Journal of Electrical, Electronics and Informatics, p-ISSN:2549-8304 e-ISSN:2622-0393

Security Risk Evaluation of Licensing System Using NIST SP 800-30 Framework and Maturity Level with CMMI

Ni Kadek Widiartini[1] Anak Agung Hary Susila[1], Putu Veda Andreyana[1]

[1] Information Technology Study Program
Faculty of Engineering, Udayana University
Denpasar, Indonesia
kwidiartini128@student.unud.ac.id

Abstract The use of information and communication technology in the field of government is an important thing to support an electronic-based government system or what is commonly called e-government. Responding to the instruction, the Investment and Integrated One-Stop Service Office (DPMPTSP) of Badung Regency in carrying out its duties and responsibilities utilizes the application of information technology by using web-based and mobile applications. The service system is called licensing services or abbreviated as laperon. This study uses the NIST SP 800-30 framework in evaluating risks in the four systems and uses the CMMI framework to determine the maturity level. The results of the risk identification show that the licensing service information system has 4 high-level risks, 12 medium-level risks and 29 low-level risks. The results of the maturity level assessment questionnaire show that the licensing service system has a maturity level gap of 1. Recommendations are given to minimize the identified risk threats and achieve the expected maturity level based on the NIST SP 800-53 revision 4 guidelines.

Index Terms— NIST SP 800-30, CMMI, licensing services, maturity level.

I. INTRODUCTION

The use of information and communication technology in the government sector is an important thing to support an electronic-based government system or what is commonly called e-government. E-government aims to facilitate all activities that run in government. Currently, the central and regional governments are trying to improve the quality of products and services used by the government internally and provided to the general public in order to fulfill the vision and mission of the organization. The application of information technology in the government sector has provided many conveniences, but the use of information technology can also have a negative impact on the government system if the security of the information is not maintained. Risk management plays an important role in protecting user information in the application of technology in the government sector. The government must pay attention to the security of information assets, data leaks and system failures that can cause losses in terms of finance and government productivity.

The Investment and One-Stop Integrated Service Office (DPMPTSP) of Badung Regency is a regional government institution that plays a strategic role and function in the field of licensing and investment which is formed based on Badung Regency Regional Regulation Number 8 of 2016 concerning the Formation and Composition of Badung Regency Regional Apparatus. Based on the main tasks and functions of the information system owned by the agency, it is undeniable that dependence on IT is very high, one example of which is the existence of a web-based and mobile public service system that integrates all public service products in Badung Regency. Online licensing services or abbreviated as laperon are web-based and mobile licensing service systems that are integrated with the entire licensing service process aimed at ensuring the smoothness and continuity of services to the public in submitting non-business licensing applications online which are the authority of the Badung Regency government.

The licensing service system manages employee data and all residents of Badung Regency who process non-business permits online so that there is an opportunity for information security risks to arise that disrupt public services and government administration. In the operation of this system, several problems occurred, such as the absence of proper supervision and planning in the management and security of information data at DPMPTSP Badung, servers down, power outages. One of the frameworks used in risk management is the National Institute of Standards and Technology framework which provides information security risk management guidelines that aim to improve cybersecurity. One of the maturity level assessments can use CMMI (Capability Maturity Model Integration) which is an approach model for assessing the maturity level and capabilities of a software organization in assessing the risk management process [19].

Several previous studies have applied this risk assessment model to conduct risk assessments on its objects such as those conducted by Delpia Amanda, et al. at SIAKAD Tanjungpura University, which was able to provide a solution for assessing the level of security of academic information systems in detail. Research conducted by Desak Made Novita, et al. on 11 IT start-ups using the CMMI and TMMi methods obtained different results in testing the level of maturity, where 6 teams got level 3, 3 teams were at level 2 and 2 teams were at level 1. Based on the problems and facts above, this study will examine the management of information system security risks in the licensing service system with the NIST and CMMI frameworks in order to measure the level of system maturity in assessing the risk management process. This study is expected to determine the level of maturity of information security in the licensing service system and provide recommendations for improvement in order to achieve the expected level so that it can protect the organization's business processes from security threats and minimize the risk of loss or data leakage.

II. LITERATURE REVIEW

1. Licensing Services

Online licensing services or what can be abbreviated as laperon is an electronic licensing service system that is integrated with the entire licensing service process that can be managed online starting from permit registration, payment of levies or taxes to distribution of permits to the public. The advantages of laperon are that permit application registration can be done anywhere and anytime, online officer verification, implementation of FIFO and auto disposition, notification and service messages related to permits submitted via SMS and email, payment of tax levies that can be done online, issuance of permits using electronic signatures and permit applications can be monitored directly by the public.

2. Risk Management

Risk management is the process of measuring or assessing risk and developing management strategies. Strategies that can be taken include transferring risk to other parties, avoiding risk, reducing the negative effects of risk and accommodating some or all of the consequences of certain risks [18]. According to the National Institute of Standards and Technology (NIST) in the publication NIST SP 800-30, it is a process that allows IT managers to balance operational costs and economic costs and security measures in achieving benefits by having a mission to protect IT systems and data in supporting the organization's mission. Risk management is an ongoing process to assess, mitigate, and evaluate the impact of risks [11].

Risk management begins with the risk assessment stage or risk assessment analysis. Each of these steps identifies aspects that influence the information technology system, including asset identification, threat and vulnerability identification, control identification, likelihood level analysis, impact analysis, determining the level of risk and evaluating the risk.

3. NIST Framework (National Institute Standards and Technology)

NIST (National Institute Standards and Technology) is a guide designed to help organizations improve the cybersecurity of an organization or company [8]. This framework helps organizations manage cybersecurity risks, build readiness, and improve their ability to respond to security threats. NIST SP 800-30 was chosen as the framework in this study because the guidelines for implementing the risk management process are explained in more detail and are suitable for all areas of the organization. This framework can be freely used without any copyright restrictions. Risk management at NIST has 3 stages, namely

1. Risk Assessment

Risk assessment is the first process carried out in implementing the risk management method. When conducting a risk assessment, there are 9 steps to identify potential threats and risks associated with the information system shown in Figure 1.

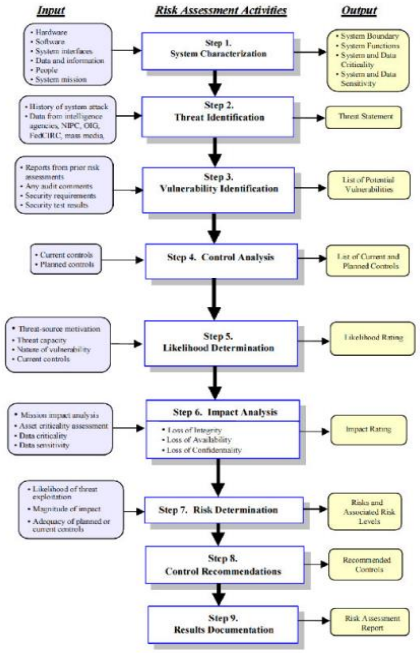

Figure 1 Risk Management Stages

These nine stages are used to determine future possibilities, threats to IT systems must be analyzed in relation to potential vulnerabilities and controls for IT systems.

a. System Characteristics

The initial stage in assessing information technology system risk is to determine the scope of an information technology system [9]. At this stage, the boundaries and resources and information that form the information technology system are identified. Information that needs to be collected related to the system, namely hardware, software, system interfaces, data, information, people who

Journal of Electrical, Electronics and Informatics, p-ISSN:2549-8304 e-ISSN:2622-0393

support and use the system, system missions (processes carried out by the information technology system), system and data criticality (value and importance of the system to the organization), and system and data sensitivity. The results of this stage are the characterization of the information technology system in the form of information and resources that form the system, a good understanding of the information technology system environment, and the boundaries of the system.

b. Threat Identification

Threat identification is carried out to determine the types of threats and sources of existing risk threats. Natural threats are threats that come from nature such as floods, earthquakes, tsunamis, hurricanes and others as well as threats that come from humans, namely a series of efforts made to take over organizational resources or assets in illegal ways such as malicious code, viruses, social engineering, hacking, cracking, terrorists [20]. Human error is a threat condition owned by human users based on intentional or accidental factors.

c. Vulnerability Identification

At this stage, a list of system vulnerabilities that can be exploited by potential threat sources is identified. The result of this process is a list of security requirements and can be used as input for evaluation. This process identifies systems, processes, and procedural weaknesses that describe potential vulnerabilities.

d. Control Analysis

The control selection stage is adjusted to the results of the previous risk identification. The result of this stage is a list of controls used or controls that are planned to be used by the information technology system to reduce the possibility of exploiting existing vulnerabilities and the impact of bad things.

e. Likelihood Determination

The likelihood determination stage is the stage used to obtain the value of the possible tendency of the system's weaknesses that can be used to identify and reduce the risks faced by the system [8]. The level of possibility is divided into 3, namely high, medium, low.

Table 1 *Likelihood Determination*

Likelihood Value	**Likelihood Level**	**Description**
1.0	*High*	Sources of threats that have high motivation that can harm the organization, this occurs because controls to prevent vulnerabilities are implemented ineffectively.
0.5	*Medium*	A threat source that has a motivation that is capable of harming the organization, but the organization can still exercise control which hinders the success of the existing vulnerability.
0.1	*Low*	Threat sources that have less or low motivation, control is used to prevent or reduce a vulnerability that will occur in the organization.

f. Impact Analysis

This stage analyzes the negative impacts of successful attacks on information system vulnerabilities such as system integrity failures, sensitive data security failures, and others. There are 3 categories in impact analysis, namely high, medium, low.

Table 2 Impact Analysis

Impact value	**Impact Level**	**Description**
100	*High*	Implementation of vulnerabilities can result in a very high cost loss of an organization's assets or resources, can cause breaches, losses or obstacles in the organization's mission.
50	*Medium*	The application of a vulnerability can result in a loss of assets or organizational resources, but may still result in a loss or hindrance to the organization's mission.
10	*Low*	Implementation of a vulnerability may result in the loss of some organizational assets or resources, and the organization can prevent the impact from affecting the organization's mission and revenue.

g. Risk Determination

The seventh stage in the NIST SP 800-30 framework is determining the risk to the system. The risk level can be determined through the results of scoring by multiplying the probability level value by the impact level value. After the risk level mapping is obtained, priorities are carried out starting from high (H), medium (M) and low (L) levels.

Table 3 Risk Level

Threat Likehood	High (1.0)	Impact Medium (0.5)	Low (0.1)
High	Low 10 x 1.0 = 10	Medium 50 x 1.0 =50	High 100 x 1.0 = 100
Medium	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	Medium 100 x 0.5 = 50
Low	Low 10 x 0.1 = 1	Medium 50 x 0.1 = 5	Low 100 x 0.1 =10

h. Control Recommendation

Control recommendation is the stage of providing control recommendations resulting from the risk assessment process and providing recommendations for the risk reduction process in order to achieve an acceptable risk level [15].

i. Result Documentation

The risk assessment report is a report that can help senior management in making decisions regarding changes to policies, procedures, budgets, systems and management [20]. The risk assessment report consists of existing threats and weaknesses, risk measurements, and recommendations for implementing controls

.

4. CMMI (Capability Maturity Model Integration)

Capability Maturity Model Integration for Development (CMMI – DEV) is a framework or maturity model used to help organizations improve their performance and capabilities in developing and maintaining products and services [3]. Knowing the process weaknesses and maturity level of an organization, it is necessary to identify the process and map the organization's maturity level using the CMMI framework.

Table 4 Maturity Level Index

No	Range	***Maturity Level***
1.	0.0 – 1.50	*Initial*
2.	1.51 – 2.50	Managed
3.	2.51 – 3.50	Defined
4.	3.51 – 4.50	Quantitatively managed
5.	4.51 – 5.00	Optimizing

The process at maturity level 1 is usually ad hoc. The success of an organization at this level is based on the hard work and high competence of each person in it. Maturity level 2 shows that the process in the organization has been planned, implemented, measured and controlled well in accordance with organizational policies. Maturity level 3 explains the process is characterized and described in standards, procedures, tools and methods well and can be understood. Maturity level 4 is a process where organizations and projects set quantitative goals for process quality and performance and use them as criteria in managing the process. Maturity level 5 focuses on continuous process improvement through technological innovation.

III. METODOLOGY

The research flow is the steps of implementing research starting with an interest in knowing a particular phenomenon and then developing into ideas, theories, conceptualizations, selection of appropriate research methods, and so on. This research flow will be depicted in Figure 2.

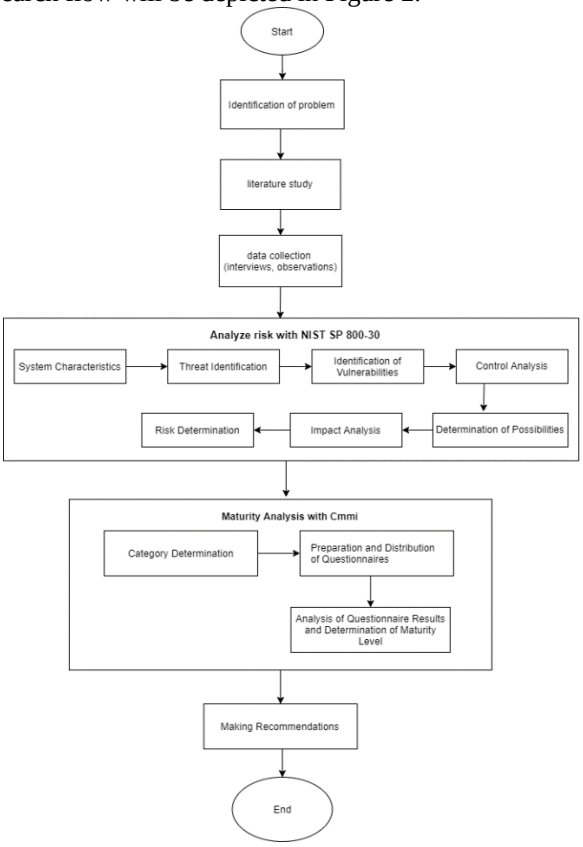

Figure 2. Research Flow

This research begins with identifying the problems that will be discussed in this research. The next stage is to conduct a literature study by looking for references through various sources, both from journals, the web and e-books to understand more deeply the use of the NIST SP 800-30 framework in conducting risk management evaluations and CMMI in determining the maturity level of the system being evaluated. The next stage is data collection by conducting interviews with the Head of the Badung Regency DPMPTSP Service and the head of IT staff who is responsible for the system and conducting direct observations at the case study location. The next stage is to analyze the risks in the licensing service system based on the stages of the NIST SP 800-30 framework according to the 9 stages of risk assessment. The next stage is to determine the category that is in accordance with the risk management evaluation based on NIST SP 800-53 revision 4. The categories used in this study are risk assessment and risk management. Each category has 6 sub-categories and each sub-category has several controls that regulate it. This control is used to compile the questionnaire

questions. The results of processing the questionnaire data will produce the current maturity level and target maturity level values in the system. so that recommendations for improvement will be obtained for the future. Furthermore, the values of the two maturity levels will be subtracted to obtain the gap value to assess the gap between the current level and the target level. After getting the gap, recommendations for improvement are given based on the NIST SP 800-53 revision 4 guidelines.

IV. RESULT

This study will identify risk assessments in the licensing service system and analyze the system maturity level.

1. System Characteristics

System Characterization includes information systems, including hardware, software, data and information, and human resources that support the information system. Hardware resources include PCs used for clients with application program software, Windows 10 Professional 64 bit as the operating system. While the software on the server uses Linux OS and PHP Programming Language. Data and information include infrastructure data, device data, server data and attacker data. There are several hardware used including 1 PC, 2 monitors, 2 servers, CCTV, LAN cables. For system development, each IT staff brings their own laptop.

2. Identification of Threats

At this stage, researchers identify threats based on their sources.

Table 5 Threats and Sources of Threats

No	Threats	Source of Threats
1.	Local viruses are not detected by antivirus	Virus
2.	Spread of viruses via flash disk	Virus
3.	There is no data loss notification	Loss or corruption of data
4.	Cyber attacks by hackers	cyber
5.	Staff make changes to the database outside of authority	Person in the agency
…		
45.	API security is still lacking	Technical

3. Vulnerability Identification

At this stage, the threat analysis to the system includes an analysis of weaknesses related to the licensing service system.

Table 6. Vulnerability Identification

No	Threats	Vulnerabillity
1.	Local viruses are not detected by antivirus	Hardware failure, no recoverable storage
2.	Spread of viruses via flash disk	No antivirus protection, autorun abuse
3.	There is no data loss notification	Not Having an Adequate Security Detection System
4.	Cyber attacks by hackers	Lack of security updates, no or insufficient software testing
5.	Staff make changes to the database outside of authority	Access rights are not managed properly, exploitation of access governance.
…		
45.	API security is still lacking	Data transmitted via the API is not encrypted, making it vulnerable to man-in-the-middle attacks.

4. Control Analysis

This stage aims to analyze existing controls that have been implemented or are being planned by the agency to minimize or eliminate the possibility of threats and weaknesses in the licensing service system.

Table 7 Control Analysis

No	Threats	Current Control	Control Plan
1.	Local viruses are not detected by antivirus	Update your antivirus regularly	Install a licensed antivirus
2.	Spread of viruses via flash disk	Make data backup	Make backups and prohibit the use of flash disks except those provided
3.	There is no data loss notification	There is no documentation done by the system	Backup data regularly
4.	Cyber attacks by hackers	Security monitoring for suspicious activity, enabling security log monitor	Perform software security testing
5.	Staff make changes to the database outside of authority	Set access rights appropriately	Prepare data recovery procedures to address unauthorized data loss.
…			
45.	API security is still lacking	All API communications are carried out over the HTTPS protocol to protect data during transmission.	Update API documentation with guidance on security, data validation, and proper usage.

5. Determination of Tendency

The results of analyzing the control analysis are used as a reference in determining the risk probability. There are three categories of probability levels, namely low, medium, high. The results of this determination show that there are 5 risks with a high probability level.

Table 8 *Likelihood Determination*

No	Threats	Possibility
1.	Local viruses are not detected by antivirus	Medium
2.	Spread of viruses via flash disk	Low
3.	There is no data loss notification	High
4.	Cyber attacks by hackers	Medium
5.	Staff make changes to the database outside of authority	High
…		
45.	API security is still lacking	Low

6. Impact Analysis

This stage is used to analyze the negative impacts of vulnerabilities exploited by threats. The output at this stage is the level of impact of weaknesses by threats along with a description of the impact.

Table 9 Impact Analysis Results

No	Threats	Impact
1.	Local viruses are not detected by antivirus	High
2.	Spread of viruses via flash disk	High
3.	There is no data loss notification	High
4.	Cyber attacks by hackers	High
5.	Staff make changes to the database outside of authority	Low
…		
45.	API security is still lacking	High

7. Risk Determination

Determination of the risk level is used to determine the level of risk in the system so that it can determine what actions need to be taken to reduce the risk. The likelihood and impact values given by IT staff will be multiplied according to the weighted values determined in the NIST SP 800-30 guidelines. The risk level assessment is obtained from the multiplication of the value of the likelihood level and the magnitude of the impact referring to the matrix table 3. Based on the results of the risk level assessment in the licensing service system, there are 4 high-level risks, 12 medium risks and 29 low risks. High-level risks include no notification of data loss, power outages, server down, and lack of server room security. The image below is a risk level assessment diagram based on percentage.

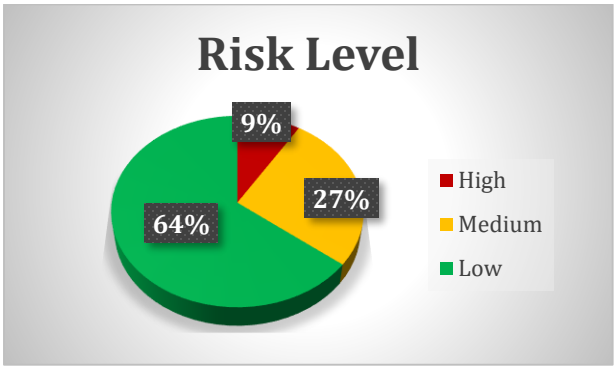

Figure 3 Risk Level

The picture above shows that the licensing system has 9 percent high risk, 27 percent medium risk and 64 percent low risk. red is a high risk level, orange is a medium risk level, and green is a low risk level.

8. Determination of Control and Preparation of Questionnaires

The preparation of questionnaire questions begins with determining the category that will be used as the basis for evaluating risk management. This is because there are many categories in NIST so it is necessary to determine the category that is appropriate to the research. This study chose the risk assessment and risk management categories which have 6 subcategories and 3 subcategories respectively. Each subcategory contains several NIST SP 800-53 controls that will be used as guidelines in preparing questionnaire questions that will be given to IT staff as system developers. The questionnaire used in this study consisted of 96 questions consisting of 88 questions for the risk assessment category and 8 questions for the risk management category. Respondents will be asked to choose 2 answers from each of the 5 (five) levels of choosing answers, namely from level 1-5 for the current maturity level and level 1-5 for the target maturity level and each question will represent the current maturity level and the target maturity level.

Table 10 Questionnare

Category	Question
ID-RA	
CA-2	what extent does the licensing system develop a security assessment plan that describes the scope of improving the system's security controls.
	Licensing systems have assessment procedures that will be used to determine the effectiveness of security controls.
	The system has an assessment team to carry out system security assessments.
CA-7	Develop and implement a continuous monitoring strategy on the system.
	The extent to which the organization determines the frequency of monitoring to assess control effectiveness
	Continuous assessment of the system in accordance with the continuous monitoring strategy.

Journal of Electrical, Electronics and Informatics, p-ISSN:2549-8304 e-ISSN:2622-0393

9. Assessment of Maturity Level of Licensing System

Based on the results of the questionnaire on the licensing service system, the average results of the current maturity level, target level and gap value were obtained. The table below is a detail of each level of each category.

Table 11 Maturity Level of Licensing Service System

Control	Current Level	Target Level	GAP
CA-2	2	3	1
CA-7	3	4	1
CA-8	2	3	1
RA-3	2	3	1
RA-5	2	3	1
SA-5	2	3	1
SA-11	2	3	1
SI-2	2	3	1
SI-4	3	4	1
SI-5	2	3	1
PM-15	2	3	1
PM-16	2	3	1
PM12	2	3	1
RA-2	2	3	1
PM-4	2	3	1
PM-9	2	3	1
PM-8	3	4	1
PM-11	2	3	1
SA-14	3	4	1

The table above is a breakdown of the current maturity level and target maturity level in the licensing service system based on the controls used in the risk assessment and risk management categories in NIST SP 800-53 revision 4. The table above shows that the gap between the current level and the target level for each control is 1, which means that an improvement plan is needed so that all control functions can reach the expected target level.

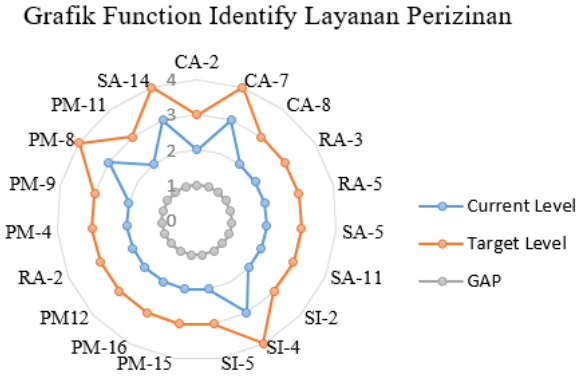

Figure 4 Function Graph of Licensing Service System

Figure 3 is a graphic mapping of the licensing service system based on the details of table 4.7. The blue line shows the current level, the orange line shows the target level and the gray line shows the gap from the maturity. The graph above helps to identify the functional aspects of the 19 controls in the risk assessment and risk management categories for future system improvements.10. Recommendations

Based on the results of the risk analysis and system maturity assessment obtained in the previous stage, the next stage is to prepare recommendations for improvements to minimize existing risk threats and increase the current maturity level to achieve the target maturity level in accordance with what is expected by the Badung Regency DPMPTSP. The following are recommendations for high-level risk threats based on the controls in the NIST SP 800-53 revision 4 guidelines shown in the table below.

Table 12 Risk Threat Recommendations

Threats	Recommendation
Local viruses are not detected by antivirus	Source: SI-4: System Monitoring 1. Install a Data Loss Prevention (DLP) solution to detect and alert if sensitive data is being accessed, transferred or changed unlawfully. 2. Prepare an incident response plan to recover lost data or ensure the cause is determined 3. Encrypt sensitive data both when stored (at rest) and when transmitted (in transit) to ensure data remains protected in the event of loss or theft
power outage	Source: CP-9: System Backup 1. Provide a backup generator with sufficient capacity to support critical operations for longer periods during power outages. 2. Install a power monitoring system that can provide early warning of power fluctuations or outages.
Server *down*	Source: SC-6: Resource Availability 1. Immediately carry out a backup of the SAP server to handle this risk. It is hoped that this recommendation can reduce the level of risk 2. Use server monitoring tools to detect performance issues, resource usage, and other anomalies that could cause a server to go down 3. Separate networks of different servers to reduce the risk that a problem on one server could spread to others.
The server room lacks security so data theft on the server can occur by outside/internal parties	Source: PE-2: Physical Access Authorizations 1. Use security doors with electronic access control systems, such as ID cards or biometrics (fingerprints, retina scans, facial recognition), to limit access to server rooms to authorized personnel. 2. Use a spare physical key in the form of a safe key, only hand it over to authorized personnel in an emergency, and make sure the key is not lost or misused.

The following are recommendations for improvement based on the results of the assessment of the maturity level of the licensing service system which aims to increase the maturity level of the system. These steps include technical, procedural, and strategic activities to achieve security goals.

Table 13 Recommendations for the Licensing Service System

Category	Current Level	Target Level	Recommendation
CA-2	2	3	1. Document a security assessment plan that includes the scope, objectives, schedule, and roles and responsibilities of each party involved. The plan must be updated regularly and adapted to the latest technological developments and security threats. 2. form a team equipped with special expertise in cyber security and information risk. providing regular training to improve the team's skills in identifying the latest threats and ensuring that they have sufficient knowledge of operating systems and security infrastructure.
CA-7	3	4	1. Ensure that ongoing assessments are carried out thoroughly using risk-based methods. Integrate internal and external audits periodically to assess whether security controls are still functioning effectively. 2. Use more detailed security performance indicators to evaluate the success of continuous monitoring strategies 3. Use a more advanced data integration platform to perform automatic correlation of multiple security data sources (logs, monitoring systems, incident reports).
….			
SA-14	3	4	1. Conduct criticality analysis on system components and functions to determine which components are most important for operational continuity. This will help in determining protection priorities.

V. CONCLUSION

Based on the results of the analysis of information security risk management evaluation using the NIST SP 800-30 framework, it shows that each system has a different level of risk influenced by the level of vulnerability and identified threats. The licensing service system has 4 high-level risks, 12 medium-level risks and 29 low-level risks. The assessment of the system maturity level using CMMI indicates that the gap of 19 controls in the risk assessment and risk management categories is 1. This means that the current system maturity level is still below the target maturity level so that the system requires improvement in the information security management process to achieve the desired level of maturity.

Recommendations designed using the NIST SP 800-53 revision 4 framework provide guidance to reduce the risk of high-level threats in the four systems by adjusting the identified threats with the controls available in NIST. In addition, recommendations to increase the maturity value are also aligned with the security standards set in the NIST control. Recommendations for improvement include strengthening access control, improving incident detection and response mechanisms, and sustainable vulnerability management. Implementation of these recommendations is expected to improve protection against information security risks and support operational efficiency of systems in government environments.

REFERENCES

[1] Anggi Elanda, D. T. (2018). Risk Management Analysis of Ids (Intrusion Detection System) Security System With NIST (National Institute Of Standards And Technology) Sp 800-30 Framework. (Case Study: Disinfolahtaau Mabes Tni AU). Journal of Informatics and Management STMIK.

[2] Anggi Elanda, R. L. (2021). Infrastructure Risk Management Analysis With NIST (National Institute of Standards and Technology) SP 800-30 Method (Case Study: STMIK Rosma). Scientific Journal of Electronics and Computers,.

[3] Arief Deswandi, B. H. (2020). Software Development Audit Using Capability Maturity Model Integration Level 3 Method. Informatics Journal, 148-155.

[4] Asyfi'na Shofiyal Izza, D. (2023). Geospatial Information Infrastructure Maturity Assessment Method for Local Governments in Indonesia Using Capability Maturity Model Integration (CMMI) and Geospatial Maturity Assessment Ordnance

Survey (GMA OS). Journal of Geospatial Information Science and Engineering, 38-46.

[5] Delpia Amanda, N. M. (2023). Analysis of Information Security Maturity Level Using NIST Cybersecurity Framework and CMMI. Journal of Computers and Applications, 291-302.

[6] Desak Made Novita, I. M. (2019). Knowing the Level of Application Maturity in IT Start-ups Using CMMI and TMMi Methods. MERPATI Journal.

[7] Dian Ayu Permatasari, W. H. (2019). Analysis of E-LKPJ Information System Risk Management at the Communication and Informatics Office of East Java Province. Journal of Information Technology Development and Computer Science, 6001-6008.

[8] Febriyanti Panjaitan, A. A. (2022). Network Security Risk Management Analysis Using the Nist Framework. Scientific Journal of Matrix.

[9] Hafizh Ghozie Afiansyah, A. A. (2022). Designing Information Technology Governance and Management Plans Using COBIT 2019 and NIST SP 800-53 Rev 5 (Case Study: ABC Government Agency). Jurnal Info Kripto.

[10] Hariani, D. W. (2020). Capability Maturity Model Integration (Cmmi) for Information Security Analysis Using the Apo13 Cobit 5 Domain at Pustipad Institution X. Jurnal Information System and Procesing.

[11] I G. N. M. Putra Eryawana, G. M. (2021). Information Security Risk Strategy at PT. X Using NIST SP 800-30. Jurnal Ilmiah Merpati.

[12] Ikrima Amanda Wulandari, A. D. (2019). Evaluation of Application Development Process Capability at the Malang City Communication and Informatics Office Using CMMI – DEV 1.3 Guidelines. Journal of Information Technology and Computer Science Development, 9579-9588.

[13] Kukuh Harsanto, D. H. (2018). Risk Management Information System Using the Mational Institute of Standards and Technology Framework in Educational Institutions. IPSIKOM JOURNAL.

[14] M. Rizeki Yuda Saputra, W. W. (2020). Evaluation of the Maturity Level of SPBE at the Banjar Regency Trade and Industry Office Using CMMI Dev. Version 1.3. Indonesian Journal of Business Intelligence.

[15] Mahardika, F. (2017). Information Security Risk Management Using the NIST SP 800-30 Revision 1 Framework (Case Study: STMIK Sumedang). Journal of IT Development (JPIT).

[16] Nur Fitrianti Fahrudin, A. N. (2022). Employee Data Security Risk Assessment in Information Systems Using the NIST Sp 800-30 Framework at PT. ABC. Applied Information Technology Scientific Journal (JITTER).

[17] Ranggi Praharaningtays Aji, M. M. (2021). Information System Risk Management at the Purwokerto Regional Library. Journal of Informatics Engineering and Information Systems, 261-272.

[18] Risma Damalia, A. A. (2021). Analysis of IT Risk Management of Retail Business Administration Systems Using the NIST SP 800-30 Method REVISION 1. Journal of Information Technology and Computer Science (INTECOMS).

[19] Rusydi Umara, I. R. (2019). Information System Security Analysis Based on the COBIT 5 Framework Using the Capability Maturity Model Integration (CMMI). Journal of Business Information Systems.

[20] Sandy, H. H. (2021). Security Audit and Risk Management in e-Learning at Sangga Buana University. Journal of Informatics Management (JAMIKA).

[21] Susilo. (2017). Analysis of the Risk Level of Information Technology Governance in Higher Education Using the National Institute of Standards & Technology (NIST) Special Publication 800-30 Framework Model and the IT General Control Questionnaire (ITGCQ) (Case Study of PTS. XYZ). Journal Industrial Servicess.

[22] Tony Tan, B. S. (2022). Cyber Attack Risk Management Using the NIST Cybersecurity Framework at ZXC University. Journal of Information System, Applied, Management, Accounting and Research (JISAMAR).

[23] Yuyun Juliasari, D. H. (2022). Analysis of Risk Management of Educator and Education Personnel Information Systems (SIMPATIKA) Using the NIST SP 800-30 Framework. Journal of the National Seminar on Research and Technology Innovation (SINARINT).