# Information System Risk Assessment on Website Jogja Smart Service using ISO 31000

Herdian Aziz Qurnia Muharam
Department Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

## ABSTRACT

Aspects of life in the current era are greatly influenced by information technology. Among others, the Yogyakarta City Information and Coding Communication Service. The information system owned is a website that functions as an online city hall, the name of the website is Jogja Smart Service (JSS). Information technology cannot be separated from the possibility of a risk emerging in the future which could hamper the website. for example, server down and unstable internet. This research aims to determine the emergence of possibilities and prevention of risks on the Jogja Smart Service (JSS) website. This research uses the ISO 31000 method. An international standard that implements risk management. Risk assessment using ISO 31000 has 5 main stages, namely communication and consultation, establishing context, risk assessment (risk identification, risk analysis, risk evaluation), risk treatment and recording and reporting. This research produced 8 possible risks, of which 3 risks were at the low level, and 5 risks were at the medium level, but the risk treatment was different, namely 7 risks received reduction treatment, then 1 risk received transfer treatment. The results of the risk assessment evaluation that has been carried out can be used as a basis for handling and maintaining information technology and can reduce losses in terms of material or data in the future.

## General Terms

Risk Assessment

## Keywords

Jogja Smart Service, Risk, Risk Management, Risk Assessment, ISO 31000.

## 1. INTRODUCTION

Technology in the current era is developing very quickly [17]. Almost all organizations or agencies are technology literate [8], especially in the information technology section. Yogyakarta has the Yogyakarta City Communication, Informatics and Encryption Service which manages the organizational structure, position, duties, functions and work procedures. The Yogyakarta City Information Communication and Cryptography Department has information technology in the form of a website, namely Jogja Smart Service (JSS). Jogja Smart Service (JSS) is a virtual City Hall in order to provide direct services to the people of Yogyakarta city. According to an interview with the project manager (Candra), "Current conditions on the Jogja Smart Service (JSS) website have several problems, including users not being familiar with Jogja Smart Service (JSS), then there are system bugs that disrupt the website's business processes in the form of bugs when they want to scan. "KTP and also facial verification using a camera, then user traffic from this website increases and becomes denser, so it is possible that there will be a server down which will hamper or stop the performance of the website." When a website is not managed properly, it will have possible risks that can threaten the continuity of the website's performance or the business processes within it, so risk management analysis is needed [16].

## 2. LITERATURE STUDIES

### 2.1 Risk

Risk is an uncertainty and has a negative impact on an organization's goals that it wants to achieve [16]. This risk can be a challenge in itself that an organization must pay attention to. So uncertainty is a condition that causes risk to arise [4].

### 2.2 Risk Management

Risk management is a management effort carried out at the level of an executive leader. With the understanding that systematic discovery and analysis efforts are based on losses experienced by a company or organization, due to a risk and the methods used to respond to these losses which are related to the level of profitability of the company, agency or organization. [12].

### 2.3 Risk Assessment

Risk assessment is a process for evaluating a risk that has been identified. Risk assessment has several steps as follows [1]:

1. Identify the potential impact that is likely to occur on each risk that has been identified.
2. Determine the possible impact of the risk.
3. Determining the level of risk by controlling potential impacts and also the possibility of impacts occurring.
4. Determine the priority level of risk based on the level of risk and its potential impact.

### 2.4 ISO 31000

The International Organization for Standardization (ISO) 31000 is an international standard that implements risk management. ISO was first founded in London, England in 1946. ISO is a body or organization consisting of countries from all over the world to form standards which will later become a measure for a quality company. The aim of ISO 31000 itself is to create an international standard for implementing risk management that can be used by various types of organizations, from small to large scale, to deal with various kinds of risks related to organizational business processes. The principles of ISO 31000 aim to provide principles and guidelines that have a generic nature, which can be used by all types of companies, from small to large scale in an effort to deal with various kinds of risks that will arise in the future [ 11].

### 2.5 ISO 31000 Risk Management Process

ISO 31000 risk management has 6 main processes that are continuous with each other as shown in Figure 1 [11].

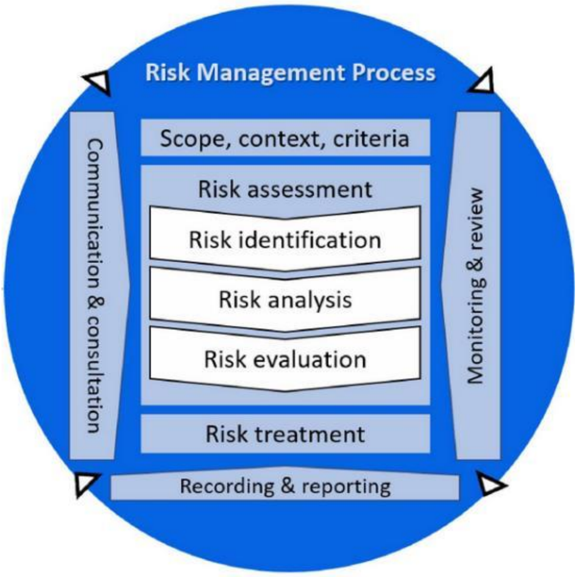

**Fig 1: ISO 31000 Risk Management Process**

1. Communication and consultation
   The aim of this process is to help stakeholders understand risk, so all decisions and actions should consider the risk aspects they will face [23].
2. Context, scope and criteria
   The purpose of this process is to manage the organization to determine external and internal context boundaries which will be taken into consideration in risk management and also to determine the scope of work and risk criteria for the process that will be carried out next.
3. Risk assessment
   Risk assessment has 3 stages, namely:
   a) Risk Indentify
      The process of identifying a risk that can affect the goals of the organization itself [23].
   b) Risk analysis
      Measuring the impact of risks and also their possibilities can be completed quantitatively, qualitatively or semi-quantitatively. This risk analysis produces input for the next process, namely risk evaluation and can also be used as a decision-making process regarding the treatment of a risk [11].
   c) Risk evaluation
      Comparing the results of the risk analysis process against the risks that have been determined, in order to determine whether these actions are necessary [11].
4. Risk Treatment
   Risk treatment is the process of modifying risks to overcome possible risks that will occur in the future. Risk treatment is categorized into 4, namely [23].:
   1. *Risk avoidance*
   2. *Mitigation*
   3. *Transfer*
   4. *Acceptance*
5. Monitoring and review
   The aim is to improve and ensure the effectiveness of design as well as the quality, results of the process and implementation.
6. Recording and reporting
   Aims to provide information for the decision making process and also increase the effectiveness of risk management. All activities in risk management can be documented by recording to become a basis for improving tools and methods and also improving all risk management processes.

# 3. METHODOLOGY

## 3.1 Research object

The subject of this study is the analysis of risk management on the Jogja Smart Service (JSS) website. The ISO 31000 framework will be used in this study. This risk management analysis is carried out on the Jogja Smart Service (JSS) website to determine the level of risk and provide recommendations on how to handle risks that may occur on the Jogja Smart Service (JSS) website.

## 3.2 Method of collecting data

This study uses a data collection method in accordance with the ISO 31000 risk management process. The data collection stage is carried out through observation, interviews and also filling out questionnaires to managers of the Jogja Smart Service (JSS) website.

1. Literature review
   At this stage of the literature study, a search is carried out regarding previous research journals and also books regarding methods and topics which will later be used as references and literature in this research. This stage is carried out to find reliable and appropriate sources to support the progress of the research.
2. Observation
   Observations will produce information which will later become material for further study in research. This stage also aims to increase understanding of the working system of the object being studied, then the researcher will adjust the problem and also the methods used.
3. Interview
   This stage aims to collect information from trusted sources and will understand the object deeply and accurately. Sources who support research related to information about the object of research are people who really understand the conditions and activities that occur with the object.
4. Linkert Scale
   The Linkert model will be used, with a number range from 1 to 5. The risk variables that have been created are then validated by the main informant by combining probability and consequence values to determine the level of risk which will be categorized at various levels to determine risk priorities.

# 4. RESULTS AND DISCUSSION

## 4.1 Risk Assessment

Risk assessment is a combination of three stages in accordance with the ISO 31000 assessment standard which can be seen in chapter 2, namely risk identification, risk analysis and finally risk evaluation. This risk assessment will determine the possibility of a risk occurring later by utilizing the insights and perspectives of stakeholders who provide information.

## 4.2 Identify Risks

Risk identification is extracting information about risks. The following are the results of risk identification that have been explored using brainstorming and interview methods in accordance with the ISO 31000 standard.

### 4.2.1 *Asset Identification*

Identification of these assets was carried out using the interview method with key informants. In the interview stage to identify assets, this is accompanied by filling in asset identification, questions are given on a sheet related to information technology, a checklist is made, and free discussion or brainstorming takes place. data consisting of data assets, software, hardware. The assets used to manage Jogja Smart Service can be seen in Table 1.

**Table 1: Ssset Identification on the JSS Website**

| Jogja Smart Service Asset Identification | |
|---|---|
| Data | Registrant data |
| Software | **WEB**<br>1. PHP / Laravel<br>2. JQuery<br>**WEB Server**<br>1. Nginx<br>**Back End**<br>1. JavaScript<br>2. Kong API Gateway<br>3. MySQL<br>**IDEA**<br>1. Visual Studio Code<br>2. Android Studio |
| Hardware | 1. PC<br>2. Laptops<br>3. Servers |

### 4.2.2 *Identify Possible Risks*

This stage will analyze possible risks that have been experienced by Jogja Smart Service and collect all risk information in the present or future with the aim of having a lot of information related to risk and can cover various sources rather than the risk itself. What if and check lists are used in gathering information. Risks are determined using a brainstorming approach and then every event that could give rise to undesirable consequences will be formulated. The results of possible risks come from extracting information from key informants and also interviews, which are then combined with the results of self-assessment which will enrich the results of possible risks. The results of the possible risks can be seen in Table 2.

**Table 2: Identification of Potential Risks on the JSS**

| Sources of Risk | Risk ID | Possible Risks |
|---|---|---|
| Nature and Environment | A.01 | Earthquake |
| Human | M.01 | Abuse of access rights or user ID |
| | M.02 | Human error |
| | M.03 | Cybercrime |
| | M.04 | Data leak |
| Systems and Infrastructure | SI.01 | System bugs |
| | SI.02 | Server down |
| | SI.03 | Data backup failure |

### 4.2.3 *Identify Risk Impact*

Impact identification will provide an overview of the impact that Jogja Smart Service will receive in accordance with the possible risks experienced. Based on the ISO 31000:2009 guideline, in the identification stage, tools are recommended in the form of brainstorming, strongly applicable brainstorming and interviews which will determine the potential risks that occur and later produce risk impacts that are in accordance with the risk identification. Identification of the impact of the risks obtained in the previous stages can be seen in Table 3.

**Table 3: Identification of Risk Impacts on JSS Website**

| Sources of Risk | Risk ID | Possible Risks | Impact |
|---|---|---|---|
| Nature and Environment | A.01 | Earthquake | Damage to infrastructure assets occurs and can hamper business processes. |
| Human | M.01 | Abuse of access rights or user ID | Data theft and company information being leaked and cyber threats will arise. |
| | M.02 | Human error | Disruption of business and operational processes. |
| | M.03 | Cybercrime | Data theft, use of data for illegal activities, company losses. operational disruption |
| | M.04 | Data leak | Reputation decreases, pay fines, Users start to lose trust, operasional distruption. |
| Systems and Infrastructure | SI.01 | System bugs | Security vulnerabilities , data loss, Reputation decline, SEO decline. |
| | SI.02 | Server down | Hackers can easily attack and disrupt websites, thereby disrupting existing business processes. |
| | SI.03 | Data backup failure | Data will be lost and cannot be recovered and result in loss to the Company. |

## 4.3 Risk Analysis

In the previous stage, we have obtained a context for designing Likehood and Impact which will then be included in the risk assessment questionnaire table. This risk analysis stage is carried out by taking a qualitative approach with key informants to obtain values or information from the level of risk that has been identified in the previous stage. Assessment indicators based on frequency of occurrence and their descriptions can be seen in Tables 4 and 5.

**Table 4: ISO 31000 Possible Value Criteria**

| Mark | Frequency | Description | Criteria |
|---|---|---|---|
| 1 | 1 time within one year | Very unlikely to happen | *Rare* |
| 2 | 1-2 times within a year | It's unlikely to happen | *Unlikely* |
| 3 | 3-4 times within a year | The chances of it happening and not happening are the same | *Possible* |
| 4 | 4-5 times within one year | It's very likely to happen | *Likely* |
| 5 | >5 times within one year | It's very likely to happen | *Certain* |

In Table 4, the likelihood value criteria based on the probability matrix explain a probability in qualitative form regarding the estimated frequency of risk events in a certain time period. Has a function to determine the level of risk can be determined through the numbers obtained from selected respondents. The magnitude of the risk impact is then formulated with risk appetite and provides a criterion for each impact. Then the impact value criteria can be seen in Table 5.

**Table 5: ISO 31000 Impact Value Criteria**

| Mark | Criteria | Impact |
|---|---|---|
| 1 | *Insignificant* | Has no impact on business processes |
| 2 | *Minor* | Has a small impact on not achieving a target |
| 3 | *Moderate* | The target delay is quite significant or large, and the performance achieved is below the target |
| 4 | *Major* | Target delays were very significant, and performance was achieved far below the target |
| 5 | *Catastrophic* | Failed to achieve targets and performance |

Table 5 contains the types of impacts that can be accepted by a risk that occurs and also the level of this impact which will be an indicator to measure the level of a risk. This impact assessment will be a reference material in research to determine a recommendation to be made.

When filling in the questionnaire containing all possible risk variables, it is validated by one main informant and one supporting informant in order to obtain the probability and impact values. To make it easier to fill in, the questionnaire was created using the Linkert method which contains several columns. The results of the stakeholder assessment using the Linkert questionnaire to assess possible risks and impacts. This assessment has been compiled and summarized in Tables 6 and 7.

## 4.4 Risk Evaluation

In making decisions in risk evaluation, this is obtained by ranking the risk results which are then entered into a consequence or probability matrix. The consequence and probability matrix table is an example of a qualitative assessment method that uses a numerical scale for assessment. In accordance with the consequence or probability matrix technique, this stage will rank the risk from the highest to the lowest level. The consequence or probability matrix will formulate a risk that is referred to using the Impact and Likehood criteria. The ranking results in the form of a consequence and probability matrix can be seen in Table 6.

**Table 6: Consequence or Probability Matrix Evaluation**

| | | | | | | |
|---|---|---|---|---|---|---|
| *Likehood* | 5 | Medium | | | | |
| | 4 | | | | | High |
| | 3 | Low | | | | |
| | 2 | | **M.02,**<br>**M.04** | **M.01,**<br>**M.03,**<br>**SI.01,**<br>**SI. 03** | | |
| | 1 | | | | | **A.01** |
| | **Impact** | 1 | 2 | 3 | 4 | 5 |

The results of the risk matrix evaluation are known, then the results are formulated which can be seen in Table 7.

**Table 7: Risk Level on JSS Website**

| ID | Possible Risks | Likehoo d | Impact | Level (Score) |
|---|---|---|---|---|
| A.01 | Earthquake | 1 | 5 | *Medium (5)* |
| M.01 | Abuse of access rights or user ID | 2 | 3 | *Medium (6)* |
| M.02 | Human error | 2 | 2 | *Low (4)* |
| M.03 | Cybercrime | 2 | 3 | *Medium (6)* |
| M.04 | Data leak | 2 | 2 | *Low (4)* |
| SI.01 | System bugs | 2 | 3 | *Medium (6)* |
| SI.02 | Server down | 1 | 3 | *Low (3)* |
| SI.03 | Data backup failure | 2 | 3 | *Medium (6)* |

Table 7 shows the results of the risk assessment by the informant which contains a risk level at a low level with a total of 3 possible risks and the remaining 5 possible risks are at a medium level, which indicates that there are several possible risks that could disrupt business process activities at Jogja Smart Service. Once the level of risk has been determined, recommendations for how to handle it will be made, as shown in Table 8.

**Table 8: Risk Treatment Mapping on JSS Website**

| | | | | | | |
|---|---|---|---|---|---|---|
| *Likehood* | 5 | | | | | |
| | 4 | Reduction | | Transfer | | Avoidance |
| | 3 | | | | | |
| | 2 | Retention | **M.02,**<br>**M.04** | **M.01,**<br>**M.03,**<br>**SI.01,**<br>**SI. 03** | | |
| | 1 | | | | | **A.01** |
| | **Impact** | 1 | 2 | 3 | 4 | 5 |

It can be seen in Table 8 which shows that there are 7 risks M.02, M.04, M.01, M.03, SI.01, SI. 02, SI.03 which is in the reduction category, carries out activities to increase the effectiveness of the management's risk control. There is 1 risk in the transfer category, namely A.01, where risk sharing will be carried out with other parties in order to reduce the impact experienced.

## 4.5 Risk Treatment

Provide recommendations on how to handle risks that are necessary and appropriate to minimize risks and also make improvements in accordance with the level of risk that has been obtained in the previous stage. Risk recommendations can be reviewed in Table 9.

**Table 9: Risk Treatment ISO 31000 on the JSS Website**

| ID | Risk | Risk Treatment | Score | Risk Treatment |
|---|---|---|---|---|
| A.01 | Earthquake | Transfer | Medium (5) | Providing backup hardware, servers and networks in different locations. |
| M.01 | Abuse of access rights or user ID | Reduction | Medium (6) | password and also username using a combination of letters, numbers and symbols. |
| M.02 | Human error | Reduction | Low (4) | Understand system handling and management according to SOP, and carry out regular evaluations |
| M.05 | Cybercrime | Reduction | Medium (6) | Protect data with "High Security Software" on the website |
| M.06 | Data leak | Reduction | Low (4) | Conduct data security training for all management staff. |
| SI.01 | System bugs | Reduction | Medium (6) | Report to the programmer when the latest version is released. |
| SI.04 | Server down | Reduction | Low (3) | Perform Load Balancing. |
| SI.05 | Data backup failure | Reduction | Medium (6) | Perform "Backup Verification". |

## 4.6 Monitoring and Review

In the process of monitoring a risk, it must be ensured that it goes through 3 stages, namely identification, evaluation and risk treatment. All activities or changes in this research can be identified through a risk list that has been validated by the management or related parties, as well as by carrying out communication and consultation.

## 4.7 Recording and Reporting

Recording and reporting in the risk management process can be adapted to an approach and report format that suits the organizational context.

# 5. CONCLUSION

Risk assessment was carried out on the Jogja Smart Service website using the ISO 31000 method. Identification, interview and brainstorming techniques were used for data collection and risk assessment, resulting in 8 possible risks in terms of nature and environment, humans and systems and infrastructure.

The results of the risk analysis which was carried out by calculating using the likelihood and impact matrix obtained 8 possible risks, of which 3 risks were at the low level, and 5 risks were at the medium level, but the risk treatment was different, namely 7 risk reduction treatments, then 1 risk received transfer treatment.

Then, the management of Jogja Smart Service (JSS) can use the risk assessment guide that has been prepared using ISO 31000 as a reference in managing risks that may later hinder the running of business processes or website systems.

# 6. REFERENCES

[1] A. Royyan. (2023). Konsep manajemen risiko. Jurnal Penelitian Ilmu Ekonomi Dan Keuangan Syariah (JUPIEKES), 1(3), 6–14.

[2] Butarbutar, N., & Tanaamah, A. R. (2021). Analisis Manajemen Risiko Menggunakan COBIT 5 Domain APO12 (Studi Kasus: Yayasan Bina Darma). Journal of Information Systems and Informatics, 3(3). http://journal-isi.org/index.php/isi

[3] Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. http://www.sei.cmu.edu/publications/pubweb.html

[4] Darmawi, H. (2022). Manajemen Risiko. PT Bumi Aksara.

[5] Fachrezi, M. I. (2021). Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000:2018 Diskominfo Kota Salatiga. JATISI (Jurnal Teknik Informatika Dan Sistem Informasi), 8(2), 764–773. https://doi.org/10.35957/jatisi.v8i2.789

[6] Henkens, B., Verleye, K., & Larivière, B. (2021). The smarter, the better?! Customer well-being, engagement, and perceptions in smart service systems. International Journal of Research in Marketing, 38(2), 425–447. https://doi.org/10.1016/j.ijresmar.2020.09.006

[7] Jantce TJ Sitinjak, D. D., Maman, ., & Suwita, J. (2020). Analisa Dan Perancangan Sistem Informasi Administrasi Kursus Bahasa Inggris Pada Intensive English Course Di Ciledug Tangerang. Insan Pembangunan Sistem Informasi Dan Komputer (IPSIKOM), 8(1). https://doi.org/10.58217/ipsikom.v8i1.164

[8] Junianti, D., & Fibriani, C. (2021). Analisis Resiko Aplikasi Sistem Informasi Pengelolaan Data Umat Menggunakan ISO 31000 (Studi Kasus: Gereja Katolik Santo Paulus Miki Salatiga). In Journal of Computer and Information Systems Ampera (Vol. 2, Issue 2). https://journal-computing.org/index.php/journal-cisa/index

[9] Kashef, M., Visvizi, A., & Troisi, O. (2021). Smart city as a smart service system: Human-computer interaction and smart city surveillance systems. Computers in

Human Behavior, 124(May), 106923. https://doi.org/10.1016/j.chb.2021.106923

[10] Kasidi. (2010). Manajemen Risiko. Ghalia Indonesia.

[11] Leo, J, S., & Kaho, R. (2018). Manajemen Risiko berbasis ISO 31000: 2018 Panduan untuk Risk Leader dan Risk Practitioner.

[12] Linda Lole, K. M., & Maria, E. (2022). Analisis Manajemen Risiko Pada Aplikasi Pegadaian Digital Service Menu Tabungan Emas Menggunakan ISO 31000:2018. https://doi.org/10.30865/json.v3i3.3891

[13] Liperda, RI, & Ayu Septia Nieng, U. (2023). Analisis Manajemen Risiko Pada Aplikasi Pegadaian Digital Service Menu Tabungan Emas Menggunakan ISO 31000. INFOTECH Journal, 9(2), 361–370. https://doi.org/10.31949/infotech.v9i2.6232

[14] Maydianto, & Ridho, M. R. (2021). Rancang Bangun Sistem Informasi Point of Sale Dengan Framework Codeigniter Pada Cv Powershop. Jurnal Comasie, 02, 50–59.

[15] Pamungkas, G., Bagas, M., & Atmojo, T. (2021). Analisis Manajemen Risiko Teknologi Informasi pada Website UMKM XYZ berdasarkan Framework ISO 31000. 4(1), 12–17.

[16] Pebriani, O. D., Zulfikar, D. H., Kom, S., Cs, M., Islam, U., Raden, N., & Palembang, F. (n.d.). SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Website SIMPEG di Kantor Kementerian Agama Kota Palembang. https://doi.org/10.31284/p.snestik.2022.2716

[17] Putri, A. A., & Irnanda, D. I. (n.d.). Volume 4 issue 1 1 Aisyah Journal of Informatics and Electrical Engineering Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi Kasus : Aplikasi J&T Express Indonesia). http://jti.aisyahuniversity.ac.id/index.php/AJIEE

[18] S. Hardianti, I. Riadi (2022) Service Risk Assessment Learning Management System using ISO 31000:2018/31010. https://doi.org/10.5120/ijca2022921993

[19] Sabir Muh. (2023). Manajemen Risiko. CV. Intelektual Manifes Media.

[20] Sitorus, J. H. P., & Sakban, M. (2021). Perancangan Sistem Informasi Penjualan Berbasis Web Pada Toko Mandiri 88 Pematangsiantar. Jurnal Bisantara Informatika (JBI), 5(2), 1–13.

[21] Sukoco, S., & Azmi, F. (2022). Komponen-Komponen Manajemen Resiko Dalam Aplikasi Resiko Kredit (Pembiyaan) Di Bank Syariah Indonesia Unit Pandan Tapanuli Tengah. Warta Dharmawangsa, 16(3), 522–530. https://doi.org/10.46576/wdw.v16i3.2244

[22] Theodoridis, T., & Kraemer, J. (n.d.). Konsep Dasar Sistem Inromasi. 1–9.

[23] Vorst, C. R., Proyarsono, D. S., & Budiman, A. (2018). Manajemen Risiko Berbasis SNI ISO 31000. Badan Standarisasi Nasional.

[24] Yoewono, J. O., & Prasetyo, A. H. (2022). Rancangan Dan Proses Manajemen Risiko Pada Pt Surya Selaras Cita. Jurnal Muara Ilmu Ekonomi Dan Bisnis, 6(1), 56. https://doi.org/10.24912/jmieb.v6i1.12207

[25] A. Nuriyanti, I. Riadi (2023) Risk Assesment Analysis on Bumil-KU Application using COBIT 5 Framework. https://doi.org/10.5120/ijca2023923310

[26] N Kartika, I. Riadi (2023) Analysis of Risk Management on DAPODIK System Services using OCTAVE Allegro Framework. https://doi.org/10.5120/ijca2023922759

[27] A. Rghioui, A. Khannous, S. Bouchkaren et al. (2014) 6lo Technology for Smart Cities Development: Security Case Study. https://doi.org/10.5120/16089-5402

[28] T. Setianingrum, D. Putri, I. Riadi (2022) Analysis of Risk Management on Learning Management System using Octave Allegro Framework