate the potential for significant financial impact.



Risiko	Probabilitas	Dampak	Expected_Loss
Server down	0.15	Rp 200.000.000	Rp 30.000.000
Hacking	0.10	Rp 170.000.000	Rp 17.000.000
Cybercrime	0.09	Rp 180.000.000	Rp 16.200.000
Gempa bumi	0.03	Rp 400.000.000	Rp 12.000.000
Kebakaran	0.06	Rp 200.000.000	Rp 12.000.000
Penyalahgunaan hak akses	0.10	Rp 120.000.000	Rp 12.000.000
Pencurian data/perangkat keras	0.07	Rp 150.000.000	Rp 10.500.000
Human error	0.12	Rp 80.000.000	Rp 9.600.000
Koneksi jaringan bermasalah	0.10	Rp 90.000.000	Rp 9.000.000
Kerusakan hardware	0.07	Rp 120.000.000	Rp 8.400.000
Trouble web server	0.08	Rp 100.000.000	Rp 8.000.000
Banjir	0.05	Rp 150.000.000	Rp 7.500.000
Listrik mati	0.12	Rp 60.000.000	Rp 7.200.000
Trouble backup	0.07	Rp 100.000.000	Rp 7.000.000
Data corrupt	0.05	Rp 130.000.000	Rp 6.500.000
UI design sulit dipahami	0.08	Rp 60.000.000	Rp 4.800.000
Overheat	0.06	Rp 70.000.000	Rp 4.200.000
Petir	0.04	Rp 50.000.000	Rp 2.000.000

Fig. 5. Risk ranking visualization.

Fig. 6. Risk heatmap visualization.

4.4.2. Risk ranking

Fig. 5 displays the simulation results that obtained from the Monte Carlo simulation. These results are derived from probability and potential impacts of each identified risk. This approach is consistent with the ISO risk management framework for determining risk mitigation priorities.

4.4.3. Risk heatmap

A Shiny App was developed to visualize the identified risks at XYZ Company using heatmap and risk-

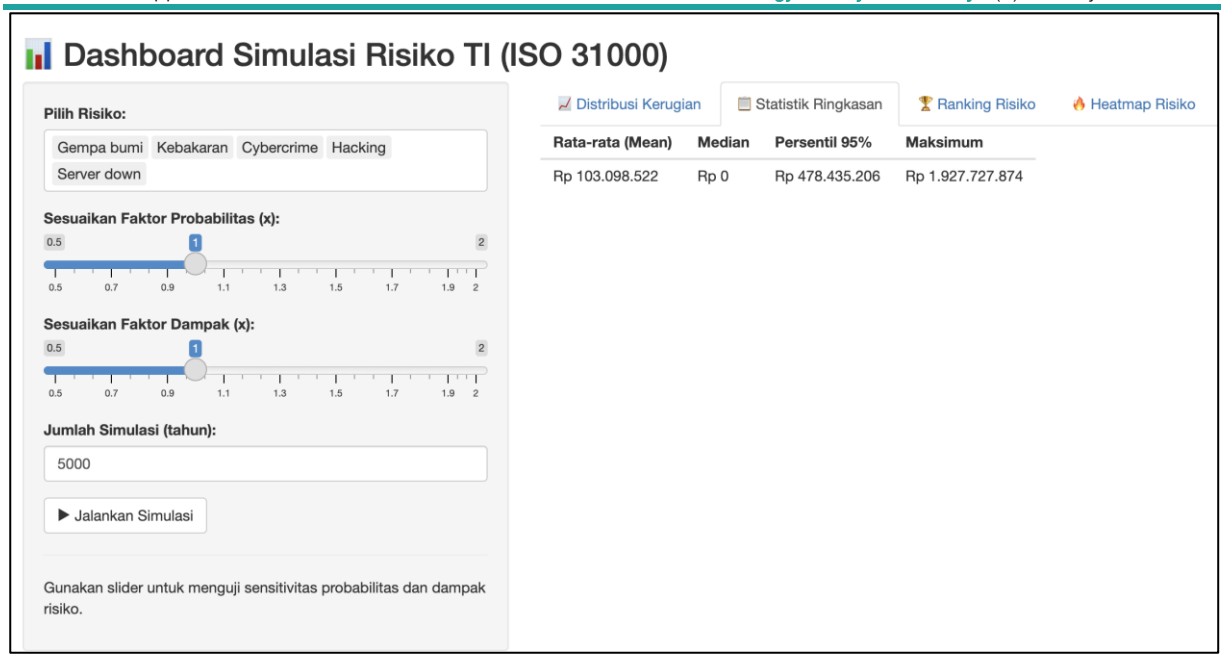


Fig. 7. Potential loss visualization.

Table 6
Risk mitigation recommendations.

ID	Risk	Probability	Expected Loss (Million IDR)	Suggested Mitigation Measures
R017	Server Down	0.15	41.31	Implement server redundancy, load balancing, daily automated backups, and a Disaster Recovery Plan (DRP) to ensure service availability.
R009	Cybercrime	0.09	24.29	Strengthen network security through multi-layer firewalls, Intrusion Detection Systems (IDS), and cybersecurity awareness training for staff.
R010	Hacking	0.10	21.72	Implement multi-factor authentication (MFA), patch management, and real-time security log monitoring.
R002	Earthquake	0.03	17.99	Establish a disaster recovery site in a separate location, utilize cloud-based backups, and obtain natural disaster risk insurance.
R004	Fire	0.06	16.53	Install automatic fire detection and suppression systems, use fire-resistant materials, and conduct trained emergency response procedures.

ranking representations based on their probability and expected loss values. Fig. 6 presents the interactive Shiny App dashboard, which displays the annual loss distribution generated using the Monte Carlo method and allows users to adjust probability levels, impact factors, and the number of simulation iterations to explore different risk scenarios. The dashboard also enables comparison of risks according to their probability and expected loss, thereby facilitating the identification of risks that require greater attention and supporting the development of appropriate risk treatment and mitigation strategies.

4.4.4. Financial impact

The Shiny App dashboard presents potential losses (in Indonesian Rupiah) and corresponding risk levels. Through its interactive features, users can perform sensitivity analysis and examine loss distributions for either the highest-ranked risks or all 18 identified risks, thereby enhancing understanding of the overall risk profile (Fig. 7).

4.4.5. The relevancy of ISO 31000

This study follows the ISO 31000 framework (Fig. 1), encompassing the stages of establishing the context through IT risk identification within the IT Division of PT XYZ to understand risks from both internal and external perspectives. The subsequent stages of risk analysis and risk evaluation are supported by simulation outputs while monitoring and review are facilitated through the Shiny App dashboard.

The final stage of the ISO 31000 framework, risk treatment, is conducted based on the analysis

results. From the simulation of 18 identified risks, this study prioritizes the five risks with the highest Expected Loss as the primary focus for risk control. Table 6 presents the recommended mitigation strategies for these prioritized risks.

The integration of ISO 31000 and Monte Carlo Simulation effectively supports data-driven decision making in risk management. Through this approach, PT XYZ can prioritize risk mitigation efforts based on the highest potential financial losses, enhance risk mitigation visually and reduce potential losses in a targeted and quantitative manner.

This study demonstrates that probabilistic analysis combined with interactive dashboards represents a more modern approach to IT risk management, aligned with the principles of the ISO 31000 framework. Moreover, the dynamic and value-oriented nature of ISO 31000 enables organizations to adapt risk management practices to evolving risk contexts, thereby strengthening strategic decision-making and organizational resilience.

5. Conclusions

The IT Division of PT XYZ currently lacks a structured and internationally standardized risk management approach. Existing mitigation practices are largely reactive and implemented only after incidents such as server disruptions or cyberattacks occur. There is no real-time risk monitoring system or early warning mechanism to anticipate potential losses.

This study enhances practical applications of ISO 31000 by integrating ISO 31000 with quantitative Monte Carlo Simulation to identify and analyse potential risk in an organization. The results were visualizes using Shiny Dashboard to provide risk evaluation, communication, and management. From a theoretical perspective, the study extends the application of ISO 31000 in IT risk management by incorporating modern computational simulation methods. Practically, it provides actionable guidance for IT management to implement interactive risk monitoring systems that support continuous evaluation, stakeholder communication, and data-driven decision-making. The findings also offer a foundation for developing continuous risk monitoring and early warning systems, thereby enhancing organizational resilience in a proactive and adaptive manner.

During the simulation, we successfully identified top five risks with the highest Expected Loss: server downtime, cybercrime, hacking, earthquakes, and fire. These findings provide an objective and quantitative basis for organizational decision-making in prioritizing risk mitigation strategies, as summarized in Table 5. The results indicate that infrastructure failures and cybersecurity risks pose the most significant threats to IT service continuity. This aligns closely with ISO 31000 principles, particularly in the risk assessment and risk evaluation stages.

The quantitative simulation outputs reveal both the loss distribution and the uncertainty level of risks, which are then used to guide the risk treatment process. High-risk scenarios such as server downtime and cybercrime highlight the need for enhanced cybersecurity controls, system redundancy, data backup strategies, and disaster recovery planning. External risks such as earthquakes and fire further emphasize the importance of structured emergency response plans.

Risk visualization through heatmaps and the Shiny App dashboard enables real-time decision-making, improves transparency, and enhances risk communication among stakeholders. This approach supports continuous monitoring and aligns with ISO 31000 principles across risk assessment, treatment, and monitoring stages. The Shiny-based visual outputs serve as a strategic tool for supporting data-driven risk management decisions.

This study is subject to several limitations. The analysis is based on data from a single division within PT XYZ, with a focus on internal and operational risks. The Monte Carlo Simulation relies on expert judgment and predefined assumptions, meaning the results may not be directly generalizable to other organizations. Additionally, simulation outcomes depend on initial parameter settings, including probability estimates and distribution assumptions (e.g., lognormal impact distribution). As the study is exploratory and simulation-based, empirical validation has not yet been conducted.

Future research may address these limitations by incorporating broader data sources, additional external risk variables, and improved simulation algorithms. Further integration with early warning systems and enterprise risk management (ERM) frameworks is also recommended to support predictive and sustainable IT risk management in dynamic organizational environments.

6. Declaration of AI and AI assisted technologies in the writing process

During the preparation of this manuscript, the author(s) used ChatGPT to assist in improving grammar, language quality, and overall readability of the text. After using this tool, the author(s) carefully

reviewed and edited the content as necessary and take full responsibility for the content of the publication.

7. CRediT Authorship Contribution Statement

Rahmania Kumalasari: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Project administration, Resources, Software, Validation, Visualization, Writing – original draft, and Writing – review & editing. **Lutfiyah Dwi Setia:** Conceptualization, Supervision, Validation, and Writing – review & editing. **Tri Septianto:** Formal Analysis, Funding acquisition, Investigation, Project administration, Resources, and Software.

8. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

9. References

Abdillah, L. A., Alwi, M. H., Simarmata, J., Bisyri, M., Nasrullah, N., Asmeati, A., . . . Bachtiar, E. (2020). *Aplikasi Teknologi Informasi: Konsep dan Penerapan.* Medan, Indonesia: Kita Menulis.

Anita, S. Y., Kustina, K. T., Wiratikusuma, Y., Sudirjo, F., Sari, D., Nurchayati, N., . . . Ayu, N. L. (2023). *Manajemen Risiko.* Padang, Indonesia: Global Eksekutif Teknologi.

Ariyandi, I. R., & Purwanti, P. (2025). Strategi Efektif Untuk Meningkatkan Efisiensi Operasional Perusahaan. *Journal of Business Economics and Management, 1*(3), 328-334. Retrieved January 20, 2026, from https://jurnal.globalscients.com/index.php/jbem/article/view/205

Glette-Iversen, I., Flage, R., & Aven, T. (2023). Extending and improving current frameworks for risk management and decision-making: A new approach for incorporating dynamic aspects of risk and uncertainty. *Safety Science, 168*. doi:https://doi.org/10.1016/j.ssci.2023.106317

Hojjati, S. N., & Noudehi, N. R. (2015). The use of Monte Carlo simulation in quantitative risk assessment of IT projects. *International Journal of Advanced Networking and Applications, 7*(1), 2616-2621. Retrieved January 21, 2026

Institute of Risk Management. (2018, February 15). *Standard Deviations – A Risk Practitioners Guide to ISO 31000 – 2018.* London, England: IRM. Retrieved January 20, 2025, from https://www.theirm.org/media/6884/irm-report-iso-31000-2018-v2.pdf

Jak, S., Jorgensen, T. D., Verdam, M. G., Oort, F. J., & Elffers, L. (2021). Analytical power calculations for structural equation modeling: A tutorial and Shiny app. *Behavior Research Methods, 53*, 1385–1406. doi:https://doi.org/10.3758/s13428-020-01479-0

Khedr, A., & Hilal, S. (2021). Interactive Visualization for Statistical Modelling through a Shiny App in R. *2021 International Conference on Data Analytics for Business and Industry (ICDABI).* Sakheer, Bahrain: IEEE. doi:https://doi.org/10.1109/ICDABI53623.2021.9655841

Kramarz, K., & Korpysa, J. (2023). The evolution of the concept of risk management in IT+ organizations. *Procedia Computer Science, 225*, 4843-4849. doi:https://doi.org/10.1016/j.procs.2023.10.484

Liu, D., Xu, Z., Zhou, Y., & Fan, C. (2019). Heat map visualisation of fire incidents based on transformed sigmoid risk model. *Fire Safety Journal, 109*. doi:https://doi.org/10.1016/j.firesaf.2019.102863

Miftakhatun, M. (2020). Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000. *Journal of Computer Science and Engineering (JCSE), 1*(2), 129-146. Retrieved January 21, 2026, from https://icsejournal.com/index.php/JCSE/article/view/76

Muryanti, E., & Hartomo, K. D. (2021). Analisis Risiko Teknologi Informasi Aplikasi CATTER PDAM Kota Salatiga Menggunakan ISO 31000. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 8*(3), 1265-1277. doi:https://doi.org/10.35957/jatisi.v8i3.948

Ningsih, S., & Arsal, A. (2022). Penerapan Simulasi Monte Carlo untuk Pengukuran Value at Risk (VaR). *Research in the Mathematical and Natural Sciences, 1*(2), 8–16. doi:https://doi.org/10.55657/rmns.v1i2.62

Orellano, M., & Gourc, D. (2025). What typology of risks and methods for risk management in innovation projects?: A systematic literature review. *International Journal of Innovation Studies, 9*(1), 1-15. doi:https://doi.org/10.1016/j.ijis.2024.10.001

Rhamadhani, M. H., & Iswari, L. (2022). Pengembangan Aplikasi Berbasis Web dengan R Shiny untuk Analisis Data Menggunakan Algoritma PCA. *Automata, 3*(1). Retrieved January 21, 2026, from https://journal.uii.ac.id/AUTOMATA/article/view/21870

Saputra, Y., & Hasanudin, A. I. (2025). The Role of ISO 31000 Risk Management in Moderating the Influence of the Management Control System and Leadership Style on Financial Performance at PT Angkasa Pura I and II (Persero) Period 2020-2023. *International Journal of Accounting, Management, Economics and Social Sciences, 3*(3), 840-853. doi:https://doi.org/10.61990/ijamesc.v3i3.510

Tanamaah, A. R., & Berliana, L. D. (2021). Information System Risk Management Analysis with ISO 31000 Method at the Industry and Manpower Office. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 8*(3), 1105-1118. doi:https://doi.org/10.35957/jatisi.v8i3.1037

Wibowo, A. (2022). *Manajemen Resiko.* Semarang, Indonesia: Prima Agus Teknik; Universitas Sains dan Teknologi Komputer.

Zagoto, S. P., & Sitokdana, M. N. (2021). Analisis Risiko Teknologi Informasi di Organisasi XYZ Cabang Salatiga Menggunakan ISO 31000. *Jurnal Mnemonic, 4*(1), 1-9. doi:https://doi.org/10.36040/mnemonic.v4i1.2877