Journal of Information Systems and Informatics
Vol. 6, No. 1, March 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i1.641 Published By DRPM-UBD

# SIOLGA Information Technology Risk Management Analysis Using ISO 31000

**Hizkia Brayn Minggos Mamuaja[1], Ariya Dwika Cahyono[2]**

[1,2]Information Systems, Faculty of Information Technology, Satya Wacana Christian University
[1,2]Diponegoro Street No. 52 – 60, Salatiga, Central Java, Indonesia 50711
Email: [1]682019@student.uksw.edu, [2]ariyadc@uksw.edu

**Abstract**

Salatiga City Disperinnaker, a government agency focusing on industry and labor, has developed the Salatiga Job Vacancy Information System (SIOLGA) to streamline its operations. As the SIOLGA application has recently completed its development phase, there arises a necessity for robust risk management to anticipate potential threats and vulnerabilities. Employing ISO 31000 standards, the research aims to mitigate risks effectively. The ISO 31000 framework encompasses risk identification, analysis, evaluation, and treatment phases. Through this process, the study identified 18 potential risks within the SIOLGA application, categorized into three levels: high, medium, and low. Specifically, there are 5 high-level risks, 10 medium-level risks, and 3 low-level risks. By implementing rigorous risk management strategies, the expectation is for the SIOLGA application to operate more efficiently and optimally, fulfilling its intended objectives.

**Keywords**: risk management, risk analysis, ISO 31000

## 1. INTRODUCTION

Disperinnaker, also known as the Salatiga City Industry and Manpower Service, is a pivotal government agency situated in Salatiga City, specifically located at Jalan Ki Pejawi No.12a, Sidorejo Lor, Sidorejo District, Salatiga City, Central Java Province [1]. At the core of its responsibilities lies the management of the Salatiga Job Vacancies Information System, known as SIOLGA. This web-based application is meticulously designed for easy accessibility via smartphones and laptops, offering comprehensive listings of job vacancies within Salatiga City.

Within its operational framework, SIOLGA engages various stakeholders. Firstly, companies post job vacancies for prospective employees. Secondly, job seekers, often referred to as "pencakers," navigate the platform to identify suitable job opportunities aligning with their individual criteria. Thirdly, Disperinnaker oversees the validation process for submitted job vacancies, ensuring the integrity of listings and guarding against fraudulent entries within the SIOLGA application.

Despite completing its developmental phase, SIOLGA necessitates robust risk management protocols to anticipate and mitigate potential threats. To this end, researchers have employed the ISO 31000 framework, endorsed by the International Organization for Standardization (ISO), to fortify risk management practices within companies, agencies, and organizations [2]. Distinguished by its comprehensive and conceptual approach, ISO 31000 aids in identifying forthcoming risks, enabling entities to devise bespoke strategies for risk mitigation and evaluation [3].

The research endeavors to identify conceivable risks inherent in the SIOLGA application. Following a comprehensive assessment of potential risks and their associated levels, the subsequent phases involve designing risk mitigation strategies and conducting thorough risk evaluations. Through meticulous risk management practices, the aim is to enhance the effectiveness and efficiency of the SIOLGA application, ensuring optimal functionality and reliability.

## 2. METHODS

The research uses qualitative methods. This research data was taken through an interview process and direct observation at the Salatiga City Manpower Department. The interview process is carried out from sources who have direct access rights regarding the SIOLGA application. The following are the activities in this research stage.

a) Literature study, looking for information related to risk management analysis using the ISO 31000 framework through journals, books and the internet.
b) Data collection and research regarding the SIOLGA application was carried out through an interview process with IT staff responsible for the SIOLGA application.
c) Conclusions and analysis results, contain conclusions related to the results of the risk analysis on SIOLGA and provide suggestions so that the application runs well and optimally.

Research methods serve as structured approaches for managing and organizing data and information, essential for subsequent processing and analysis. This research entails a two-stage process. Firstly, information will be gathered by conducting interviews directly with internal stakeholders at the Salatiga City Manpower Department. Subsequently, the collected data will be meticulously managed and organized before undergoing analysis, following the guidelines outlined in the ISO 31000 framework. This comprehensive approach ensures a systematic and thorough exploration of the problem at hand. The following are the stages of the process risk management:

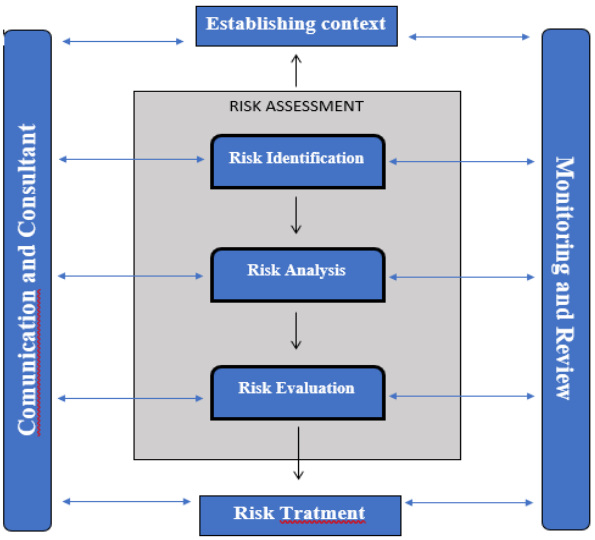


Figure 1. ISO 31000 Framework Principles

In research, communication and consultation are very important and crucial because the resource person will provide responses and risk assessments based on the source's opinion regarding a risk. In determining a context, there are 4 contexts that must be known first, namely the internal and external context, risk management context, and risk criteria [12]. This stage aims to understand the risks that will affect the company in achieving business goals [3].
Risk assessment includes:

a) At this stage the aim is to know, discover and recognize risks and be able to describe the information obtained through the interview process.
b) At this stage, an evaluation process is carried out in which risks are assessed that could hinder the company's vision and mission.
c) At this stage, an assessment of the potential risks can be seen based on the determined risk level.
d) This stage is the process of selecting and also implementing appropriate steps to reduce the impact of risks so as to minimize the possibility of risks occurring [5].

## 3. RESULTS AND DISCUSSION

### 3.1 Risk Assessment

The risk assessment stage has 3 main stages, the first is risk identification, the second is risk analysis, and the third is the risk evaluation stage.

p-ISSN: 2656-5935 http://journal-isi.org/index.php/isi e-ISSN: 2656-4882

### 3.1.1 Risk Identification Stage

The risk identification stage is required before risk management is carried out on the application. In this process, potential risks that will arise in the application can be seen. To see potential risks, asset identification is carried out in the SIOLGA application from these assets to see what risks will arise, so it is necessary to identify possible risks and risk impacts.

1) SIOLGA Asset Identification
In this risk identification stage, researchers conducted direct interviews with IT staff who manage and are responsible for the SIOLGA application regarding data, software and hardware requirements that are needed or used by the SIOLGA application as follows:

Table 1. Identification of SIOLGA Assets

| Information System Components | SIOLGA Assets (Salatiga Job Vacancies Information System) |
|---|---|
| Data | 1. Data of Job Seekers (Job Seekers) |
| | 2. Vacancies data from companies or agencies |
| Software | 1. SIOLGA web-based application |
| Hardware | 1. Application server, database, network and security |
| | 2. Personal Computer PC |

2) Identify Possible Risks and Risk Impacts
In the identification stage of possible risks, after interviews were conducted, 18 risks were found. This risk includes risks that have already occurred at SIOLGA and risks that have the potential to disrupt SIOLGA's activities. So researchers identified the impact of risks that would arise in the future. There are 3 risk impacts that arise, the first is natural factors, the second is human factors, then the third is infrastructure factors. So that the impacts that arise at this stage can be identified. The following are the results of the risk impact:

Table 2. Identification of Possible Risks and Risk Impacts

| Id | Possible Risks | Impact |
|---|---|---|
| R01 | Earthquake | There was damage to infrastructure which hampered agency activities. |
| R02 | Fire | Infrastructure damage occurs, and agencies experience financial losses. |
| R03 | Lightning strike | There was damage to infrastructure, especially servers, and the agency suffered financial losses. |
| R04 | Lack of quality human resources in system management | Experiencing difficulties in dividing existing job desks. |
| R05 | Lack of Quantity of Human Resources | The division of tasks to manage becomes ineffective and work piles up. |

| Id | Possible Risks | Impact |
|---|---|---|
| R06 | *Human error*/ Miss Coordination between employees | Business processes are disrupted because employees are negligent in updating and deleting data in applications. |
| R07 | Data theft is like hacking | Agencies will lose important data, and cause financial losses. |
| R08 | Abuse of access rights | User data will be intercepted and misused by irresponsible parties because some employees can log in to this application. |
| R09 | Theft of hardware in the Disperinnaker office | Causing financial losses and important data that was stored is also lost. |
| R10 | Cleaning or data cleansing | Resulting in a lot of junk data in the SIOLGA application. |
| R11 | Damage to hardware such as servers and PCs | The agency's business processes are disrupted, and financial losses result |
| R12 | Software failure | Business processes are disrupted and hamper SIOLGA application business processes. |
| R13 | The server or web server suddenly dies | *Server down*resulting in users not being able to access the application, server downs occurred as a result of a lightning strike so that the application business process stopped. |
| R14 | Power outage | Agency activities are disrupted. |
| R15 | Virus attack | The application process is disrupted and data loss can occur if it is not handled quickly. |
| R16 | Unscheduled application maintenance and data maintenance processes are rarely even carried out | If there is no application maintenance, at any time the SIOLGA data and application will crash, which will disrupt the application process. |
| R17 | *Overcapacity*data | The application will get stuck because there is not enough storage. |
| R18 | Not having an SOP in the Application business process | So, there are no clear and consistent guidelines so that employees work not in accordance with business processes because there are no clear work guidelines. |

### 3.1.2 Risk Analysis

Risk Analysis is a process that aims to assess possible risks that have been previously identified in table 2. In determining or managing risk management, 2 stages will be used in determining existing risk criteria. The first is the risk occurrence criteria within a certain period of time (likelihood) as seen in table 3, the second is the risk probability impact criterion (impact) as seen in table 4. Risks can be classified as low or high depending on the impact of each risk. which is there.

Table 3. Values for likelihood

| Likelihood | | Description | Frequency of Occurrence |
|---|---|---|---|
| Mark | Criteria | | |
| 1 | *Rare* | The risk almost never occurs | > 2 years |
| 2 | *Unlikely* | Risks are rare | 12 years old |

p-ISSN: 2656-5935 http://journal-isi.org/index.php/isi e-ISSN: 2656-4882

| Likelihood | | Description | Frequency of Occurrence |
|---|---|---|---|
| Mark | Criteria | | |
| 3 | *Possible* | Risks sometimes occur | 7 - 12 months |
| 4 | *Likely* | Risk is likely to occur (often) | 4 - 6 months |
| 5 | *Certain* | Risks almost always occur | 13 months |

In table 3 or the likelihood criteria table in this table there are 5 criteria based on how often the risk is likely to occur in a certain time period[13]. In determining the period, it can be seen from how many times the risk can occur in the SIOLGA application.

Table 4. Values on Impact

| Impact | | Description |
|---|---|---|
| Mark | Criteria | |
| 1 | *Insicnificant* | Does not interfere with agency business processes and activities |
| 2 | *Minor* | Activities are slightly hampered but main activities are not disrupted |
| 3 | *Moderate* | Hampering the agency's business processes so that some activities are disrupted |
| 4 | *Major* | Hampering the running of almost all agency business processes |
| 5 | *Catastrophic* | Hampering the agency's business processes as a whole and stopping agency activities completely |

After determining the likelihood value, the next step is determining the impact as shown in table 4. This impact determination aims to measure whether a possible risk has an impact which is divided into 5 criteria [14]. After determining the risk assessment by looking at the likelihood table and impact table for the SIOLGA application, risks will be visible and identified based on the risk levels that have been categorized.

### 3.1.3 Risk Evaluation

At this stage, researchers carry out identification and analysis according to the likelihood table and impact table that have been determined. The results of the analysis are then entered into the risk matrix evaluation table. The risk matrix is a table that will later group or categorize risks according to level. In this matrix table there are 3 levels of risk, the first is low, categorized at the lowest level, the second is medium, categorized at the middle level, and the third is high, categorized at the highest level in a risk evaluation matrix table. Determining the level of risk aims to find out what risks must be considered or handled first in the SIOLGA application.

Table 5. Risk Evaluation Matrix

| Impact | Likelihood | | | | |
|---|---|---|---|---|---|
| | Rare (1) | Unlikely (2) | Possible (3) | Likely (4) | Certain (5) |
| Insignificant (1) | | | R15 | | R01<br>R13 |
| Minors (2) | | | R08 | | R03 |

p-ISSN: 2656-5935 http://journal-isi.org/index.php/isi e-ISSN: 2656-4882

| Impact | Likelihood | | | | |
|---|---|---|---|---|---|
| | Rare (1) | Unlikely (2) | Possible (3) | Likely (4) | Certain (5) |
| | | | | | R14 |
| Moderate (3) | R02<br>R12 | R06 | R05<br>R07 | | R17<br>R18 |
| Majors (4) | R09 | R11 | | R16 | R10 |
| Catastrophic (5) | | | R04 | | |

Information

| | |
|---|---|
| Low | |
| Medium | |
| High | |

After all existing risks have been identified and entered into a risk evaluation matrix table adjusted for likelihood and impact. Of the 18 possible risks that exist, it can be seen which risks fall into the Low, Medium, High levels.

Table 6. Grouping of Possible Risks Based on Levels

| Id | Possible Risks | Likelihood | Impact | Risk Level |
|---|---|---|---|---|
| R10 | Cleaning or data cleansing | 5 | 4 | High |
| R17 | *Overcapacity*data | 5 | 3 | High |
| R18 | Not having an SOP in the Application business process | 5 | 3 | High |
| R16 | Unscheduled application maintenance and data maintenance processes are rarely even carried out | 4 | 4 | High |
| R04 | Lack of quality human resources in system management | 3 | 5 | High |
| R14 | Power outage | 5 | 2 | Medium |
| R06 | *Human error*/ Miss Coordination between employees | 5 | 2 | Medium |
| R03 | Lightning strike | 2 | 5 | Medium |
| R11 | Damage to hardware such as servers and PCs | 2 | 4 | Medium |
| R13 | The server or web server suddenly dies | 1 | 5 | Medium |
| R07 | Data theft is like hacking | 3 | 3 | Medium |
| R05 | Lack of Quantity of Human Resources | 3 | 3 | Medium |
| R08 | Abuse of access rights | 2 | 3 | Medium |
| R09 | Theft of hardware in the Disperinnaker office | 1 | 4 | Medium |
| R01 | Earthquake | 1 | 5 | Medium |
| R15 | Virus attack | 3 | 1 | Low |
| R02 | Fire | 1 | 3 | Low |
| R12 | Software failure | 1 | 3 | Low |

From Table 6, it can be seen that there are 5 possible risks with a High level as follows: RO10, RO17, RO18, R16, R04. At the Medium level risk level there are 10 possible risks as follows: RO14, RO6, RO3, R11, RO13, RO7, RO5, RO8, R09, R01. Meanwhile, for risks at the Low level, there are 3 possible risks as follows;

RO15, RO2, RO12. From the results of grouping 18 possible risks, the next stage will be to provide appropriate treatment to possible risks that arise so as to reduce the possibility of risks occurring.

### 3.2 Risk Treatment

After the risks are categorized and the possible risks are analyzed, it can be seen which risks have an impact that can disrupt the running of business processes in the SIOLGA application, resulting in the application not running optimally. In this stage the researcher will provide suggestions for treating risks and also the possible risks that exist in the SIOLGA application so that the possible risks that have been identified can be suppressed and minimized.

Table 7. Proposed Risk Treatment

| Id | Possible Risks | Risk Level | Risk Treatment |
|---|---|---|---|
| R10 | Cleaning or data cleansing | *High* | Controlling data by deleting data periodically so that nothing is duplicated. |
| R17 | *Overcapacity*data | *High* | Increase storage capacity and regularly delete non-important data. |
| R18 | Not having an SOP in the Application business process | *High* | Create clear SOPs related to application business processes so that you can know the right actions in implementing the application. |
| R16 | Unscheduled application maintenance and data maintenance processes are rarely even carried out | *High* | Determine the maintenance schedule according to the agency's needs and must be done so that you can find out what problems are occurring with the SIOLGA application. |
| R04 | Lack of quality human resources in system management | *High* | Provide training to existing employees and recruit employees who are experienced and competent. |
| R14 | Power outage | *Medium* | Plan and provide backup electrical power in the form of generators and remind employees to diligently back up data. |
| R06 | *Human error*/ miss coordination between employees | *Medium* | Providing firm action if irresponsible and a clear division of tasks between employees, it is necessary to evaluate work every week. |
| R03 | Lightning strike | *Medium* | Setting up a lightning rod in a place is important for the smooth running of the application. |

| Id | Possible Risks | Risk Level | Risk Treatment |
|---|---|---|---|
| R11 | Damage to hardware such as servers and PCs | *Medium* | Maintain and care for hardware. |
| R13 | The server or web server suddenly dies | *Medium* | Carry out routine checks on server security, so that the server does not die due to a lightning strike. |
| R07 | Data theft is like hacking | *Medium* | Install a firewall and check regularly. |
| R05 | Lack of quantity of human resources | *Medium* | Add or recruit more experienced and competent employees. |
| R08 | Abuse of access rights | *Medium* | Provide access restrictions for each user in the agency. |
| R09 | Theft of hardware in the Disperinnaker office | *Medium* | Equip the data storage area with CCTV and carry out nightly patrols in the area. |
| R01 | Earthquake | *Medium* | Have a place that is safe or a building that is specifically earthquake resistant. |
| R15 | Virus attack | *Low* | Provides anti-virus to protect important data. |
| R02 | Fire | *Low* | Provide automatic extinguishers in rooms that contain important company data. |
| R12 | Software failure | *Low* | Carry out routine checks on drivers or resources in the SIOLGA application. |

Of the 18 possible risks, researchers have offered recommendations and interventions for mitigating risks with the aim of not only suppressing them but also minimizing their potential impact. This research holds the promise of serving as a valuable blueprint for agencies tasked with navigating potential risks, offering nuanced strategies and insights that extend beyond mere hazard management into proactive risk mitigation and resilience-building measures.

## 4. CONCLUSION

Based on the results of research conducted at the Salatiga City Department of Industry and Manpower with the application object SIOLGA (Salatiga Job Vacancy Information System) which uses the ISO 31000 framework, after going through the risk management stages, namely risk assessment, risk identification, risk analysis and risk evaluation. So, 18 possible risks were found in the SIOLGA application. The risks are divided into 3 levels, namely low, medium and high levels. There are 5 possible risks with Level High, namely R10 (Cleaning or data cleansing), R17 (Data overcapacity), R18 (Not having SOPs in application business processes), R16 (Unscheduled and even rarely carried out application maintenance and data maintenance processes), and R04 (Lack of quality human resources in system management). At the Medium level there are 10 possible risks, namely R14

(Power outage), R06 (Human error / Miss Coordination between employees), R03 (Lightning strike), R11 (Hardware damage such as servers and PCs), R13 (Sudden server or web server death), R07 (Data theft such as hacking), R05 (Lack of Quantity of Human Resources), R08 (Abuse of access rights), R09 (Theft of hardware in the Manpower Department office), and R01 (Earthquake). Meanwhile, at the Low level there are 3 possible risks, namely R15 (Virus attack), R02 (Fire), and R12 (Software failure).

## REFERENCES

[1] A. R. Tanamaah and L. D. Berliana, "Risk Analysis Using the ISO 31000 Method at the Salatiga City Manpower Department in the Industrial Sector," *Journal of Informatics Engineering and Information Systems*, vol. 8, 2021.

[2] A. J. Prieto Ibáñez, J. M. Macías Bernal, M. J. Chávez de Diego, and F. J. Alejandre Sánchez, "Expert system for predicting buildings service life under ISO 31000 standard. Application in architectural heritage," *J Cult Herit*, vol. 18, pp. 209–218, 2016.

[3] E. Muryanti, and K. D. Hartomo, "Analisis Risiko Teknologi Informasi Aplikasi CATTER PDAM Kota Salatiga Menggunakan ISO 31000," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. *8* no. 3, pp. 1265-1277, 2021.

[4] E. Evinia and M. Sitokdana, "Risk Management Based IT Analysis Using ISO 31000 (Case Study: PT Bawen Mediatama)", *Journal of Information Systems and Informatics*, vol. 5, no. 1, pp. 380-390, Mar. 2023.

[5] M. I. Fachrezi, A. Dwika Cahyono, and P. F. Tanaem, "Information Technology Asset Security Risk Management Using ISO 31000:2018 Diskominfo Salatiga City," Department of Information Systems, vol. 8, 2021.

[6] R. H. Pangestu, A. Dwika Cahyono, and P. F. Tanaem, "Risk Management Analysis of SIPP Applications at the Salatiga Class 1B District Court Using ISO 31000," *Journal of Computer and Information Systems Ampera*, vol. 2, 2021.

[7] Y. Erlika et al., "Analysis of IT Risk Management at Bina Darma University Using ISO31000," 2020.

[8] U. Nugraha, "Design of information systems for population data collection based on client-server at Bagolo village," *in AIP Conference Proceedings*, vol. 1855, American Institute of Physics Inc., 2017.

[9] F. M. Hutabarat, and A. D. Manuputty, "Information Technology Risk Analysis of PT Visionet Data Internasional's VCare Application," *J. Computing*, vol. *2* no. 1, pp. 52-65, 2020.

[10] C. A. Mursid and W. Sutopo, "Risk Management in the Process of Selecting Vendors Using ISO 31000 and Financial Report Analysis: Case study," *IDEC National Seminar and Conference*, 2017.

[11] N. Putri and A. Wijaya, "Information Technology Risk Management in Educational Institutions Using ISO 31000 Framework", *Journal of Information Systems and Informatics*, vol. 5, no. 2, pp. 630-649, May 2023.
[12] F. L. Nice, "Information Technology Risk Analysis at the National Aeronautics and Space Agency (LAPAN) on the SWIFTS Website Using ISO 31000," *Juisi*, vol. 02, 2016.
[13] V. Putri and A. Wijaya, "Information Technology Risk Management Analysis Using ISO: 31000 at PT. XYZ", *Journal of Information Systems and Informatics*, vol. 4, no. 3, pp. 574-588, Sep. 2022.
[14] T. Rahardian and A. Wijaya, "Analisis Risiko Sistem Informasi Berbasis Web Pada Perusahaan CV. Mega Komputama Menggunakan ISO 31000", *Journal of Information Systems and Informatics,* vol. 4, no. 2, pp. 428-443, Jun. 2022.