VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480 /jitk.v9i1.4080

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

# RISK MANAGEMENT OF INFORMATION SYSTEM IN DISKOMINFO STATISTIC AND ENCODING USING NIST SP 800-30

**Budi Tjahjono[1*]; Miri Ardiansyah[2]; Gerry Firmansyah[3]; Habibullah Akbar[4]**

Master of Computer Science[1,2,3,4]
Universitas Esa Unggul
www.esaunggul.ac.id
budi.tjahjono@esaunggul.ac.id[1], miriardiansyah805@student.esaunggul.ac.id[2] , gerry@esaunggul.ac.id[3], habibullah.akbar@esaunggul.ac.id[4]

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

***Abstract—*** E-Government is a form of government service in digital form that utilizes the internet network which makes government services to the community easy. However, behind the perceived convenience, of course, there will be risks that arise, for example data loss, data theft, mis-access, illegal access, hardware damage, hacking, etc. which will have a negative impact on an organization, including in the Statistics and Encryption Communication and Information Service, XYZ Regency. The most commonly found threats are those that come from humans and electricity. In addition, there are still many sources of threats that have the potential to pose risks that will interfere with the implementation of electronic-based government. From the results of risk measurements that have been carried out based on NIST SP 800-30 By multiplying between the levels determined in the likelihood and impact processes to produce a number to be used as a guide in determining the level of risk, it was found that the risk threats originating from humans are 60% risk with Low level, 30% risk with Medium level, and 10% risk with High level. While the risk derived from electricity was 20% risk with Low level, 20% risk with Medium level, and 60% risk with High level. Lastly sourced from Technical is 34% risk with Low level, 33% Medium level risk, and 33% High level risk. Overall the risk assessment results were 39% risk threats with Low level, 33% risk threat with Medium level, and 28% risk threat with High level.

***Keywords****: E-Government, Diskominfo of XYZ District, Risk Management, NIST SP 800-30.*

**Abstract**— *E-Government* merupakan bentuk pelayanan pemerintah dalam bentuk digital yang memanfaatkan jaringan *internet* yang membuat pelayanan pemerintah kepada masayrakat menjadi mudah. Namun dibalik kemudahan yang dirasakan tentunya akan ada risiko yang muncul misalnya kehilangan data, pencurian data, salah akses, akses illegal, kerusakan *hardware*, peretasan, dll yang akan menimbulkan dampak negatif bagi suatu organisasi tidak terkecuali di Dinas Kominfo Statistik dan Persandian Kab. XYZ. Ancaman yang paling sering ditemukan adalah ancaman yang bersumber dari manusia dan listrik. Selain itu juga masih banyak sumber-sumber ancaman yang berpotensi menimbulkan risiko yang akan mengganggu penyelenggaraan pemerintahan berbasis elektronik. Dari hasil pengukuran risiko yang sudah dilakukan berdasarkan NIST SP 800-30 dengan melakukan perkalian antara level-level yang ditetapkan pada proses *likelihood* dan *impact* sehingga menghasilkan angka untuk dijadikan pedoman dalam menetapkan level risiko, didapatkan hasil bahwa ancaman risiko yang bersumber dari manusia adalah 60% risiko dengan tingkat *Low*, 30% risiko dengan tingkat *Medium*, dan 10% risiko dengan tingkat *High*. Sedangkan risiko yang bersumber dari listrik adalah 20% risiko dengan tingkat *Low*, 20% risiko dengan tingkat *Medium*, dan 60% risiko dengan tingkat *High*. Dan terakhir yang bersumber dari Teknis adalah 34% risiko dengan tingkat *Low*, 33% risiko tingkat *Medium*, dan 33% risiko tingkat *High*. Secara keseluruhan hasil penilaian risiko adalah 39% ancaman risiko dengan tingkat *Low*, 33% ancaman risiko dengan tingkat *Medium*, dan 28% ancaman risiko dengan tingkat *High*.

***Keywords****: E-Government, Diskominfo Kab. XYZ, Manajemen Risiko, NIST SP 800-30*

## INTRODUCTION

E-Government is a form of government service in digital form that utilizes the internet network which aims to make government services to the community easy. However, behind the ease of being felt, of course, there will be risks that arise, for example data loss, data theft, mis-access, illegal

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4080

access, hardware damage, hacking, etc. which will otherwise have a negative impact on an organization, including the Department of Communication and Information Statistics and Encoding of XYZ Regency which supervises applications in the Regional Device Organization (OPD) of XYZ Regency in running and maximizing its government services. However, the problem that arises is that there are several types of threats that exist in the application implementation in XYZ Regency. The most commonly found threats are those that come from humans and electricity. Apart from the two sources of threats described above, of course, there will be many other sources of threats that can occur and can pose risks that will interfere with the running of government services.

Risk is a state of uncertainty over the level of probability. Risk is closely related to unpleasant things, so it is very important to continue to be careful in all aspects with the right calculations [1]. Risk can be considered as a possible obstacle that has the potential to have a negative impact on the goals to be achieved [2]. Risks cannot be allowed to appear so casually that they have a negative impact. Risk can be controlled by doing risk management [3].

Risk management is defined as the implementation of internal management functions dealing with various kinds of uncertain situations that will be faced company, which includes the function of planning, organizing, implementing, supervising, and evaluating risk management programs [4]. Risk is an integral part of business and inherent in company activities [5]. The aim of risk management is to create level protection Which mitigate vulnerability to threats and potential consequences, thus reducing the risk to acceptable level [6].

There are many methods that can be used to perform information security risk management such as Octave, NIST SP 800-30 and ISO 27001 [7]. However, in this study, the method that will be used in carrying out risk management is NIST SP 800-30 (National Institute Of Standarts and Technology SP 800-30). NIST (National Institute of Standard Technology) is a non-regulatory federal agency in the United States that has a mission to develop and promote measurements, standards and technology to increase productivity and improve the quality of human life[8].

The reason for choosing NIST SP 800-30 is based on previous research, namely research conducted by [7] that NIST SP 800-30 has been shown to make more contributions such as: providing consistent and comprehensive information security insights for policymakers, structured resource modeling, information security insights acceptable to various risk takers, threat determination can be identified easily, decision makers do not hesitate to take risks because each risk has been properly investigated. NIST SP 800-30 is the best of 3 methods for risk analysis, namely Mehari, Magerit and Microsoft's Security Management Guide, especially when conducting risk analysis, NIST SP 800-30 provides control recommendations.

The stages of risk management using NIST are divided into three stages, namely :

1. Risk Assesment
   Organizations use risk assessment to define potential threats and risks related to the use of information technology. The output of this process is expected help identify how controls to perform reductions and omissions risks during the mitigation process. This process consists of 9 (nine) steps in the risk assessment activities [9].
2. Risk Mitigation
   Risk mitigation Is the second stage of the risk management process issued by NIST, mitigation or reduction risk is a systemic methodology used by management to reduce the impact of risk [10].
3. Risk Evaluation
   The evaluation stage is the stage where an assessment of the implementation is carried out risk control. For example every year this is done to reassess whether the tool or method of risk reduction still relevant [11].

in this study will focus more on the risk assessment stage.

## MATERIALS AND METHODS

### A. Research Methodology

The stages of research that will be carried out consist of 4 (four) systematic stages can be seen in figure 1 below.

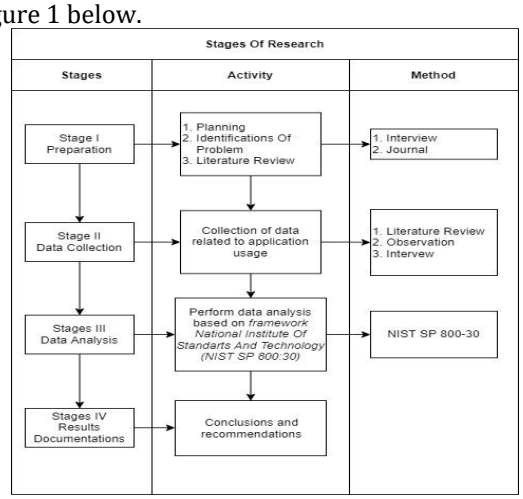


Figure 1. Stages of Research

The stages from beginning to end that will be carried out in this study are as follows :

1. Preparation

The preparation stage includes Designing, Problem Identification, and Literature Study. While the method used is an interview to find out if there has ever been a problem in the use of the application in the Regency, then what problems occur most often, the source of the problem that occurs, what control is carried out on the problem that occurs.

2. Data Collection

Data collection is carried out to obtain data related to the research carried out. The methods used in this data collection are literature studies, observations and interviews. Observation is a form of observation or direct sensing of something object, condition, situation, process or behavior [12]. Interviews is a technique data collection is done through face-to-face and direct Q&A between collectors sources/data sources [13]. Interviews at the data collection stage were conducted to obtain data that will be used for the analysis process in accordance with the NIST SP 800-30 method.

3. Analysis Stage

The third stage is to analyze the data that has been obtained in the previous process using the NIST SP 800-30 framework. Analysis is a way of finding and processing data properly (systematically) good record of the results of interviews, observations, and others in order to increase knowledge researcher of the research problem under study and its presentation as subsequent findings [14].

4. Documentation / Conclusions and Suggestions

The last stage is carried out documentation of the report of conclusions and suggestions in the form of a final project in accordance with the applicable format.

**B. Data Analysis with NIST SP 800-30**

At the Analysis stage, the framework NIST SP 800-30 is used.

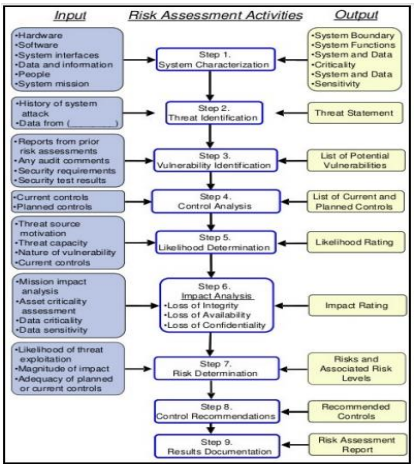


Figure 2. NIST SP 800-30 Risk Assessment Activities [15]

The following is an explanation of the stages / risk assessment activities as well as the inputs and outputs of each stage in NIST SP 800-30 [15] :

1. System Characterization

Assessing the characteristics of the system, see the point of view of hardware, software interface, data and information, to the purpose of the system. This point of view will be the input of the process, so that it will produce outputs, namely system limitations, system functionality, data and sensitivity levels, users and others.

2. Threat Identification

Recognizing various threats and sources that will be a disruption to the system / recognize the sources of threats on the system. The input of this process is a report of a problem or attack that has occurred. While the output of this process is a threat statement, which is a set of risks that may occur as well as a source of risk that can cause vulnerabilities in the system.

3. Vulnerability Assessment

At this stage, various vulnerabilities are identified that allow threats to occur to the system. The inputs at this stage are reports or outputs from previous risk assessments. While the output produced is a list of vulnerabilities that exist in the system.

4. Control Analysis

The main objective of this stage is to analyze the controls that have been implemented or that will be applied, in order to minimize the possibility of a threat. The inputs from this stage are the controls that have been implemented in each risk/vulnerability, while the output is a list of controls on the risks that are being implemented and the control plan that will be applied to possible risks.

5. Likelihood Determination

This stage is used to obtain a value of the possible tendency to weakness of the system. The inputs of this stage are the source of risk and the motivation of the cause of the source of risk, and vulnerability. While the output of this stage is the level / level of the possibility of risk threat occurrence.

6. Impact Analysis

Assessing the impact that occurs on attacks on weak parts of a system. The input of this system is the mission of the system and the level of data sensitivity or in other words how the risk will affect the system and the data being processed. Possible considerations are issues of data integrity,



Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4080

availability of services and loss of trust. The output of this system is the magnitude of impact definition.

7. Risk Determination

Risk determination aims to assess the level of risk to the system, to assess the level of risk this refers to the possible risks and impacts of risks that have been determined. Inputs from this stage are the possibility of a threat, the magnitude of the impact of the threat, the effectiveness of controls that have already been implemented or newly planned. While the output is the risk and the level of associated risk.

8. Control Recommendation

The goal of this stage is to reduce the level of risk in the IT system so that it reaches an acceptable level. The input is the output of the previous stage i.e. risk and risk level, from here a list of control recommendations will be generated.

9. Result Document

It is a result of the activities carried out.

## RESULTS AND DISCUSSION

At this stage, risk analysis / measurement is carried out at the Statistical and Encryption Information Communication Service of XYZ Regency based on data obtained using the National Institute Of Standards And Technology framework. The processes are as follows :

### A. System Characterization

The information system application in XYZ Regency under the auspices of the Statistical and Encryption Information Communication Service of XYZ Regency is a website-based and online-based application. The hardware resource is a Personal Computer (PC) which is used to operate information system applications with the windows 10 operating system. Meanwhile, the data and information managed by the applications in the district are District Documents, Statistical Data, Community data, and other important data. Human resources are operators of information system applications. These applications are based online and operated via PC. Therefore, the use of the application is very dependent on electricity and internet resources patent in its use.

### B. Threat Identification

Based on the results of interviews that have been conducted with two speakers at Statistical and Encryption Information Communication Service of XYZ Regency The interview was conducted with two people, namely Mr. Ayubi Khaafidh as the head of the technical team / local it supports and Mr. Indra Asura as the team that manages and controls the use of SPBE / E-Government as well as the general operator of SPBE Statistical and Encryption Information Communication Service, the threat data can be seen in table 1 below :

Table 1. Threat Identification

| Source | Motivation | Threat | Code |
|---|---|---|---|
| Human | Human Error | Forgot Password / Username | A001 |
| | | Data Leakage by Internal | A002 |
| | | Application Crash | A003 |
| | | Access Errors | A004 |
| | | Misuse of Access Rights | A005 |
| | | Data Deleted | A006 |
| | | Forgot the way /flow of using the app | A007 |
| | Ego | Former Employee Rogue | A008 |
| | | Hacker / Cracker | A009 |
| | | Internal Rogue | A010 |
| Elctricity | Electrical Network Damage | Hardware Damage / PC Damage | A011 |
| | | Burnt Hardware | A012 |
| | | Lost Data/Corrupt Data | A013 |
| | | Lost Internet Signal | A014 |
| Technical | Virus | Unusable Application | A015 |
| | | Loss of important data/assets | A016 |
| | | Software cannot be accessed | A017 |
| | | Lost or damaged data - important data | A018 |

### C. Vulnerability Identification

Based on the interviews conducted, it was found that the system vulnerabilities in Statistical and Encryption Information Communication Service of XYZ Regency are shown in table 2 below :

Table 2. Vulnerability Identification

| Code | Gaps / Insecurity |
|---|---|
| A001 | High Turn Over so as to cause frequent changes of operators / Poorly trained operators |
| A002 | Unavailability of Cooperation Agreement containing responsibility to OPD application operators |
| A003 | Granting Full Access Rights To HR who do not fully understand the application being used. |
| A004 | Lack of HR Training, |
| A005 | Operator Does Not Logout / Exit after using the application. |
| A006 | Lack of trained human resources, |
| A007 | High Turn Over causing frequent operator changes |
| A008 | OPD did not confirm the release of the application operator. So that the technical team does not freeze the operator's access rights / still have access. |
| A009 | There is no special team responsible for system security. |
| A010 | Unavailability of a Cooperation Agreement containing responsibility for OPD application operators |
| A011 | Hardware Damage / PC Damage |

| Code | Gaps / Insecurity |
|---|---|
| A012 | Burnt Hardware |
| A013 | Lost Data/Corrupt Data |
| A014 | Lost Internet Signal |
| A015 | Unusable Application |
| A016 | Irregular use of Flashdisk |
| A017 | Improper use of anti-virus |
| A018 | Downloading and installing apps carelessly |

### D. Control Analysis

Based on the results of the interview that has been conducted, the results are obtained in the form of control are shown in table 3 below :

Table 3. Control Analysis

| Code | Control |
|---|---|
| A001, A004, A007 | Coordinating and re-explaining things that are not yet known or forgotten to the relevant operator. |
| A002, A003, A005, A006, | Coordinating related to data sensitivity and the importance of data security and responsibility for data security by operators. |
| A008, A010, A009 | Socialization / coordination with employees and leaders related to strengthening system security. |
| A011, A012, A014, A015 | Socialization / coordination with employees / leaders of related OPDs related to prevention. e.g. using a UPS. |
| A013 | Socialization to operators so that they can often save files that have been created / edited so that they are not lost or corrupted. As well as backing up important files. |
| A016, A017, A018 | Coordinating and socializing with operators related to data sensitivity, in order to install anti-virus, orderly use of flasdisks, and virus danger to data and sources of viruses. |

### E. Likelihood Determination

At this stage, the possibility of a risk from the existing threat is sought. The determination of possibilities is divided into three types, namely High, which includes threat sources that have high motivation, with open loopholes and controls to prevent ineffective loopholes, medium, namely threat sources have sufficient motivation and there are gaps that can be passed but there are controls that are carried out that are likely to minimize loopholes and threats, while Low is a source of threat that lacks motivation and there are controls that are useful for preventing or blocking gaps for threats can occur. The level of possible risk of each threat is are shown in table 4:

Table 4. Likelihood Determination

| Code | Threat |
|---|---|
| A001 | *Medium* |
| A002 | *High* |
| A003 | *Low* |
| A004 | *Low* |
| A005 | *Low* |
| A006 | *Medium* |
| A007 | *Medium* |
| A008 | *Medium* |
| A009 | *Low* |
| A010 | *Low* |
| A011 | *High* |
| A012 | *High* |
| A013 | *High* |
| A014 | *High* |
| A015 | *Medium* |
| A016 | *High* |
| A017 | *Low* |
| A018 | *Medium* |

### F. Impact Analysis

Impact Analysis is a stage of measuring or analyzing the influence of existing risk threats. In determining the impact, it also consists of three parts, namely Low, Medium, High. Low is the effect that occurs caused by the risk of lowering the reputation of the organization. Medium is the effect that is felt not only can damage the reputation but also damage to some equipment / hardware and can cause financial losses. While high, the effect felt or produced can damage the reputation of the organization at a high level because it can eliminate public trust in the organization, can damage some parts of the hardware so that it can cause high financial losses, even to the point of being life-threatening or causing death. the levels of impact generated by the risk threat can be seen in table 5 below :

Table 5. Impact Analysis

| Code | Impact Analysis |
|---|---|
| A001 | *Low* |
| A002 | *High* |
| A003 | *Low* |
| A004 | *Low* |
| A005 | *Medium* |
| A006 | *High* |
| A007 | *Medium* |
| A008 | *High* |
| A009 | *High* |
| A010 | *Medium* |
| A011 | *High* |
| A012 | *High* |
| A013 | *High* |
| A014 | *Medium* |
| A015 | *Low* |
| A016 | *High* |
| A017 | *Medium* |
| A018 | *High* |

### G. Risk Determination

This stage aims to assess the level of risk faced in the use of information system applications in Statistical and Encryption Information Communication Service of XYZ Regency. This risk assessment is obtained by multiplying between the levels set in the Likelihood Identification process with impact analysis as shown in the following formula :

Risk Assessment = Impact x Likelihood



Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4080

To determine or assess risk, a matrix is used as in the Table 6 as a reference for calculations. This matrix shows what the overall level of risk is. The range of numbers in determining this risk assessment is 1 to 10 Low risk levels, more than 10 to 50 Medium risk levels, while more than 50 to 100 High risk levels.

Table 6. Risk Level Matrix [16]

| Thread Likelihood | Impact | | |
|---|---|---|---|
| | Low (10) | Medium (50) | High (1oo) |
| **High (1.0)** | Low 10x1.0=10 | Medium 50x1.0=50 | High 100x1.0 = 100 |
| **Medium(0.5)** | Low 10x0.5=5 | Medium 50x0.5=25 | Medium 100x0.5 = 50 |
| **Low (0.1)** | Low 10x0.1=1 | Low 50x0.1=5 | Low 100x0.1 = 10 |

Furthermore, Based on the table 6, the process of calculating and assessing risks can be seen in the table 7 below :

Table 7. Risk Determination

| Code | Likelihood Determination | Impact Analysis | Likeli x Impact |
|---|---|---|---|
| A001 | *Medium (0.5)* | *Low (10)* | 0.5 x 50 = 5 (*Low*) |
| A002 | *High (1.0)* | *High (100)* | 1.0 x 100 =100 (*High*) |
| A003 | *Low (0.1)* | *Low (10)* | 0.1 x 10 = 1 (*Low*) |
| A004 | *Low (0.1)* | *Low (10)* | 0.1 x 10 = 1 (*Low*) |
| A005 | *Low (0.1)* | *Medium (50)* | 0.1 x 50 = 5 (*Low*) |
| A006 | *Medium (0.5)* | *High (100)* | 0.5 x 100 =50 (*Medium*) |
| A007 | *Medium (0.5)* | *Medium (50)* | 0.5 x 50 = 25 (*Medium*) |
| A008 | *Medium (0.5)* | *High (100)* | 0.5 x 100 =50 (*Medium*) |
| A009 | *Low (0.1)* | *High (100)* | 0.1 x 100 =10 (*Low*) |
| A010 | *Low (0.1)* | *Medium (50)* | 0.1 x 50 = 5 (*Low*) |
| A011 | *High (1.0)* | *High (100)* | 1.0 x 100 = 100 (*High*) |
| A012 | *High (1.0)* | *High (100)* | 1.0 x 100 = 100 (*High*) |
| A013 | *High (1.0)* | *High (100)* | 1.0 x 100 = 100 (*High*) |
| A014 | *High (1.0)* | *Medium (50)* | 1.0 x 50 = 50 (*Medium*) |
| A015 | *Medium (0.5)* | *Low (10)* | 0.5 x 10 = 5 (*Low*) |
| A016 | *High (1.0)* | *High (100)* | 1.0 x 100 = 100 (*High*) |
| A017 | *Low (0.1)* | *Medium (50)* | 0.1 x 50 = 5 (*Low*) |
| A018 | *Medium (0.5)* | *High (100)* | 0.5 x 100 = 50 (*Medium*) |

*(Calculation based on table 5 and 6)*

based on the results of the calculation in table 7 above, risks sourced from humans have not been found risks with High, or Medium levels. Based on the calculations in table 7, the level of risk originating from humans is 6 risks with Low risk levels, 3 risks with Medium risk levels, and 1 risk with High risk levels. The graph can be seen in figure 3 below.

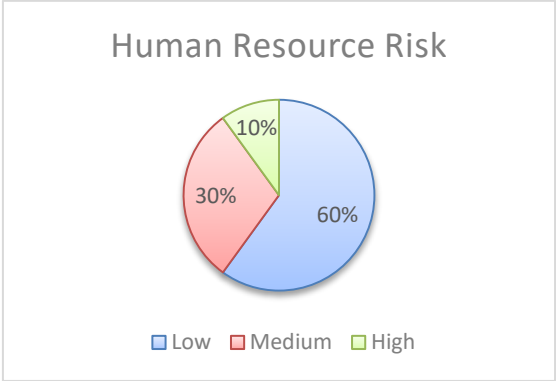


Figure 3. Human Resource Risk

Meanwhile, the risks derived from electricity based on the calculations made table 7 are 1 risk with a Low level, 1 risk with a Medium risk level, and 3 risks with a High level. In figure 4 below a look at the graph of the level of risk sourced from Electricity.

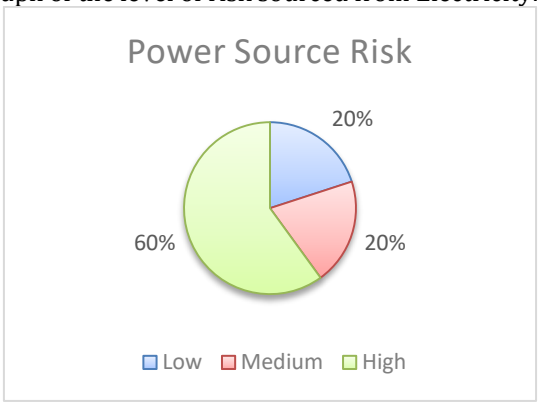


Figure 4. Power Source Risk

Meanwhile, risks derived from Technical sources (Viruses) based on calculations in the table 7 obtained results of 1 risk with a Low risk level, 1 Medium level risk, and 1 High level risk. The graph can be seen in figure 5 below.

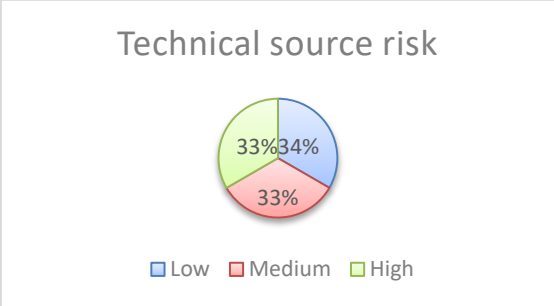


Figure 5. Technical source risks

Overall, the risk assessment chart based on the calculations in the table 7 is obtained 8 risks with Low risk levels, 5 risks with Medium risk levels, and 5 risks with High levels. In the figure 6 below is a graph that is the overall result of calculating or measuring risks in the Statistical and Encryption Information Communication Service of XYZ Regency.

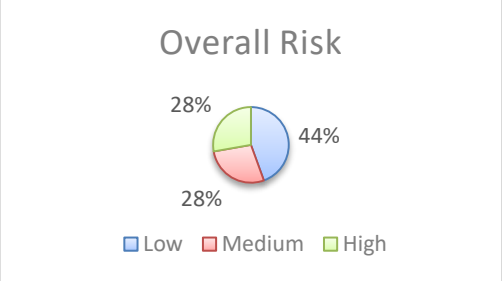


Figure 6. Overall Risk

Based on the source of risk can be seen in figure 7 below.

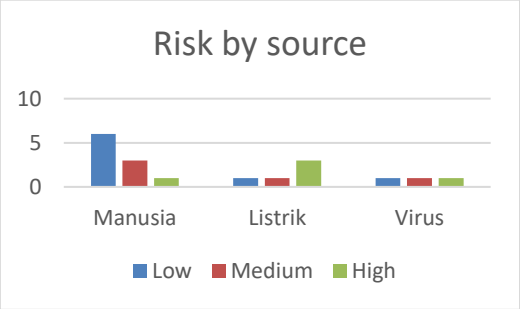


Figure 7. Risk by Source

## H. Control Recommendation

Control Recommendation is the stage of providing control recommendations from researcher to eliminate or minimize risk. For recommendations given on each type of risk can be seen in table 8 below.

Table 8. Control Recommendation

| Code | Risk Level | Control Recommendation |
|---|---|---|
| A001 | *Low* | 1. Giving operators a username and password that is easy to remember.<br>2. Providing the operator with a specific account note and require the relevant operator to keep and maintain the record so that when forgotten they can reopen the record.<br>3. The technical team creates and stores a document containing a list of accounts used by the operator of each OPD as a backup to quickly respond to risk mitigation. |
| A002 | *High* | 1. Creating an employment agreement related to the obligation to be responsible for the security and integrity of data managed by the operator.<br>2. Conducting socialization related to the level of data sensitivity and the importance of data or document security. |
| A003 | *Low* | Creating SOPs related to the granting of operator Access Rights types by the technical team. |
| A004 | *Low* | Conducting socialization / training and creating documents containing explanations of the character of each application, the sensitivity of the data being managed, as well as complete instructions on using the application. |
| A005 | *Low* | Creating and pasting SOPs related to the use of applications at the operator's workplace |
| A006 | *Medium* | Conducting socialization / training and creating documents containing explanations of the character of each application, the sensitivity of the data being managed, as well as complete instructions on using the application. |
| A007 | *Medium* | Conducting socialization / training and creating documents containing explanations of the character of each application, the sensitivity of the data being managed, as well as complete instructions on using the application. |
| A008 | *Medium* | 1. Creating an employment agreement related to the obligation to be responsible for the security and integrity of data managed by the operator.<br>2. Coordinating and requiring each OPD to always confirm the entry and exit of the operator to the technical team so that the technical team can act to freeze accounts owned or known by the former employee in question. |
| A009 | *Low* | Establishing a special team responsible for information system security in order to focus on preventing outside attacks |
| A010 | *Low* | Creating an employment agreement related to the obligation to be responsible for the security and integrity of data managed by the operator. |



Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4080

| Code | Risk Level | Control Recommendation |
|---|---|---|
| A011<br>A012<br>A013<br>A014<br>A015 | *High*<br>*High*<br>*High*<br>*Medium*<br>*Low* | 1. Providing an Uninteruptible Power Supply (UPS) so that the PC does not turn off suddenly when the power goes out in order to save the documents that are done so that files are not lost / corrupted. Then in order to be able to turn off the PC normally.<br>2. Providing a generator / generator as a backup power source. |
| A016<br>A017 | *High*<br>*Low* | 1. Always install and maintain anti-virus.<br>2. Downloading apps from trusted sources. |
| A018 | *Medium* | 3. Using an officially licensed application.<br>4. Always back up important data. |

## CONCLUSION

Based on the discussion that has been discussed in the previous chapter, the conclusions that can be drawn from the results of this study are as follows : The risk threats that exist in the use of the XYZ Regency information system application managed or shaded by the XYZ Regency Statistical and Encryption Informatics Communication Service that are detected come from three sources, namely 10 risk threats sourced from humans, 5 risk threats sourced from electricity, and 3 risk threats sourced from technical, with a total of 18 risk threats. From the results of risk measurements that have been carried out based on NIST 800-30, it is found that the risk threats originating from humans are 60% risk with Low level, 30% risk with Medium level, and 10% risk with High level. While the risk derived from electricity is 20% risk with Low level, 20% risk with Medium level, and 60% risk with High level. And lastly sourced from Technical is 34% risk with Low level, 33% Medium level risk, and 33% High level risk. Overall risk assessment results are 39% risk threats with Low level, 33% risk threat with Medium level, and 28% risk threat with High level. From the results of measurements made for the high-risk level, the most comes from electricity sources, the medium level comes the most from humans, while for the low risk threat level, the most also comes from humans. Based on the analysis that has been carried out, it is concluded that the risk threats that arise in accordance with the results of interviews conducted in general are caused by the immature system that is run related to the use of applications in government.

## REFERENCE

[1] O. Arifudin, U. Wahrudin, and F. D. Rusmana, *Manajemen Risiko*. 2020.

[2] I. B. Indonesia, *Manajemen Risiko 1*. 2015.

[3] P. Y.A.P, *Manajemen Risiko Perusahaan*. 2017.

[4] F. H. Hotdiana, A. Ahmad Yani, M. Putri, P. Syari, and F. Ekonomi Dan Bisnis Islam, "Analisis Risiko Bisnis," *J. Visions Ideas*, vol. 2, no. 2, pp. 119–125, 2022.

[5] Muhammad Asir, R. A. Yuniawati, K. Mere, K. Sukardi, and M. A. Anwar, "Peran manajemen risiko dalam meningkatkan kinerja perusahaan: studi manajemen sumber daya manusia," *Entrep. Bisnis Manaj. Akunt.*, vol. 4, no. 1, pp. 32–42, 2023, doi: 10.37631/ebisma.v4i1.844.

[6] W. Muka and M. A. Wibowo, "Penerapan Manajemen Risiko pada Proses Pengembangan Properti," *J. Permukim.*, vol. 16, no. 1, p. 31, 2021, doi: 10.31815/jp.2021.16.31-40.

[7] A. Elanda and R. L. Buana, "Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus: STMIK Rosma)," *Elkom J. Elektron. dan Komput.*, 2021, [Online]. Available: https://journal.stekom.ac.id/index.php/elkom/article/view/387

[8] N. fitrianti Fahrudin, A. Nugraha S, and K. Ramadhan Putra, "Penilaian Risiko Keamanan Data Karyawan Pada Sistem Informasi Dengan Menggunakan Framework Nist Sp 800-30 pada PT. ABC," *J. Ilm. Teknol. Infomasi Terap.*, vol. 8, no. 3, 2022, doi: 10.33197/jitter.vol8.iss3.2022.900.

[9] D. S. Valena, rizky prabowo, anie rose irawati, and aristoteles aristoteles, "Analisis Manajemen Risiko Sistem Informasi Perpustakaan Universitas Lampung Menggunakan Metode Nist Sp 800-30," *J. Komputasi*, vol. 7, no. 1, 2019, doi: 10.23960/komputasi.v7i1.2053.

[10] D. I. Izatri, N. I. Rohmah, and R. S. Dewi, "Identifikasi Risiko pada Perpustakaan Daerah Gresik dengan NIST SP 800-30," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 50, 2020, doi: 10.30865/jurikom.v7i1.1756.

[11] A. N. SUSANTO and N. F. FAHRUDIN, "Penilaian Risiko Sistem Informasi Keamanan Data Karyawan Dengan Menggunakan Framework Nist Sp 800-30 pada Perusahaan XYZ Institut Teknologi Nasional Bandung," *Pros. Disem. FTI Ganjil 2021/2022*, 2022.

[12] Z. Yusra, R. Zulkarnain, and S. Sofino, "Pengelolaan Lkp Pada Masa Pendmik

Covid-19," *J. Lifelong Learn.*, vol. 4, no. 1, pp. 15–22, 2021, doi: 10.33369/joll.4.1.15-22.

[13] E. Trivaika and M. A. Senubekti, "Perancangan Aplikasi Pengelola Keuangan Pribadi Berbasis Android," *Nuansa Inform.*, vol. 16, no. 1, pp. 33–40, 2022, doi: 10.25134/nuansa.v16i1.4670.

[14] Ahmad and Muslimah, "Memahami Teknik Pengolahan dan Analisis Data Kualitatif," *Proceedings*, vol. 1, no. 1, pp. 173–186, 2021.

[15] K. Harsanto and D. Hidayat, "Sistem Informasi Manajemen Risiko dengan Menggunakan Framework National Institute of Standards and Technology pada Lembaga Pendidikan," *J. Ipsikom*, vol. 6, no. 1, 2018.

[16] B. A. Nugraha, A. R. Perdanakusuma, and ..., "Analisa Manajemen Risiko pada Sistem Informasi Tata Naskah Dinas Elektronik dengan Kerangka Kerja NIST 800-30 pada Dinas Komunikasi dan Informatika …," *… Teknol. Inf. dan …*, 2020, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6884



Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri