Analysis Of Information Technology Risk Management In Raja Computer Balikpapan Branch Using ISO 31000 Framework

Ayu Sri Wahyuni¹, Darlinda², Joy Nashar Utamajaya³

¹,²,³Sistem Informasi, STMIK Borneo Internasional Balikpapan
Jl. AW. Syahranie No.04, RT.32, Batu Ampar, Kec.Balikpapan Utara,Kota Balikpapan, Kalimantan Timur 26136
Email: ¹ayu_sri_wahyuni.18@stmik-borneo.ac.id, ²darlinda.18@stmik-borneo.ac.id, ³joy.nashar@stmik-borneo.ac.id

Abstrak. Raja Computer Cabang Balikpapan merupakan toko yang bergerak dibidang penjualan komputer, toko tersebut sudah menggunakan SI/TI dalam menunjang setiap kegiatan usaha yang dijalankannya. Toko menggunakan aplikasi Ipost yang digunakan untuk mendukung penjualan komputer, pencatatan stok barang, dan dapat digunakan untuk mencatat kontes harian yang dibutuhkan toko. Namun dalam dunia manajemen selalu ada kemungkinan risiko yang mungkin terjadi dan dapat mengganggu aktivitas bisnis dalam menggunakan sistem tersebut. Oleh karena itu, diperlukan suatu analisis terhadap suatu aplikasi Ipost yang terdapat pada toko komputer tersebut. Oleh karena itu, diharapkan dengan menggunakan ISO 31000 dapat membantu meminimalisasi setiap risiko yang terdapat pada aplikasi Ipost. Hasil analisis risiko ini berupa analisis risiko yang mungkin terjadi, dapat mengelompokkan kemungkinan risiko berdasarkan aplikasi yang dapat menghasilkan penawaran dan risiko yang ada di Ipost, sehingga toko komputer dapat menangani risiko yang ada sesuai dengan tingkat prioritas risiko, serta mampu mencegah dan meminimalisir gangguan kegiatan usaha di toko Raja Computer cabang Balikpapan.

Kata Kunci: ISO 31000, Analisis Risiko, Dan Manajemen Risiko

Abstract. Raja Computer Balikpapan Branch is a store that is engaged in selling computers, the store already uses IS/IT in supporting every business activity it carries out. The store uses the Ipost application which is used to support computer sales, record stock of goods, and can be used to record daily contests needed by the store. However, in the world of management, there is always the possibility of risks that may occur and can interfere with business activities in using the system. Thus, an analysis is needed of the IS/IT resources contained in the computer shop. Therefore, it is hoped that using ISO 31000 can help minimize every risk contained in the Ipost application. The results of this risk analysis are in the form of an analysis of possible risks, can group possible risks based on applications that can generate offers and risks that exist in Ipost, so the computer shop can treat existing risks according to the priority level of risk and be able to prevent and minimize disrupting business activities at Raja Computer store Balikpapan branch.

Keywords: ISO 31000, Risk Analysis, And Risk Management

1. Preliminary

The development of technology today is very fast and rapid so that technology becomes a very intimate need in everyday life, especially in the business world. Technology has a very important role for the progress of an organization or company to be able to compete with its competitors, even more so by optimizing the utilization of good IS/IT management for the organization or company will make an organization or company more effective and efficient in carrying out every business process. that exist within an organization or company [1].

Not a few organizations or companies are willing to spend a very large amount of money to invest in the information system. For successful companies, they must realize the importance of the benefits of IS/IT and use IS/IT to drive stakeholder values, as well as realize and perform risk management on the risks associated with planning and IS implementation [2].

Management of IS/IT in a company is indeed important as well as Raja Computer Store Balikpapan Branch, a Computer Store that has optimized IS/IT management in every company management activity, this
can be proven by the Ipost Application. However, it is undeniable that even though the management of IS/IT at the Raja Computer Store is optimal, it certainly has several possible threats and risks and can interfere with running business process activities, especially those that can still be seen visually clearly, there are several risks at the Raja Computer Store Balikpapan branch that have not yet been completed. Get risk treatment such as Human Error, Overheat, and Server Down so that risk management analysis and evaluation is needed for the Raja Computer Store Balikpapan branch by identifying every possible risk that exists as well as potential risks that will come, this risk management action has been regulated in ISO 31000:2018 about risk management. Risk Management is a management effort that aims to control the risk of the company's operational activities by conducting risk analysis, evaluation and mitigation [3].

In this case, the information technology risk analysis uses the Ipost application at the Raja Computer Store Balikpapan branch by applying the ISO 31000:2018 method approach. In February 2018, the National Standards Organization (ISO) introduced ISO 31000:2018 to the public. This ISO contains Risk Management Standards. With the issuance of the latest version of ISO 31000, it is hoped that it will replace the many different standards currently used by many companies. ISO 31000:2018 is a standard guide, instructions, and demands for an organization or company to build a foundation and framework for a risk management program [4]. The foundation includes the rules, objectives, and commitments to build a comprehensive risk management program. The framework includes planning, accountability of employees, processes and activities used to manage risks in the company's performance. To manage risk at the Surabaya branch of the Surakarta Store, a risk assessment is required which is regulated in ISO 31000:2018. Risk analysis using ISO 31000:2018 can be seen as risk value or risk value with three levels, namely risk with low, medium, and high levels [5].

By using the ISO 31000:2018 method where the standard of this method has a broader view and can be applied in various organizational scopes and is more conceptual than other standards[6]. The focus of this research method is to identify several information technology assets at the Raja Computer Store Balikpapan branch and identify every possible risk that will occur, how much impact the risk will have, and be able to provide recommendations to the Raja Computer Store Balikpapan branch on the risks involved. Future risks and risks that may arise at any time. That way the performance of IS/IT activities and business processes at the Raja Computer Store Balikpapan branch can be optimized by the organization and company. In the world of Management, every thing that is carried out in an organization or company must always be accompanied by threats and risks. Risk always overshadows every activity undertaken to prevent an organization or company from achieving their goals as well as their vision and mission, therefore a risk control is needed to be able to help an organization or company to handle any existing risks and be able to realize the goals of the organization or company.

Previous research that also discussed ISO 31000 was conducted by Andi Novia Rilyani with the title "Risk Analysis of Information Technology Based on Risk Management Using ISO 31000" in 2015. This research focuses on i-Gracias (Integrated Academic Information System), which is an application that is accessed by lecturers, students, and staff at Telkom University. This study discusses risk analysis regarding assets related to the i-Gracias system in terms of technology and infrastructure. In this study, the results show that the risk that has the highest risk value is the database crash. Meanwhile, those in the medium risk quadrant have 30 risks and those in the low risk quadrant have 12 risks. Risk management is focused on assets that have high risk by identifying the causes and finding the right solution [7].

Another research related to ISO 31000 was written by Francisca Lady Nice with the title "Information Technology Risk Analysis at the National Aeronautics and Space Institute (LAPAN) on the SWIFTS website using ISO 31000” in 2016. This research focuses on the SWIFTS website. From this research, the results of the risk level that have a high probability and impact value are assets, both software data, hardware, human resources and procedures related to the SWIFTS system which are considered to be able to interfere with the LAPAN business process itself. So a review is needed by the head of the LAPAN IT Division and the application of the recommended risk treatment [8]. In 2017, Stefan Agustinus also conducted a research entitled "Information Technology Risk Analysis in the HRMS programal. The research discusses the risk assessment of the assets around the company. In this study, it was found 2 possible risks having a high level of risk and 18 possible risks with a medium level that could interfere with the company's performance. With the risk assessment, it is expected to be able to minimize losses experienced by the company. From the three studies above, both of them use ISO 31000, but they are still guided by ISO 31000:2009, where in February
2018, the ISO international standards organization issued ISO 31000:2018 Risk management — Guidelines. This standard replaces ISO 31000:2009 Risk management — Principles and guidelines published in November 2009. This revision is part of a systematic review process that applies to all ISO standards. This paper briefly reviews the changes that the 2018 version of ISO 31000 has made to the 2009 version.

2. Research Method

Research at Store Raja Computer Balikpapan branch is about risk management using ISO 31000:2018 framework. Where ISO 31000:2018 has internationally recognized principles and guidelines for risk management. Risk Management is the process of identifying risks, analyzing and evaluating risks which is able to form a strategy to manage risk in the Ipost application in the Raja Computer Store Balikpapan branch. ISO 31000 is a risk implementation guide consisting of three elements: principle, framework, and process. The principle of risk management is the basis of risk management practice or philosophy. The framework is the structured and systematic management of risk management systems throughout the organization. Processes are sequential and interconnected risk management activities. In general, ISO 31000:2018 simplifies the 2009 version. It was immediately seen among others d.

Figure 1. Differences ISO 31000:2009 ISO 31000:2008

In this study, researchers used case study research method with qualitative approach. This approach is done by describing or deciphering the data and facts that occur in the object of the case study into the form of words. One type of qualitative approach is the Case Study Research research method, where this method focuses only on one particular object, with this method researchers will easily obtain the data needed to solve problems that occur in case study objects. In this Case Study Research method is done with several stages where these stages are in accordance with the risk management of the ISO 31000:2018 framework. Where to do this research in finding all the information needed to support research on Ipost application in Store Raja Computer Balikpapan branch. The data obtained is primary data obtained.

3. Data Retrieval

Method Data retrieval method is a technique used by researchers for data collection to obtain all information used by researchers as research materials to achieve research objectives. In this study, researchers took data by interviewing internal speakers from Toko Raja Computer Balikpapan branch, which is one of the company's stakeholders who are the internal source of this study.

Figure 2. Data Analysis Methods
In figure 2 describes the methods used by researchers in analyzing data, the stages that start from Risk Assessment to Risk Treatment, with the ways used for the research to run well, among others, taking into account the scope, context, and criteria of risk, then conducting consultations and communication with related parties, then looking at the track record of sera reporting. And lastly do monitoring and review. As in figure 1, the first stage is Risk Assessment. Risk assessment is a systematic method in determining whether in the application of Ipost in Toko Raja Computer Balikpapan branch has an acceptable risk or not. In this Risk Assessment consists of several stages. Risk Identification is an effort to find and know the risks that have the possibility to appear in activities carried out by the company. Risk Analyst In this method of risk analysis includes assessment, characterization, management and policy related to risk in the company. Risk Evaluation This risk evaluation is a process to compare between the lowest risk levels to the highest risks found during the analysis process. In this evaluation aims to help the risk-taking process based on the results of risk analysis. In the next stage, Risk Treatment in this stage involves choosing one or more options to overcome risks and implement risk management. Once implemented, risk management can be done or modified in risk management control [13].

3. Results And Discussion

Risk Assessment

At this stage is the risk assessment stage at Toko Raja Computer Balikpapan branch. In the risk assessment process, Ipost application consists of 3 stages, namely: Risk identification, risk analysis, risk evaluation.

Asset Identification

Risk Identification In the first phase, identification of assets related to Ipost applications such as data assets, software assets, and hardware assets is carried out. And in this identification interview The King Computer Shop Owner and IT Staff or the part that manages the Ipost system. At this stage it focuses on its data assets, software and hardware.

Table 1. Asset Identification

| Information System Components | Assets                        |
|-------------------------------|------------------------------|
| DATA                          | Goods data, supplier data, employee data |
| SOFTWARE                      | Aplikasi Ipost                |
| HARDWARE                      | Personal computer, database server |

Table 1 shows the assets of information system components in the form of data, software, and hardware that support the development of Ipos applications. Identify Possible Risks After identifying assets that generate information from data, software, and hardware related to Ipost applications. Furthermore, it is necessary to identify possible risks that could be a threat to the Ipost application. Possible risks can be grouped based on 3 factors, namely; natural/environmental factors, human factors and system and infrastructure factors. What can be seen in table 2. below.

Table 2. Identification of Possible Risks

| Factor | ID    | Possible Risks                       |
|--------|-------|--------------------------------------|
| Nature | R001  | Flood R002                           |
|        | R003  | Fire                                 |
|        | R004  | Lightning                            |
|        | R005  | Human Error                          |
|        | R006  | Misuse of Access Rights              |
|        | R007  | Theft and Data Leakage               |
|        | R008  | Hardware Theft                       |
|        | R009  | Hacking                              |
From the risk identification stage, there are 20 possibilities - possible risks derived from these three factors, namely: nature / environment, human, system and infrastructure. Identification of Possible Risk Impacts After knowing the identification of possible risks, at a later stage identify the impact of the risks of the possibilities - possible risks that exist. Can be seen in table 3.

| Table 3. Identify Possible Risks |
|----------------------------------|
| **Factor** | **ID** | **Possible Risks** | **Impact** |
| Nature     | R001  | Flood             | Kerusakan pada infrastruktur dan mengganggu jalannya proses bisnis |
|            | R002  | Earthquake        | Mengganggu jalannya proses bisnis |
|            | R003  | Fire              | Kerusakan pada infrastruktur dan mengganggu jalannya proses bisnis |
|            | R004  | Lightning         | Kerusakan pada infrastruktur |
| Human      | R005  | Human Error       | Inputted data does not match |
|            | R006  | Misuse of Access Rights | User permissions can be abused |
|            | R007  | Theft and data leakage | Data may be misused by others |
|            | R008  | Theft Hardware    | Financial losses |
|            | R009  | Hacking           | The system can be intercepted and disrupted |
|            | R010  | Elusive User Interface | Users may have difficulty Understanding and running sistem |
|            | R011  | Vandalism (damaging facilities such as computer devices) | Financial loss and cause the device to become damaged |
|            | R012  | New employees who do not understand the system workflow | Data completion process is not timely |
| Systems and Infrastructure | R013  | Poor network connection | Users will have difficulty in accessing the system |
|            | R014  | Hardware malfunction | Hinder business processes and users will have difficulty in accessing the system |
|            | R015  | Server Down       | Unable to access system and database |
|            | R016  | Corrupt Data      | User cannot view valid data |
|            | R017  | Overheat          | May cause hardware damage due to rising temperatures |
|            | R018  | Trouble Backup    | May cause data loss |
|            | R019  | System Error      | Users will have difficulty running the system |
|            | R020  | Power Outage      | Business process activities can’t run |

From table 3 on identifying the possible impacts of risk above, you can see the impact of the possible risks that occur.

**Further Risk**

Analysis enters the risk analysis stage. At this stage, an assessment of possible risks is carried out at the previous stage of risk identification, using the Likelihood criteria table. In the Likelihood table there are 5 criteria based on the frequency of possible risk events occurring.
Then in table 5 below is a table of impact value or impact that occurs from possible risks in Toko Raja Computer Balikpapan. In this impact assessment table is grouped into 5 criteria and grouped by ranging from the least influential impacts to the most influential impacts.

| Impact | Information |
|--------|-------------|
| Value  | Criteria |
| 1      | Insignificant | Does not interfere with activities |
| 2      | Minor        | The company's activities are slightly hampered |
| 3      | Moderate     | Causes disruption to business processes |
| 4      | Major        | Inhibits almost all activities |
| 5      | Catastrophic | Company activities stop |

After getting the probability criteria (Likelihood) in table 4, and the impact criteria in table 5. Then further assessment of possible risks based on tables 4 and 5.

| Factor            | Kemungkinan Resiko | Likelihood | Impact |
|-------------------|--------------------|------------|--------|
| Nature            |                    |            |        |
| R001 Flood        | 1                  | 4          |        |
| R002 Earthquake   | 2                  | 2          |        |
| R003 Fire         | 1                  | 5          |        |
| R004 Lightning    | 2                  | 3          |        |
| Human             |                    |            |        |
| R005 Human Error  | 4                  | 3          |        |
| R006 Abuse Of Access Rights | 2 | 2 |        |
| R007 Data theft   | 1                  | 2          |        |
| R008 Data hardware| 1                  | 3          |        |
| R009 Hacking      | 1                  | 3          |        |
| R010 Elusive User Interface | 2 | 1 |        |
| R011 Vandalism (damaging facilities such as computer devices) | 1 | 3 |        |
| R012 New employees who do not understand the system workflow | 4 | 2 |        |
| R013 poor network connection | 4 | 4 |        |
| R014 Hardware malfunction | 2 | 4 |        |
| R015 Server down  | 4                  | 4          |        |
| R016 Corrupt data | 1                  | 4          |        |
| R017 Overhead     | 4                  | 1          |        |
| R018 Trouble Backup | 1 | 2 |        |
| R019 Sistem error | 3                  | 4          |        |
| R020 Power outage | 3                  | 3          |        |

From table 6 above can find the value of possible risks in the Table Likelihood and Impact. After finding the value of Likelihood and Impact, then enter at the risk evaluation stage.

**Risk Evaluation**
In the last stage, the risk evaluation will be conducted risk evaluation process of the possibilities - possible risks that have been analyzed at the previous stage. From the results of the analysis will be included in the risk evaluation matrix based on the guidelines contained in the ISO 31000 framework. Matrix evaluation is distinguished into 3 risk levels, namely: Low, Medium, and High.

Table 7. Risk Evaluation Matrix

| ID  | Possible Risks                            | likelihood | Impact | ID |
|-----|------------------------------------------|------------|--------|----|
| R013| Poor network connection                   | 4          | 4      | High |
| R015| Server Down                              | 4          | 4      | High |
| R001| Flood                                    | 1          | 4      | Medium |
| R003| Fire                                     | 1          | 5      | Medium |
| R004| Lighting                                 | 2          | 3      | Medium |
| R005| Human Error                              | 4          | 3      | Medium |
| R012| Nouveaux employés qui ne comprennent pas le flux de travail du système | 4          | 2      | Medium |
| R014| Dysfonctionnement matériel                | 2          | 4      | Medium |
| R016| Data Korup                               | 1          | 4      | Medium |
| R017| Overhead                                 | 4          | 1      | Medium |
| R019| System Error                             | 3          | 4      | Medium |
| R020| Power Outage                             | 3          | 3      | Medium |
| R002| Earthquake                               | 2          | 2      | Low |
| R006| Abuse of access                          | 2          | 2      | Low |
| R007| Data Theft                               | 1          | 2      | Low |
| R008| Hardware Theft                           | 1          | 3      | Low |
| R009| Hacking                                  | 1          | 3      | Low |
| R010| Elusive User Interface                   | 2          | 1      | Low |

Table 7 describes the ratio of groupings based on risk levels from high to low. The next step is to include each identity of possible risks into the risk evaluation matrix in accordance with the Likelihood criteria and Impact criteria.

Table 8. Matrix Risk Evaluation Based on Likelihood and Impact

Based on Likelihood and Impact several possible risks can be categorized by the appropriate ratio as in table 8. After entering the possibility of risk into the evaluation matrix based on Likelihood and Impact, in the next stage will be grouped 20 possible risks above into high, medium and low levels.
In the table of 9 stages of the risk evaluation process above, there are 20 possible risks that have been analyzed and grouped based on the risk level. There are 2 possible risks that are categorized into high-level risk levels, namely: R013 and R015. Then there are 10 possible risks that are categorized into medium level risk levels, namely: R001, R003, R004, R005, R012, R014, R016, R017, R019 and R020. And there are also 8 possible risks that are categorized into low level risk levels, namely: R002, R006, R007, R008, R009, R010, R011, and R018.

Risk Treatment

After conducting the risk identification process regarding assets that are in the Ipost application environment, then the risk treatment stage will be carried out. In this stage provide risk action against possible risks that have been grouped based on the risk level in table 9. In table 10 is expected to minimize the possible risks that can occur for the application Ipost, which is owned Toko Raja Computer Balikpapan branch.

| ID   | Possible Risks                                | Risk Level | Risk Measures                                                                 |
|------|-----------------------------------------------|------------|--------------------------------------------------------------------------------|
| R013 | Poor network connection                       | High       | Replace with a new ISP (Internet Service Provider)                             |
| R015 | Server down                                   | High       | Perform scale checks on the database                                           |
| R001 | Flood                                         | Medium     | Setting up a fire extinguisher                                                 |
| R003 | Fire                                          | Medium     | Installing a lightning rod                                                     |
| R004 | Lighting                                      | Medium     | Training users                                                                 |
| R012 | New employees who do not understand the system workflow | Medium | Create SOP system work and conduct training to new employees                   |
| R014 | Hardware malfunction                          | Medium     | Provide insurance against existing hardware assets                             |
| R016 | Data korup                                    | Medium     | Perform backups periodically                                                   |
| R017 | Overhead                                      | Medium     | Provides a room that has ac (Air Conditioner) and adds fan to all hardware      |
| R019 | System Error                                  | Medium     | Increase bandwidth, perform system updates, and perform antivirus updates.      |
| R020 | Power Outage                                  | Medium     | Provides an electric generator set with power to suit your needs. Then set up Uninterruptible Power Supply (UPS) |
| R002 | Earthquake                                    | Low        | Provides a safe enough place to place the devices                              |
| R006 | Right of Access Abuse                         | Low        | Impose access restrictions on each device                                      |
| R007 | Data Theft                                    | Low        | Installing CCTV, alarms, and sensors in every room                             |
| R008 | Hardware Theft                                | Low        | Installing CCTV, alarms, and sensors in every room                             |
| R009 | Hacking                                       | Low        | Using private networks and improving the security of their systems             |
| R010 | Elusive User Interface                        | Low        | Change the look of the user interface to make it simpler and functional        |
| R011 | Vandalism (damaging facilities such as computer devices) | Low | Provide indemnification warning to each user                                  |
| R018 | Trouble Backup                                | Low        | Make SOP backups and perform backups on a scaled basis.                        |

In table 10 get the action that needs to be done Toko Raja Computer Balikpapan branch to minimize the risk in Toko Toko Raja Computer Balikpapan branch in accordance with the ratio ofカテゴリ Likelihood and Impact.
4. Conclusions And Suggestions

Based on SI/IT risk analysis research using ISO 31000:2018 in Ipost application owned by Toko Raja Computer Balikpapan branch starting from the risk assessment stage, risk identification, risk analysis, risk evaluation, to risk treatment stage. From these stages, this risk analysis obtains 20 possible risks that can at any time interfere with the performance of the Ipost application as well as interfere with the business process contained in the Toko Raja Computer Balikpapan branch. There are 2 possible risks with High level including poor network connection and server down. Then there are 10 possible risks with medium level including flood, fire, lightning, human error, new employees who do not understand the system workflow, hardware damage, corrupt data, overheating, system error, and power outages. Then there are also 8 possible risks with low levels that include earthquakes, misuse of access rights, data theft, hardware theft, hacking, elusive user interface, vandalism, and trouble backup. After this research is conducted, it is expected that this research can be used Toko Raja Computer Balikpapan branch as a guideline or policy to minimize the possibilities - possible risks that can occur by using the proposed risk measures that are already available in table 10 such as conducting scale checks on the database, checking the.

Referensi

A. R. Tampubolon and Suhardi, Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 : 2009 Studi Kasus : Pembobolan ATM BCA Tahun 2010, J. Telemat., vol. 7, no. 2, pp. 1–10, 2011.

H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square), J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 2, no. 11, pp. 4991–4998, 2018.

D. E. di and N. Susanto, Analisis Manajemen Risiko Aktivitas Pengadaan pada Percetakan Surat Kabar, J. Metris, vol. 18, pp. 113–118, 2017.

I. Lanin, Standar Baru Manajemen Risiko ISO 31000:2018, JIBFG Institute, 2018. https://ibfgi.com/risk-management-31000/ (accessed Apr. 12, 2018).

Angraini and I. D. Pertiwi, Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan ISO 31000, J. Ilm. Rekayasa dan Manaj. Sist. Inf., vol. 3, no. 2, pp. 70–76, 2017, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/RMSI/article/view/4317.

D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ, JURIKOM (Jurnal Ris. Komputer), vol. 7, no. 1, p. 91, 2020, doi: 10.30865/jurikom.v7i1.1791.

A. Novia Rilyani, Y. A. Firdaus W ST, and D. S. Dwi Jatmiko, Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University) Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University), e-Proceeding Eng., vol. 2, no. 2, pp. 6201–6208, 2015.

F. L. Nice and R. V. Imbar, Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000, J. Inform. dan Sist. Inf., vol. 2, no. 2, pp. 1–11, 2017.