
Analysis of IT Risk Management on The Security of Data LMS and IT Resources Using NIST SP 800-30**Reska Nugroho Sudarto¹, Teguh Raharjo², Ni Wayan Trisnawaty³**reska.nugroho@ui.ac.id¹, teguhr2000@gmail.com², ni.wayan05@office.ui.ac.id³^{1,2,3} University of Indonesia

Article Information

Received : 20 Des 2024
Revised : 30 Des 2024
Accepted : 31 Des 2024

Keywords

Ministry of Law and Human Rights e-learning, NIST SP 800-30 Revision 1, IT risk management, information security, risk assessment

Abstract

Learning management systems (LMS) play a critical role in modern education by facilitating communication and access to learning resources for educators and students. However, these systems are susceptible to significant IT security threats due to the sensitive nature of the data they manage, including personal information and instructional materials. This study focuses on the Ministry of Law and Human Rights e-learning platform used by the Ministry of Law and Human Rights in Indonesia for distance learning and online training. Despite its benefits, the platform faces various IT security risks that could compromise its functionality and data integrity. Using the NIST SP 800-30 Revision 1 framework, this research identifies four primary operational risks—data security, password vulnerabilities, process inefficiencies, and exposure to cyberattacks—and analyzes their impact. The study then proposes comprehensive mitigation strategies to address these risks. The findings provide actionable recommendations for strengthening IT security and ensuring the continuity of business processes for ministry of law and human rights e-learning. These results highlight the importance of robust risk management in protecting sensitive information and enhancing the resilience of e-learning systems.

A. Introduction

Learning Management Systems (LMS) have become an essential tool in modern education, allowing teachers to create and manage online courses, assign and grade tasks, and track student progress. The LMS also serves as a platform for users to access learning materials, collaborate with peers, and communicate with instructors. Studies have shown that using Moodle can enhance students' independent work in foreign language learning, providing variability and flexibility in learning at an individual pace [1]. Nevertheless, LMS contains significant IT security flaws. The LMS stores sensitive data, including students' personal information, grades, and learning materials, making it a prime target for hackers. A data breach in an LMS can have serious consequences, such as identity theft, financial fraud, and reputational damage.

Today's organizations/agencies flourish in a complicated, uncertain, and constantly changing environment. The Human Resource Development Agency of the Ministry of Law and Human Rights, as a stakeholder in human resource development at the Ministry of Law and Human Rights as known as human resource development agency Law and Human Rights, must deal with an increasing number of hazards. As a result, BPSDM Law and Human Rights created a distance learning application. Given the 'increasingly unpredictable' world, all institutions must create a risk management system that can identify, assess, and manage actual and potential hazards.

The Human Resource Development Agency of the Ministry of Law and Human Rights uses Moodle as its e-learning platform; this LMS is designed for distance learning and online training users. E-Learning Ministry of Law and Human Rights can be accessible using a browser. To access this learning system, the user must have a computer, laptop, or smartphone linked to the internet. E-learning has numerous benefits; thus, its presence is critical due to time and cost savings. Furthermore, online learning may be done anywhere and anytime, eliminating the need to study in a classroom. There are numerous benefits to e-learning, but there are also some drawbacks and risks.

The Ministry of Law and Human Rights e-learning platform serves as a dynamic distance learning center. The platform enables Ministry of Law and Human Rights employees to access a range of training materials, participate in online courses, and engage with instructors through virtual interaction. The learning mechanism employs the use of digital modules, video tutorials, interactive quizzes, and discussion forums, which facilitate flexible learning at the individual's own pace. In this context, the significance of IT risk management cannot be overstated. Ensuring the security of participant data, maintaining system integrity, and ensuring service continuity are of paramount importance. By implementing comprehensive security measures, the Ministry of Law and Human Rights e-learning platform can continue to operate optimally and provide maximum benefits to its users.

The Ministry of Law and Human Rights e-learning platform is susceptible to a multitude of risks that have the potential to impede its optimal functioning. Operational risks that frequently emerge include access disruptions resulting from network or server complications, system failures attributable to software defects or configuration inconsistencies, and data loss due to cyber-attacks or human

error. To illustrate, in 2022, the platform was subjected to pervasive access disruptions as a consequence of a DDoS attack, which resulted in the cessation of the learning process for a period of several hours. Furthermore, it is imperative to recognize the potential for a security breach of participants' personal data, which could have a significant adverse impact on the institution's reputation. To guarantee the sustainability and security of the platform, Ministry of Law and Human Rights must implement a comprehensive risk management system, comprising regular risk assessments, the formulation of mitigation plans, and the execution of periodic system tests.

The Ministry of Law and Human Rights is confronted with a significant challenge in the form of an increasing prevalence of sophisticated and organized cyber-attacks. Additionally, the limited budgetary resources and the lack of qualified human capital in the cybersecurity domain impede the Ministry of Law and Human Rights ability to safeguard its e-learning system. Furthermore, the integration of the e-learning system with other information systems within the Ministry of Law and Human Rights introduces an elevated risk of cybersecurity breaches.

Emphasizes the importance of a process-oriented framework, drawing on principles from quality management [2]. Various approaches to analyzing information security risk management include Mehari, Megarit, Microsoft's Security Management Guide, and the National Institute of Standards and Technology (NIST). The NIST 800-30 technique outperforms the others since it can provide control recommendations [3]. In this study, many stages are carried out that use the NIST 800-30 framework to evaluate information security risk management in the Ministry of Law and Human Rights e-learning application.

B. Research Method

2.1. Research Stages

Research stages refer to a systematic sequence to ensure a structured and valid research process. These stages help researchers address their objectives effectively and produce results that contribute to the academic or practical knowledge base. The research process employed in this study consists of six interconnected stages: data collection, literature study, interviews, analysis, recommendations, and conclusion, as shown in Figure 1.

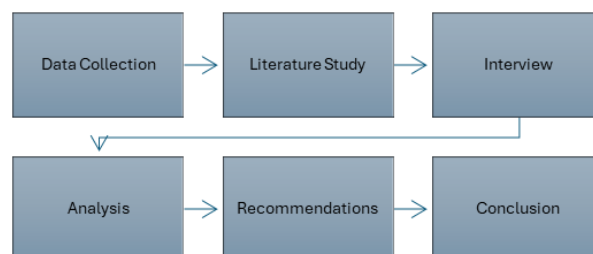


Figure 1. Research stages

The process begins with collecting relevant information from various sources to establish a foundational understanding of the research topic. This process is followed by a literature study, which involves a comprehensive review of existing

research to identify knowledge gaps, build a theoretical framework, and align the study with prior academic work. Subsequently, interviews with key stakeholders or experts are conducted to obtain in-depth insights that complement the findings from the literature study.

The collected data is then subjected to systematic analysis, utilizing appropriate methods such as statistical techniques for quantitative data and thematic analysis for qualitative data. Based on the analysis, actionable recommendations are formulated to address the research objectives and provide practical solutions or strategies. The process concludes with a synthesis of the findings as a conclusion, which summarizes the study's contributions, implications, and suggestions for future research. An iterative feedback loop ensures that insights gained during later stages can refine earlier phases, enhancing the overall validity and reliability of the research outcomes.

2.2. Literature Study

Obtaining information on current issues in the e-learning Ministry of Law and Human Rights system and data on potential dangers that have occurred and can affect ongoing processes - for this research through responses to questions and face-to-face meetings between the head of the information systems division and the employees who help manage the system.

2.3. Interview

The data was gathered from various sources, including books, journals, and the internet, focusing on information technology risk management using the NIST 800-30 Revision 1 technique. Additionally, the application of risk management standards was examined. "To gain further insight, the study interviewed operators responsible for the LMS server and users of the LMS application.

2.4. Analysis

NIST is an agency of government in the United States that develops and promotes evaluations, standards, and technologies for enhanced facilities and quality of life [4]. Its primary purpose is to conduct research on numerous disciplines in order to promote and strengthen technical infrastructure. NIST provided guidelines in its standard publication 800-30 Revision 1 on Guideline for Conduct Risk Evaluations. The application of NIST SP 800-30 to the Ministry of Law and Human Rights e-learning platform provides a systematic framework for identifying, analyzing and managing information security risks. The process begins with identifying existing systems, threats and vulnerabilities. Then, the security controls already implemented are evaluated. An impact and probability analysis is performed to determine the level of risk. In Ministry of Law and Human Rights e-learning, the risk of SQL injection attacks can threaten the leakage of participants' personal data. By understanding these risks, the Ministry can implement appropriate mitigation measures, such as strengthening network security and conducting user security training. Through the implementation of NIST SP 800-30, Ministry of Law and Human Rights can protect its digital assets, maintain data integrity, and ensure the sustainability of e-learning services.

2.4.1. Conduct The Assessment

2.4.1.1 Identifying Threat Sources

Identify and explain threat sources in the e-learning system, such as targeting characteristics for hostile threats and varied impacts for non-hostile threats [5].

2.4.1.2 Threat event (Threat Event Identification)

Threat events are identified from the results of interviews and observations. Possible risk events will be obtained after interviews and observations in the e-department. Emphasizes the significance of a specialized framework for university networks, employing semi-structured interviews and experimental data collecting to evaluate network vulnerabilities [6].

2.4.1.3 Vulnerabilities

In this stage, various weaknesses or shortcomings of the e-learning Ministry of Law and Human Rights system allow threats to occur. Learning system that allows threats to the system [7]. Input from attacks that have occurred, from the results of checking/testing the system, and from the resulting process a list of vulnerabilities or vulnerabilities that allow risks to be attacked.

2.4.1.4 Likelihood

The likelihood, or probability, is one of the key elements in project risk management. This key raises the possibility of another risk occurring. Likelihood level is divided into five categories: very high, high, moderate, low, and very low.

2.4.1.5 Impact

The impact analysis step will describe how the risks will damage the system's mission, and the data processed on the Ministry of Law and Human Rights e-learning system will result in a definition of the impact of these risks.

2.4.1.6 Risk Determination

This risk determination tries to measure the amount of risk to the system. To assess this level of risk, consider the possibility of risk and the risk impact as determined by the NIST SP 800-30 Revision 1 approach.

To ensure valid and reliable risk assessment results, it is necessary to maintain the quality of the data collected. In the process, data triangulation can be one of the effective techniques. data from interviews with IT officers is triangulated with data obtained from system logs and security policy documents.

C. Result and Discussion

3.1 Asset Identification

Each asset should have a designated asset owner responsible and accountable for it. The asset does not own the asset but is responsible for its creation, development, maintenance, use, and adequate security. The asset owner is often the best individual to determine the asset's value to the company. Key assets comprise processes and information essential to the operations in question. Other essential assets, such as organizational processes, may be considered when designing information security policies or service continuity plans. Table 1 shows some of the assets included in the Ministry of Law and Human Rights e-learning program. All assets are located in the data center managed by data center and information technology.












Table 1. Asset identification







Asset	Asset Type	Person in Charge	Specification	Asset Location
Cisco	Supporting assets	Data and network division of data center and information technology	Vcpu: 8 RAM: 16GB Storage: 5000 GB	Data Center and Information Technology
Cisco	Supporting assets	Data and network division of data center and information technology	Vcpu: 8 RAM: 16GB Storage: 5000 GB	Data Center and Information Technology
Cisco Software Define Network	Supporting assets	Data and network division of data center and information technology	Cisco Software Define Network	Data Center and Information Technology

3.2 Threat Sources (Identification of Threat Sources)

Identify and explain threat sources in the online educational system, including hostile threat characteristics and non-hostile threat impacts, as shown in Table 2.

Table 2. Threat identification

No.	Identification	Threat Source	Risk Level
1	Ministry of Law and Human Rights E-learning	<p>Improper system operation that causes the system to crash</p> <p>Data theft (password) of the e-learning application that can access personal data profiles.</p> <p>Data management errors by staff or lecturers</p> <p>Errors in data management by staff or lecturers</p> <p>Occurrence of malware or virus attacks caused by external parties</p> <p>Exploitation of security vulnerabilities in the e-learning application by internal or external parties.</p> <p>Loss of sensitive data.</p>	 HIGH  HIGH  VERY HIGH  MODERATE  MODERATE  MODERATE  VERY HIGH  Moderate
2	Ubuntu Server	<p>Operational errors caused by IT staff</p> <p>Software vulnerabilities: Ubuntu Server, like other operating systems, is prone to software vulnerabilities that hackers can exploit to gain access to the server or LMS data</p>	 HIGH
3	Cisco Vcpu: 8 RAM: 16GB Storage: 5000 GB	<p>Database Server</p> <p>Storage Server</p> <p>Application and database servers do not have standard security configurations.</p> <p>Using weak passwords or using default passwords</p>	 VERY HIGH  MODERATE

No.	Identification	Threat Source	Risk Level
4	Cisco Vcpu: 8 RAM: 16GB Storage: 5000 GB	OS Server	Not running correctly (Pirated) 
		Database Server	Application and database servers do not have standard security configurations. 
		Storage Server	Using weak passwords or using default passwords 
		OS Server	Not running correctly (Pirated) 
5	Cisco Software Define Network	A poor password uses a standard password. Hackers might attack the router and gain control of the network.	
			

3.3 Threat Event Identification





Risk assessment methodologies for cybersecurity face challenges due to the dynamic nature of cyber systems and their complex network structures [8]. A more rigorous analysis is required to enhance the efficacy of risk assessment. This condition necessitates a more profound examination of the implications of specific threats, the motives underlying attacks, and the most effective mitigation strategies.










Organizations can prioritize their efforts and optimally allocate resources by analyzing the potential impact of threats. Furthermore, Regular risk assessments are crucial due to rapid technological advancements and adaptations. The risk management process should consider various risk types, including operational, financial, regulatory, and technological [9]. A proactive approach to risk management, coupled with a robust security culture, can assist organizations in mitigating risks and safeguarding their valuable assets.

3.4 Vulnerabilities

At this point, several flaws or deficiencies in the Ministry of Law and Human Rights E-learning e-learning system enable threats to materialize. Input from previous assaults, the results of system testing, and the resultant processes a list of vulnerabilities or weaknesses that allow risks to attack. In the remainder of Table 3.

Table 3. Vulnerabilities

No	Identification	Vulnerability	Level
1	Ministry of Law and Human Rights E-learning Management System Application	Delay in upgrading antivirus software, allowing malware viruses to penetrate the system.	
		Staff bringing laptops to work increases the chance of stealing sensitive information or viruses.	
		Negligence and delay in staff handling information materials	
		Users use default passwords, leaving them exposed to password theft.	

No	Identification	Vulnerability	Level
		No upgrade is utilized for the programming language or database version, which leads to decreased security.	 MODERATE
		There is no backup system for database security, which can lead to critical data loss.	 VERY HIGH
		The enormous number of students and inadequate staff resources can cause problems in student grade management.	 VERY HIGH
2	Ubuntu Server	The antivirus software is not up-to-date on computers or pirated operating systems.	 HIGH
3	Cisco Vcpu: 8 RAM: 16GB Storage: 5000 GB	The application and database servers do not have a standard security configuration.	 VERY HIGH
		Unstable server room temperature.	 MODERATE
4	Cisco Vcpu: 8 RAM: 16GB Storage: 5000 GB	Inadequate protection in the data centre allows strangers to take the server.	 MODERATE
		The application and database servers do not have a standard security configuration.	 VERY HIGH
5	cisco Software Define Network	The network that is connected to that device is having trouble.	 HIGH













3.5 Likelihood

























Used to obtain the likelihood value that may occur, the likelihood level is divided into three categories, namely [10]:

- High-threat sources with high motivation can harm the organization because controls to prevent vulnerabilities are ineffective.
- Medium threat sources be motivated that can harm the organization, but the organization can still carry out controls that can hinder the success of existing vulnerabilities.
- Low-threat sources that have less, or low motivation controls are used to prevent or reduce vulnerability.

Used to prevent or reduce vulnerability in the organization, as shown in Table 4.

Table 4. Identifying of Potentially Risk






No.	Risk	The Possibility that a Threat Event Will Occur, Resulting in	Negative Impact	Overall Chance
1	Loss of sensitive data.	 LOW	 VERY HIGH	 MODERATE
2	System operations that force the system to cease.	 LOW	 VERY HIGH	 MODERATE
3	Stealing passwords in e-learning programs, as well as errors in data	 LOW	 VERY HIGH	 MODERATE
4	input by staff or teachers might compromise user profiles.	 MODERATE	 VERY HIGH	 HIGH








No.	Risk	The Possibility that a Threat Event Will Occur, Resulting in	Negative Impact	Overall Chance
5	Voltage disturbance.			
6	IT staff, operational failures,			
7	malware or virus attacks from both within and outside parties,			
8	asset destruction due to age or damage.			
9	errors in deploying e-learning software.			
10	Both internal and external parties can exploit security flaws in e-learning applications.			
11	Natural disasters such as floods, fires, and earthquakes can harm all assets significantly.			
12	The network interruption			

3.6 Impact

The impact analysis stage will describe how the risk will influence the system's mission, and the data processed on the e-learning system will produce the form of The system mission and data processed on the Ministry of Law and Human Rights E-learning e-learning learning system will yield a definition of the impact of these hazards [11], as shown in Table 5.

Table 5. Impact Identification

No.	Risk	Description	Maximum Impact	Risk Code
1	Loss of sensitive data.	The impact is powerful because it contains sensitive data that impact accreditation.		R1
2	System operations that force the system to cease.	Web pages cannot be accessed, and the service process is not running.		R2
3	Theft (password) of e-learning programs with access to personal profiles or data	Because learning outcomes are applied via Ministry of Law and Human Rights e-learning , there will be issues with questions and answer keys or personal information theft.		R3
4	A large volume of participant score data, inaccuracies in data entry by staff or teachers	The impact is significant since it can influence the evaluation of participants.		R4
5	Voltage disturbance.	The impact is moderate because it may create system problems and errors when restarted.		R5






















No.	Risk	Description	Maximum Impact	Risk Code
6	Operational failures created by its employees	Configuring mistakes in e-learning activity		R6
7	Malware or virus attacks caused by external/internal parties	The impact of a virus on the server is significant because it can force the system to shut down.		R7
8	Damage to ageing or damaged assets.	The impact is high due to the issues with the server.		R8
9	Errors in deploying e-learning apps	Some functionalities might not be responding.		R9
10	Exploiting security flaws in e-learning applications by both internal and external parties	The impact is significant because it demands a team of colleagues to correct the program's errors.		R10
11	Natural disasters (such as floods, fires, and earthquakes) can cause harm to all assets.	The consequences are severe since the system may shut down altogether, losing all sensitive data.		R11
12	Network interruptions	The impact is moderate. Internet access connections will cause connection troubles, affecting the Ministry of Law and Human Rights e-learning system.		R12
















3.7 Risk Determination

The NIST SP 800-30 method determines the possibility of risk and risk impact to assess this risk level. Each of these factors is assigned as follows.

- The impact that will result from the event
- The likelihood of the event occurring.

Table 6. Risk Determination

No	Threats	Description	Maximum Impact	Risk
1	Loss of sensitive data.			
2	System operations that force the system to cease.			
3	Stealing passwords in e-learning programs, as well as errors in data input by staff or teachers might compromise user profiles.			
4	Voltage disturbance.			
5	IT staff operational failures,			
6	malware or virus attacks from both within and outside parties,			
7				

No	Threats	Description	Maximum Impact	Risk
8	asset destruction due to age or damage.	 MODERATE	 HIGH	 MODERATE
9	errors in deploying e-learning software.	 MODERATE	 HIGH	 MODERATE
10	Both internal and external parties can exploit security flaws in e-learning applications.	 MODERATE	 HIGH	 MODERATE
11	natural disasters such as floods, fires, and earthquakes can harm all assets significantly.	 LOW	 VERY HIGH	 MODERATE
12	The network interruption	 MODERATE	 HIGH	 MODERATE

D. Conclusion

This research has significantly contributed to the field of IT risk management, particularly in the context of Learning Management Systems (LMS). By applying the NIST SP 800-30 Revision 1 framework, we have conducted a comprehensive assessment of the Ministry of Law and Human Rights E-learning platform, identifying and analyzing 12 critical information security risks. This systematic approach has provided a deeper understanding of the potential threats and vulnerabilities that could compromise the platform's security and integrity.

The findings of this study highlight the importance of a robust risk management framework in ensuring the security and reliability of LMS platforms. By following the guidelines outlined in NIST SP 800-30, organizations can effectively identify, assess, and mitigate risks, thereby protecting sensitive information and minimizing the potential impact of security breaches.

The application of NIST SP 800-30 in this research has demonstrated its value as a practical and effective tool for managing IT risks in complex environments. By adopting the recommended control measures, Ministry of Law and Human Rights E-learning can enhance its security posture and safeguard the interests of its users.

E. Acknowledgment

Financial support from Indonesia's Ministry of Communication and Information Technology made this research publication possible.

F. References

- [1] I. Hontarenko, "Students' Independent Work in Studying Foreign Language based on LMS MOODLE," *Educ. Challenges*, vol. 27, no. 2, pp. 66–78, 2022.
- [2] R. D. Pambudi and K. Ramli, "Information Security Risk Management Design of Supervision Management Information System At Xyz Ministry Using Nist Sp 800-30," *J. Tek. Inform.*, vol. 4, no. 3, pp. 591–599, 2023.
- [3] A. A. Putro, A. Ambarwati, and E. Setiawan, "Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1," *J. Teknol. dan Inf.*, vol. 11, no. 2, pp. 125–136, 2021.
- [4] A. Elanda and D. Tjahjadi, "Analisis Manajemen Resiko Sistem Keamanan IDS (Intrusion Detection System) dengan Framework NIST (National Institute Of

- Standards And Technology) SP 800-30 (Studi Kasus DISINFOLAHTAAU Mabes TNI AU),” *Infoman’s*, vol. 12, pp. 1–13, May 2018.
- [5] S. Patomviriyavong, B. Samphanwattanachai, and T. Suwannoi, “eLearning operational risk assessment and management: A case study of the M. Sc in management program,” *Int. J. Comput. Internet Manag.*, vol. 14, pp. 44.1-44.5, 2006.
- [6] N. Awang, G. A. L. N. Samy, and N. H. B. Hassan, “Treat Assessment Framework in Analysing Network Threat Occurrence,” *8th Int. Conf. Recent Adv. Innov. Eng. Empower. Comput. Anal. Eng. Through Digit. Innov. ICRAIE 2023*, vol. 2023, pp. 1–6, 2023.
- [7] M. M. Hanafi, “Modul Risiko, Proses Manajemen Risiko, dan Enterprise Risk Management,” *Univ. Terbuka*, pp. 1–40, 2016.
- [8] A. A. Ganin *et al.*, “Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management,” *Risk Anal.*, vol. 40, no. 1, pp. 183–199, 2020.
- [9] J. Piper, “Risk management applications for disruptive technologies,” in *Proc.SPIE*, 2021, vol. 11751, p. 117510N.
- [10] M. M. Alhassan and A. Adjei-Quaye, “Information Security in an Organization,” *Int. J. Comput.*, no. January, 2017.
- [11] G. De Montpellier, “E-Learning Concepts , Trends , Applications,” *Exp. Psychol. Its Scope Method Iv Learn. Mem.*, pp. 51–136, 2014.