Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th February 2026. Vol. 5. No. 2; e-ISSN: 2808-4519

Information System Security Risk Analysis Using the Annual Loss Expectancy (ALE) Method (Case Study: Website of the Information Systems Department, UPN "Veteran" Jawa Timur)

Indi Ariyanti Sardi[1]*, Rania Nurbaity Winarno[2], Riska Febriana Rahmawati[3]
Agung Brastama Putra[4], Rizka Hadiwiyanti[5], Amalia Anjani Arifiyanti[6]

[1, 2, 3,4,5,6]*Universitas Pembangunan Nasional "Veteran" Jawa Timur*
indiariyanti04@gmail.com[1*], 23082010134@student.upnjatim.ac.id[2], riskafebriana132@gmail.com[3],
agungbp.si@upnjatim.ac.id [4], rizkahadiwiyanti.si@upnjatim.ac.id [5],Amalia_anjani.fik@upnjatim.ac.id[6]

Abstract

The development of information technology in higher education institutions poses significant security risks to digital assets, including the Department of Information Systems website at UPN "Veteran" Jawa Timur. This study aims to identify, analyze, and evaluate information security risks using the quantitative Annual Loss Expectancy (ALE) method. This method measures risk based on the parameters of Asset Value (AV), Exposure Factor (EF), and Annualized Rate of Occurrence (ARO). The analysis was conducted on four main risk categories: service disruption, device damage, data loss, and system security threats. The results of the study show that information system security threats have the highest potential loss of IDR 81,750,000 per year. After simulating mitigation measures, the annual loss value (ALE Projected) decreased dramatically in all categories. The investment feasibility evaluation using Return on Investment (ROI) resulted in a ratio above 2:1 for all categories, with the highest value of 3.10 in handling security threats. This shows that the proposed security investment is very feasible to implement in order to ensure the continuity of academic services and protect the department's information assets.

Keywords: *Annual Loss Expectancy (ALE), Information Security, Return on Investment (ROI), Risk Analysis, Web Information System*

1. Introduction

The development of information technology has encouraged universities to adopt web-based information systems to support academic and administrative activities[1]. One form of application of this technology is the Department Information System, which is used to manage academic data such as student data, lecturer data, lecture schedules, and other supporting information. This system plays an important role in supporting the smooth running of academic processes within the department.

However, the use of web-based information systems also presents various information security risks, such as service disruptions, data leaks, malware attacks, and system damage due to technical and non-technical factors [2]. These risks can result in disrupted academic services, loss of important data, and decreased user confidence in the information system. Similar research found 26 security risks in university information systems, with 4 medium-level risks requiring mitigation priority [3]. Therefore, efforts are needed to identify and analyze information security risks in a systematic and measurable manner [4].

One quantitative approach to analyzing information system security risks is Annual Loss Expectancy (ALE), which is recognized as a standard method in ISRA based on the latest SLR[5]. This method involves several parameters, such as asset value, exposure factor, and annualized rate of occurrence, so that the results of the analysis can be used as a basis for decision making in determining risk mitigation measures [6].

Based on this background, this study aims to analyze information system security risks using the Annual Loss Expectancy (ALE) method with a case study on the Information Systems Department website of UPN "Veteran" Jawa Timur. The results of this study are expected to provide an overview of the level of risk and recommendations for effective system security measures to reduce the vulnerability of information security threats [7].

2. Basic Theories

Risk management is a process carried out to reduce the possibility of risks occurring and minimize the impact of losses that may be incurred on organizational assets[8]. In the context of information system security, risk management aims to protect information assets from various threats that can compromise the confidentiality, integrity, and availability of information.

Each possible risk has a different level of impact and probability. Therefore, certain parameters are needed to determine the severity of the risk [9]. In general, risk can be analyzed through two approaches, namely qualitative analysis and quantitative analysis. Qualitative analysis assesses risk based on categories or levels (such as low, medium, and high), while quantitative analysis measures risk based on numerical values, particularly in financial units [10]. Examples are as follows:

Table 1: Adjective table (assumed value).[1]

ALE (Annualized Rate of Occurrence)	Financial Value
Very Low	More than £1,000
Low	£1,000 - £ 10,000
Low/Medium	£10,000 - £50,000
Medium	£ 50,000 - £100,000
Medium/High	£100,000 - £500,000
High	500,000 - £1,000,000

Quantitative ALE risk analysis uses impact and probability parameters, although probability estimates are subjective, as evaluated in the ISRA study [5]. These parameters are then used to derive the Single Loss Expectancy (SLE) value. SLE represents an estimate of the amount of financial loss that would be incurred if a disaster occurred once.

The Annualized Rate of Occurrence (ARO) is an estimate of the frequency with which a risk may occur in a year [11]. For example, if a risk occurs once in 10 years, the ARO value is 0.1. Exposure Factor (EF) is the percentage of asset loss caused by threat identification, with a value range of 0% to 100% [12]. This quantitative approach is in line with risk analysis using ISO 27005, which identifies and mitigates threats to information assets [13]. Then, Asset Value (AV) describes the value of assets in monetary or financial units. The assets in question include all components, both tangible and intangible, that play a role in supporting the continuity of organizational activities [14]. Based on these parameters, the Single Loss Expectancy (SLE) value is formulated as follows:

$$SLE = AV \times EF$$

Furthermore, the relationship between SLE and Annual Loss Expectancy (ALE) is expressed by the following equation [15]:

$$ALE = SLE \times ARO$$

Return on Investment (ROI) is the ratio between the benefits or value obtained from an investment and the total costs incurred. In the context of information security risk analysis, ROI is used as a basis for decision-making to determine the feasibility of implementing risk control measures [11. Return on Investment (ROI) = (ALEcurrent - ALEprojected) / Annual Cost An investment is considered feasible if ≥ 2:1, consistent with the analysis that ROI becomes a 'guide on whether the action is feasible to implement' after calculating ALE [16] Mathematically, the ROI value is formulated as follows:

$$ROI = (ALE_{current} - ALE_{projected}) / \text{Annual Cost Investment}$$

The ALEcurrent value is an estimate of annual losses before risk mitigation measures are implemented, while ALEprojected shows the estimated annual losses after risk control measures are implemented.

3. Analysis

The author conducted a risk analysis using a case study of the Information Systems Department website at UPN "Veteran" East Java. This system is used as a medium for delivering academic and non-academic information, supported by network infrastructure and servers that support its operations. The table of adjectives used to estimate ALE for the Information Systems Department website of UPN "Veteran" Jawa Timur is as follows:

Table 2: Table of ALE estimation adjectives for the Information Systems Department website of UPN "Veteran" Jawa Timur

ALE (Annualized Rate of Occurrence)	Financial Value (IDR)
Very Low	0 – 5.000.000
Low	5.000.000 – 25.000.000
Low / Medium	25.000.000 – 75.000.000
Medium	75.000.000 – 150.000.000
Medium / High	150.000.000 – 300.000.000
High	> 300.000.000

The assets analyzed on the UPN "Veteran" Jawa Timur Information Systems Department website consist of hardware, software, data, and supporting system infrastructure. Based on the results of the asset identification, the author then conducted a risk analysis to estimate the potential annual losses that might occur.

The ALE value estimates were grouped based on the likelihood of risks that could occur, such as system service disruptions, device damage, data loss, and information security threats. From the ALE calculation results, the Return on Investment (ROI) value was then calculated to determine whether the proposed risk management measures were feasible and appropriate to implement [17].

3.1. Service Disruption

It is estimated that there will be 6 service disruptions in 1 year on the UPN "Veteran" Jawa Timur Information Systems Department website. These service disruptions can be caused by server overload [18], system configuration errors, or internet network disruptions, which result in users being unable to access the information system. The ARO (Annual Rate of Occurrence) value used is 6/1 = 6.

Table 3: Table ALEcurrent for service disruption risk

No.	Item	Total	Unit Value (IDR)	Total Value (IDR)	Classification	EF (%)	SLE (IDR)	ARO	$ALE_{current}$ (IDR)
1.	Server	1	15.000.000	15.000.000	System	20	3.000.000	6	18.000.000
2.	Router	1	5.000.000	5.000.000	Network	15	750.000	6	4.500.000
3.	Switch	2	3.000.000	6.000.000	Network	15	900.000	6	5.400.000
4.	Database System	1	20.000.000	20.000.000	Data	10	2.000.000	6	12.000.000
5.	Web Application	1	10.000.000	10.000.000	Application	10	1.000.000	6	6.000.000
Total annual losses									45.900.000

Measures taken to reduce the risk of service disruption (Annual Cost Investment):

Table 4: Handling service interruption risks

No.	Handling Actions	Cost (IDR)
1.	Upgrade internet bandwidth	8.000.000
2.	Server monitoring implementation	5.000.000
3.	Periodic system and network maintenance	6.000.000
4.	Automatic system and database backup	4.000.000
Total		23.000.000

After implementing risk management measures, it is estimated that the level of service disruption can be reduced so that the ARO value decreases to twice a year.

Table 5: Table ALE projected for service disruption risk

No.	Item	Total Value (IDR)	EF (%)	SLE (IDR)	ARO	$ALE_{projected}$ (IDR)
1.	Server	15.000.000	10	1.500.000	2	3.000.000
2.	Router	5.000.000	5	250.000	2	500.000
3.	Switch	6.000.000	5	300.000	2	600.000
4.	Database System	20.000.000	5	1.000.000	2	2.000.000
5.	Web Application	10.000.000	5	500.000	2	1.000.000
Total annual losses						7.100.000

So, from the data above, we get the ROI value: (45,900,000 – 7,100,000) / 23,000,000 = 1.68 ≈ 2 : 1

3.2. Device Damage

It is estimated that there will be 4 device failures in 1 year at the Information Systems Department website of UPN "Veteran" Jawa Timur. These device failures can be caused by the age of the devices, overheating, power surges, or misuse. The impact of this risk is disruption to information system operations and a decline in service performance. The ARO (Annual Rate of Occurrence) value used is 4/1 = 4..

Table 6: Table ALEcurrent for device damage risk

No	Item	Total	Unit Value (IDR)	Total Value (IDR)	Classification	EF (%)	SLE (IDR)	ARO	$ALE_{current}$ (IDR)
1.	Server	1	15.000.000	15.000.000	System	30	4.500.000	4	18.000.000
2.	Router	1	5.000.000	5.000.000	Network	25	1.250.000	4	5.000.000
3.	Switch	2	3.000.000	6.000.000	Network	25	1.500.000	4	6.000.000
4.	Harddisk Server	2	2.500.000	5.000.000	Hardware	40	2.000.000	4	8.000.000
5.	Power Supply	1	2.000.000	2.000.000	Hardware	30	600.000	4	2.400.000
Total annual losses									39.400.000

Measures taken to reduce the risk of Device Damage (Annual Cost Investment):

Table 7: Handling the risk of device damage

No.	Handling Actions	Cost (IDR)
1.	Procurement of UPS and electrical stabilizers	6.000.000
2.	Periodic hardware maintenance	5.000.000
3.	Gradual replacement of obsolete equipment	7.000.000
4.	Provision of spare parts	4.000.000
	Total	22.000.000

After implementing risk management measures, it is estimated that the frequency of device damage can be reduced so that the ARO value decreases to once per year, and the level of impact of losses is also reduced.

Table 8: Table ALE projected for device damage risk

No.	Item	Total Value (IDR)	EF (%)	SLE (IDR)	ARO	$ALE_{projected}$ (IDR)
1.	Server	15.000.000	15	2.250.000	1	2.250.000
2.	Router	5.000.000	10	500.000	1	500.000
3.	Switch	6.000.000	10	600.000	1	600.000
4.	Harddisk Server	5.000.000	15	750.000	1	750.000
5.	Power Supply	2.000.000	10	200.000	1	200.000
	Total annual losses					4.300.000

So, from the data above, we get the ROI value: (39,400,000 – 4,300,000) / 22,000,000 = 1.60 ≈ 2 : 1

3.3. Data Loss

It is estimated that within one year, there will be two incidents of data loss on the UPN "Veteran" Jawa Timur Information Systems Department website. This data loss can be caused by storage device failure, human error, malware attacks, or backup processes that do not run properly [19]. This risk results in the loss of important system data, such as user data, website content data, and system configurations. The ARO (Annual Rate of Occurrence) value used is 2/1 = 2.

Table 9: Table ALEcurrent for data loss risk

No.	Item	Total	Unit Value (IDR)	Total Value (IDR)	Classification	EF (%)	SLE (IDR)	ARO	$ALE_{current}$ (IDR)
1.	Server	1	15.000.000	15.000.000	System	30	4.500.000	2	9.000.000
2.	Harddisk Server	1	2.500.000	5.000.000	Hardware	40	2.000.000	2	4.000.000
4.	Database System	1	20.000.000	20.000.000	Data	50	10.000.000	2	20.000.000
5.	Web Application	1	10.000.000	10.000.000	Application	20	2.000.000	2	4.000.000
	Total annual losses								37.000.000

Measures taken to reduce the risk of data loss (Annual Cost Investment):

Table 10: Data loss risk management

No.	Handling Actions	Cost (IDR)
1.	Implementation of daily automatic backups	6.000.000
2.	Provision of external backup media	5.000.000
3.	Implementation of data recovery and restoration procedures	4.000.000
4.	Data management and system security training	3.000.000
	Total	18.000.000

After implementing risk management measures, it is estimated that the possibility of data loss can be reduced so that the ARO value decreases to 1 time per year and the EF value also decreases.

Table 11: Table ALEprojected for data loss risk

No.	Item	Total Value (IDR)	EF (%)	SLE (IDR)	ARO	$ALE_{projected}$ (IDR)
1.	Server	15.000.000	10	1.500.000	1	1.500.000
2.	Router	5.000.000	15	750.000	1	750.000
3.	Database System	20.000.000	15	3.000.000	1	3.000.000
4.	Web Application	10.000.000	10	1.000.000	1	1.000.000
	Total annual losses					6.250.000

So, from the data above, we get an ROI value of: (37,000,000 – 6,250,000) / 18,000,000 = 1.71 ≈ 2 : 1

3.4. Information System Security Threats

It is estimated that within one year there will be three threats to the information system security of the Information Systems Department website at UPN "Veteran" Jawa Timur. These threats may take the form of malware attacks, hacking attempts, data theft, or misuse of access rights [18]. The impact of these risks is data leakage, system damage, and disruption of user confidence in the information system. The ARO (Annual Rate of Occurrence) value used is 3/1 = 3.

Table 12: Table ALEcurrent for information system security threat risks

No.	Item	Total	Unit Value (IDR)	Total Value (IDR)	Classification	EF (%)	SLE (IDR)	ARO	$ALE_{current}$ (IDR)
1.	Server	1	15.000.000	15.000.000	System	40	6.000.000	3	18.000.000
2.	Database System	1	20.000.000	20.000.000	Data	35	7.000.000	3	21.000.000
3.	Web Application	1	10.000.000	10.000.000	Application	30	3.000.000	3	9.000.000
4.	User Data	1	25.000.000	25.000.000	Data	40	10.000.000	3	30.000.000
5.	Internet network	1	5.000.000	5.000.000	Network	25	1.250.000	3	3.750.000
Total annual losses									81.750.000

Measures taken to reduce the risk of a potential Information System Security Threat (Annual Cost Investment):

Table 13: Information System Security Threat Risk Management

No.	Handling Actions	Cost (IDR)
1.	Implementation of firewalls and intrusion detection systems	8.000.000
2.	Use of licensed antivirus and anti-malware software	5.000.000
3.	Periodic information system security audits	6.000.000
4.	Information security training for administrators	4.000.000
Total		23.000.000

After implementing risk management measures, it is estimated that the level of threat to information system security can be reduced so that ARO decreases to once per year and the level of impact of losses also decreases.

Table 14: Table ALEprojected for information system security threat risks

No.	Item	Total Value (IDR)	EF (%)	SLE (IDR)	ARO	$ALE_{projected}$ (IDR)
1.	Server	15.000.000	15	2.250.000	1	2.250.000
2.	Database System	20.000.000	15	3.000.000	1	3.000.000
3.	Web Application	10.000.000	10	1.000.000	1	1.000.000
4.	User Data	25.000.000	15	3.750.000	1	3.750.000
5.	Internal Network	5.000.000	10	500.000	1	500.000
Total annual losses						10.500.000

So, from the data above, we get the ROI value: (81,750,000 – 10,500,000) / 23,000,000 = 3.10 ≈ 3 : 1

4. Conclusion

Based on the results of information system security risk analysis using the Annual Loss Expectancy (ALE) method on the Information Systems Department website of UPN "Veteran" Jawa Timur, it can be concluded that the information system has various potential risks that can cause annual financial losses, including service disruptions, device damage, data loss, and information system security threats. The ALE method, which considers asset value, exposure factor, and annualized rate of occurrence, provides a quantitative picture of the potential losses that an organization may experience. Of the four risks analyzed, information system security threats are the risks with the highest loss value [15], amounting to IDR 81,750,000 per year, which is classified as Low/Medium to Medium based on the ALE adjective table, so it needs to be a top priority in risk control.

The implementation of the proposed risk mitigation measures has been proven to significantly reduce the projected ALE value across all risk categories. Mitigation priorities for 13 medium-high risks (such as application and data servers) are recommended in similar data center assessments [20]. The Return on Investment (ROI) calculation results show that all risk management measures produce an ROI value of ≥ 2:1, even for information system security threats, which reach a ratio of 3:1, indicating that the security investments made are feasible and economically viable. Thus, the ALE method can be used effectively as a basis for decision-making in information system security risk management, particularly in determining the priority of risk control that has a significant impact on financial losses and the continuity of the department's information system services.

References

[1] S. Nur Oktaviana, V. Apriliani, W. Nova Novita, S. Mulyeni, and H. Herlina, "Implementasi Sistem Informasi Akademik Dalam Meningkatkan Mutu Pelayanan Kampus," J. Soshum Insentif, vol. 7, no. 1, pp. 53–62, Apr. 2024, doi: 10.36787/jsi.v7i1.1416.

[2] D. E. N. Hidayah, B. Irawan, and E. Paselle, "EFEKTIVITAS SISTEM INFORMASI AKADEMIK DALAM PENINGKATAN PELAYANAN AKADEMIK PADA FAKULTAS ILMU SOSIAL DAN ILMU POLITIK DI UNIVERSITAS MULAWARMAN," vol. 7.

[3] I. P. Jovano, I. R. Padiku, and B. Ahaliki, "Analisis Manajemen Risiko dan Keamanan Sistem Informasi Akademik Terpadu (SIAT) Universitas Negeri Gorontalo Menggunakan Framework NIST SP 800-30".

[4] B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," J. Teknol. Dan Inf., vol. 12, no. 2, pp. 106–117, Sep. 2022, doi: 10.34010/jati.v12i2.6829.

[5] R. K. Devi, D. I. Sensuse, Kautsarina, and R. R. Suryono, "Information Security Risk Assessment (ISRA): A Systematic Literature Review," J. Inf. Syst. Eng. Bus. Intell., vol. 8, no. 2, pp. 207–217, Oct. 2022, doi: 10.20473/jisebi.8.2.207-217.

[6] I. Kuzminykh, B. Ghita, V. Sokolov, and T. Bakhshi, "Information Security Risk Assessment," Encyclopedia, vol. 1, no. 3, pp. 602–617, Jul. 2021, doi: 10.3390/encyclopedia1030050.

[7] M. Alim, I. Rasyid Munthe, and A. Putra Juledi, "Evaluasi Keamanan Sistem Informasi dalam Lingkungan Bisnis Digital," J. Ilmu Komput. Dan Sist. Inf. JIKOMSI, vol. 7, no. 1, pp. 328–332, Mar. 2024, doi: 10.55338/jikomsi.v7i1.3088.

[8] M. K. Sari, Y. Saintika, and W. A. Prabowo, "Penyusunan Manajemen Risiko Keamanan Informasi Dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto," J. Sist. Dan Teknol. Inf. JustIN, vol. 10, no. 4, p. 423, Dec. 2022, doi: 10.26418/justin.v10i4.48977.

[9] A. Nikmat, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA SISTEM INFORMASI AKADEMIK (SIAK) UNIVERSITAS MUHAMMADIYAH SUKABUMI (UMM) MENGGUNAKAN ISO 31000: indo," J. Manaj. Dan Teknol. Inf., vol. 14, no. 1, pp. 49–58, Apr. 2024, doi: 10.59819/jmti.v14i1.3321.

[10] A. G. R. Padang, A. Ambarwati, and E. Setiawan, "Penilaian Manajemen Risiko TI Menggunakan Quantitative dan Qualitative Risk Analysis," SISTEMASI, vol. 10, no. 3, p. 527, Sep. 2021, doi: 10.32520/stmsi.v10i3.1340.

[11] A. Rohmani and M. G. Wibisono, "STRATEGI MITIGASI RESIKO KEAMANAN INFORMASI BERDASARKAN ANALISA RETURN ON INVESTMENT PADA BADAN PUSAT STATISTIK DAERAH KOTA SEMARANG".

[12] T. Soebijono, "ANALISA RESIKO KEAMANAN INFORMASI SEBAGAI STRATEGI MITIGASI RESIKO PADA TOKO ONLINE 'X'".

[13] A. N. Fanani, B. T. Hanggara, and A. R. Perdanakusuma, "Manajemen Risiko Keamanan Informasi Menggunakan ISO/IEC 27005 Studi Kasus Pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo".

[14] A. Ferdinand, K. Naristi, R. Abdillah, S. D. Walujo, L. D. Fitrani, and A. C. Puspitaningrum, "Pengukuran Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Metode FMEA Dan Framework ISO 27001:2013 pada PT. ABC," JOINS J. Inf. Syst., vol. 9, no. 1, pp. 23–33, Jul. 2024, doi: 10.33633/joins.v9i1.9059.

[15] Dian Saputra, "ANALISIS DAN PENGELOLAAN RISIKO KEAMANAN INFORMASI PUSKESMAS MENGGUNAKAN METODE OCTAVE ALLEGRO (STUDI KASUS : PUSKESMAS XYZ)," J. Comput. Sci. Inform. JOCSI, vol. 2, no. 1, pp. 12–18, Sep. 2024, doi: 10.69747/jocsi.v2i1.61.

[16] N. Shukla, "A Comparative Study on Information Security Risk Analysis Practices".

[17] V. Evrin, "Risk Assessment and Analysis Methods: Qualitative and Quantitative," 2021.

[18] Cynthia Widya Lestari, Nurul Izzah, Puti Tsabita Najwa Arief, Muhammad Ananda Giovanny R, and Agung Brastama Putra, "Analisis Risiko Keamanan Siber Website Peken Surabaya Menggunakan Standar ISO 27005:2019 dan OWASP ZAP," Saturnus J. Teknol. Dan Sist. Inf., vol. 3, no. 3, pp. 136–154, Aug. 2025, doi: 10.61132/saturnus.v3i3.983.

[19] F. Cremer et al., "Cyber risk and cybersecurity: a systematic review of data availability," Geneva Pap. Risk Insur. - Issues Pract., vol. 47, no. 3, pp. 698–736, Jul. 2022, doi: 10.1057/s41288-022-00266-6.

[20] H. Z. Artie, M. Hilman, and S. Yazid, "Penilaian Risiko Keamanan Informasi Pusat Data pada Instansi XYZ," J. Inform. Ekon. Bisnis, pp. 270–276, Jun. 2025, doi: 10.37034/infeb.v7i2.1160.