Audit Keamanan Dan Manajemen Risiko Dengan Menggunakan *Framework* NIST (Studi Kasus : *E-Learning* UNIBI)

Reynaldy Gimnastiar[1], Reni Nursyanti[2], Sardjono[3]
Fakultas Teknologi dan Informatika
Universitas Informatika dan Bisnis Indonesia
Bandung, Indonesia
e-mail: [1]reynaldygimnastiar49@gmail.com, [2]reninursyanti@unibi.ac.id, [3]sardjono@unibi.ac.id

Correspondence : *e-mail*: reynaldyg.20@student.unibi.ac.id

Diajukan: 30 Juli 2024; Direvisi: 22 Agustus 2024; Diterima: 22 Agustus 2024

Abstrak

Penelitian ini mengevaluasi keamanan dan manajemen risiko sistem *e-Learning* Universitas Informatika dan Bisnis Indonesia (UNIBI) menggunakan *framework* NIST. Tujuannya adalah menganalisis tingkat keamanan dan mengidentifikasi risiko potensial pada *platform* pembelajaran jarak jauh UNIBI. Metodologi mencakup audit keamanan berdasarkan NIST SP 800-26 melalui kuesioner, serta analisis manajemen risiko sesuai NIST SP 800-30. Data yang dikumpulkan dianalisis untuk menentukan tingkat keamanan sistem saat ini. Hasil audit menunjukkan tingkat keamanan sistem *e-Learning* UNIBI yang memadai, namun masih memerlukan peningkatan di beberapa area. Analisis risiko mengidentifikasi berbagai ancaman dan kerentanan yang perlu ditangani. Berdasarkan temuan tersebut, penelitian ini memberikan rekomendasi konkret untuk meningkatkan keamanan sistem dan mengoptimalkan pengelolaan risiko. Implementasi rekomendasi ini diharapkan dapat memperkuat keamanan dan ketahanan sistem *e-Learning* UNIBI, mendukung pembelajaran jarak jauh yang lebih efektif dan aman bagi mahasiswa dan staf pengajar.

Kata kunci: Audit Keamanan, *e-Learning*, Manajemen Risiko, NIST, Universitas Informatika dan Bisnis Indonesia.

Abstract

This research evaluates the security and risk management of Universitas Informatika dan Bisnis Indonesia (UNIBI) e-Learning system using NIST framework. The goal is to analyze the security level and identify potential risks on UNIBI's distance learning platform. The methodology includes a security audit based on NIST SP 800-26 through a questionnaire, as well as risk management analysis as per NIST SP 800-30. The collected data was analyzed to determine the current security level of the system. The audit results showed an adequate level of security of UNIBI's e-Learning system, but still requires improvement in some areas. The risk analysis identified various threats and vulnerabilities that need to be addressed. Based on the findings, this research provides concrete recommendations to improve system security and optimize risk management. Implementation of these recommendations is expected to strengthen the security and resilience of UNIBI's e-Learning system, supporting more effective and secure distance learning for students and faculty.

Keywords*: e-Learning, NIST, , Informatics and Business University of Indonesia***,** *Risk Management, Security Audit.*

1. Pendahuluan

Teknologi informasi (TI) telah membawa banyak perubahan yang sangat positif bagi perguruan tinggi salah satunya dalam hal mengakses informasi dengan mudah dan cepat, proses belajar mengajar lebih efektif dan komunikasi antar sivitas akademik semakin lancar. Akan tetapi pengguna teknologi informasi juga bisa memberikan dampak negatif untuk perguruan tinggi jika keamanan informasinya tidak dijaga [1] [2] [3]. Sudah banyak perguruan tinggi yang melakukan banyak inovasi pembelajaran menggunakan teknologi infomasi dan komunikasi ini. Kemudahan akses internet dan murahnya perangkat untuk mengakses internet, penggunaan *e-learning* di perguruan tinggi terus bertambah [4] [5]. Dengan pembelajaran yang dilakukan secara daring maka materi pembelajaran tidak lagi terbatas oleh jarak, ruang dan waktu serta bisa dilakukan dimana saja.

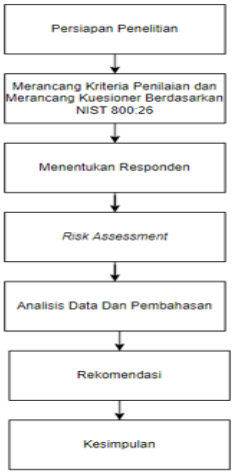
Perkembangan yang pesat sistem informasi dan teknologi informasi mendorong kebutuhan audit sistem informasi di berbagai lembaga. Audit memiliki peran penting dalam memastikan dan keandalan sistem, serta menjadikan rujukan pengembangan sistem yang ada. Pengelolaan yang tidak baik akan sangat berpengaruh kepada kinerja dan pandangan pengguna. Risiko IT merupakan risiko yang didapatkan karena hasil dari pemanfaatan teknologi informasi yang berpotensi menimbulkan dampak yang negatif, untuk mengatasinya diperlukan sebuah cara yang disebut manajemen resiko [6] [7]. Maka dari itu, penerapan manajemen risiko memegang peranan yang sangat penting dalam menjaga keamanan data dan aset apabila terjadi kesalahan yang disebabkan oleh masalah data. Dan dalam konteks organisasi, penerapan manajemen risiko bertujuan agar organisasi dapat mengelola resiko yang ada [8].

Framework NIST *(National Institute of Standard and Technology)* adalah kerangka kerja yang berfungsi untuk pengukuran, menetapkan standar dan teknologi agar mampu mengoptimalkan fungsi dari infrastruktur instansi, khususnya dalam bidang IT. Versi dan topik NIST sangat banyak tetapi saling memiliki keterkaitan. "*NIST Special Publication 800-26 : Security Self-Asessment Guide for Information Technology System*" yang berfungsi untuk melakukan audit keamanan informasi dengan menentukan kriteria penilaian dan menjadi dasar untuk merancang kusioner [9]. Dan "*NIST Special Publication 800-30 : Risk Management Guide For Information Technology System*" yang berfungsi untuk mengetahui status keamanan sistem informasi saat ini. *Framework* NIST diharapkan dapat meningkatkan kemampuan sebuah instansi dalam mengatasi permasalahan keamanan dalam komputer, baik pada saat ini maupun ini maupun yang akan datang [10]. Dengan banyaknya instansi baik nasional maupun internasional yang menggunakan *framework* ni sebagai sistem audit keamanan dan manajemen risiko, serta kejelasan setiap bagian dari NIST baik itu pertanyaan kepada responden dan tahapannya, maka NIST layak digunakan untuk penelitian ini [9].

Sistem *e-Learning* Universitas Informatika dan Bisnis Indonesia merupakan platform baru untuk menggantikan pembelajaran tatap muka. Sistem ini menyediakan materi perkuliahan, tugas, kuis, UTS dan UAS yang diberikan oleh dosen. Sistem ini masih terbilang baru dan belum diketahui sampai sejauh mana sistem keamanan sudah berjalan. Sistem *e-Learning* UNIBI ini juga belum dilakukannya penelitian tentang audit kemanan dan manajemen risiko pada sistem ini. Sering terjadi juga pada *e-Learning* UNIBI saat ini, yaitu seringkali mengalami down pada sistem ini. Peran dan tujuan NIST ini adalah sebagai standar keamanan, manajemen risiko dan dapat memberikan rekomendasi untuk sistem *e-Learning* UNIBI.

2. Metode Penelitian

Metode penelitian yang dilakukan dalam penelitian ini dapat dilihat pada alur tahapan penelitian dimulai dari persiapan penelitian sampai kesimpulan seperti pada gambar 1.



Gambar 1 Tahapan Penelitian

Tahapan dalam penelitian ini adalah :

1. Persiapan Penelitian : Mencakup pembentukan latar belakang, identifikasi masalah, penetapan tujuan, studi literatur, dan observasi sesuai teori yang relevan.
2. Menentukan kriteria penilaian dan merancang kuesioner : Kriteria didasarkan pada NIST SP 800-26 dan digunakan untuk merancang kuesioner penelitian.
3. Menetukan responden : Responden yang dipilih adalah mahasiswa dari Universitas Informatika dan Bisnis Indonesia, yang merupakan pengguna sistem *e-Learning.*
4. *Risk assessment* : Dilakukan sesuai langkah-langkah dalam NIST SP 800-30.

5. Analisis data dan pembahasan :Data kuesioner diolah dan dianalisis untuk menarik kesimpulan
6. Rekomendasi :Hasil analisis data dan pembahasan dari penelitian akan diikuti oleh rekomendasi dari peneliti. Rekomendasi ini bertujuan untuk meningkatkan peran sistem secara maksimal.

3. Hasil dan Pembahasan

E-learning merupakan metode pembelajaran jarak jauh berbasis elektronik [14] [15]. Penelitian ini fokus pada keamanan dan manajemen risiko sistem *e-Learning* UNIBI, menggunakan kuesioner berbasis standar NIST untuk mahasiswa dan analisis kerentanan dengan OWASP ZAP. Hasilnya akan menggambarkan tingkat keamanan dan risiko pada sistem *e-Learning* tersebut..

3.1 Tingkat Keamanan

Pada tingkat keamanan ini akan memaparkan hasil dari pengolahan data dari kuesioner yang sudah diisi oleh responden yang diantara : (1) Penilaian Tingkat *Management Control*, (2) Penilaian Tingkat *Operational Control*, dan (3) Penilaian Tingkat *Technical Control*.

Tabel 1. Pertanyaan Penilaian *management control*

No	Sub Kriteria	Skala Likert					Jumlah Responden	Jumlah Data	Rata Rata	Presentase (%)
		5	4	3	2	1				
1	Apakah penting untuk secara berkala membuat *backup* cadangan data yang tersimpan dalam sistem e-learning?	62	38	7	1	2	110	487	4,43	88,6%
2	Apakah diperlukan implementasi langkah-langkah keamanan untuk menjaga keamanan aset yang terkait dengan *platform e-learning*?	57	46	5	2	0	110	488	4,44	88,8%
3	Apakah sistem perlu memberikan pemberitahuan tentang kegagalan atau kesalahan setelah penyimpanan dilakukan meskipun terjadi *input* yang salah?	51	42	14	3	0	110	471	4,28	85,6%
4	Apakah pengguna mendapatkan pelatihan dari pihak Teknologi Informasi sebelum penerapan sistem dilakukan?	30	41	27	9	3	110	416	3,78	75,6%
5	Apakah diperlukan langkah-langkah keamanan tambahan untuk menjaga privasi pengguna?	53	43	12	1	1	110	476	4,33	86,6%
	JUMLAH	253	210	65	16	6	550	2338	21,26	425,4
	RATA RATA KESELURUHAN								4,252	85,04%

Pada tabel 1 bahwa kategori pengendalian manajemen memiliki persentase mencapai 85,04%. Berdasarkan hasil ini bisa diketahui bahwa tingkat keamanan yang sudah diterapkan pada sistem kuliah online ini sudah berada pada level 4 yaitu *Tested and Reviewed Procedures and Controls*.

Tabel 2. Penilaian Tingkat *operational control*

No	Sub Kriteria	Skala Likert					Jumlah Responden	Jumlah Data	Rata Rata	Presentase (%)
		5	4	3	2	1				
1	Apakah tersedia bantuan bagi pengguna dalam menggunakan *sistem e-learning*?	27	42	27	13	1	110	411	3,74	74,8%
2	Apakah ada rekomendasi atau bantuan yang diberikan oleh tim Teknologi Informasi kepada pengguna?	17	45	35	11	2	110	394	3,58	71,6%
3	Apakah ada langkah-langkah yang diambil untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses ke sistem *e-learning*?	30	49	22	8	1	110	429	3,9	78%
4	Apakah tampilan interface untuk memasukkan data mudah dimengerti oleh pengguna?	34	45	25	5	1	110	436	3,96	79,2%
5	Apakah ada langkah-langkah yang diambil untuk memastikan bahwa orang yang tidak berwenang tidak dapat mengakses identitas pengguna atau mengubah informasi mereka?	28	42	26	10	4	110	410	3,72	74,4%
	JUMLAH	136	185	135	47	9	550	2080	18,9	378
	RATA RATA KESELURUHAN								3,78	75,6%

Pada Tabel 2. proses kategori pengendalian operasional memiliki nilai yang diperoleh dari hasil keselurahan persentase yaitu 75,6%. Berdasarkan hasil ini bisa diketahui bahwa tingkat keamanan yang sudah diterapkan pada sistem kuliah ini sudah berada pada level 3 (*Implemented Procedures and Controls*).

Tabel 3 Penilaian Tingkat *Technical Control*

No	Sub Kriteria	Skala Likert					Jumlah Responden	Jumlah Data	Rata Rata	Presentase (%)
		5	4	3	2	1				

1	Apakah sistem memiliki kemampuan untuk memberikan bantuan kepada pengguna ketika terjadi insiden keamanan?	**21**	**49**	**20**	**16**	**4**	**110**	**397**	**3,61**	**72,2%**
2	Apakah penting bahwa kemampuan untuk merespons insiden harus disampaikan dengan jelas?	**46**	**53**	**8**	**2**	**1**	**110**	**471**	**4,28**	**85,6%**
3	Apakah ada prosedur untuk melaporkan kejadian insiden?	**18**	**48**	**23**	**14**	**7**	**110**	**386**	**3,51**	**70,2%**
4	Apakah ada cara untuk memastikan bahwa keterangan tentang insiden telah diterima dan direspons?	**17**	**45**	**31**	**13**	**4**	**110**	**388**	**3,53**	**70,6%**
5	Apakah penting untuk melacak insiden dari awal hingga selesai?	**54**	**37**	**16**	**1**	**2**	**110**	**470**	**4,27**	**85,4%**
	JUMLAH	**156**	**232**	**98**	**46**	**18**	**550**	**2112**	**19,2**	**384**
	RATA RATA KESELURUHAN								**3,84**	**76,8%**

Pada tabel 3 memiliki nilai yang diperoleh dari kemampuan respon insiden mencapai nilai persentase 76,8%. Berdasarkan hasil ini bisa diketahui bahwa tingkat keamanan yang sudah diterapkan pada sistem kuliah online untuk kategori technical control. Pada kemampuan respon insiden sudah berada pada Level 3 (*Implemented Procedures and Controls*).

3.1.4 Penilaian Keseluruhan

Dari tabel penilaian yang sudah dipaparkan sebelumnya mulai dari penilaian *management control*, *operational control* dan *technical control* , maka tiga penilaian tersebut dikalkulasikan pada sebuah tabel penilaian keseluruhan yang dapat dilihat pada tabel 4.

Tabel 4. Penilaian Keseluruhan

No	Sub Kriteria Pertanyaan	Rata-rata	Persentase
1	*Management Control*	**4,252**	**85,04%**
2	*Operational Control*	**3,78**	**75,6%**
3	*Technical Control*	**3,84**	**76,8%**
Rata – Rata Total		**3,95**	**79,14%**

Hasil perhitungan menunjukkan bahwa tingkat keamanan keseluruhan sistem e-Learning mencapai 79,14%, yang dikategorikan sebagai level 3 (*Implemented Procedures and Controls*) berdasarkan NIST SP 800-26.

3.2 Risk Assessment Berbasis NIST 800:30

Penilaian risiko ini bertujuan untuk mengetahui seberapa besar ancaman pada sistem e-Learning dengan mengetahui diantara nya: (1) Identifikasi Ancaman, (2) Hasil Identifikasi Kerentanan, (3) Penilaian Kecenderungan Risiko, (4) Analisis Dampak, (5) Penilaian Tingkat Risiko, dan (6) Rekomendasi Pengendalian.

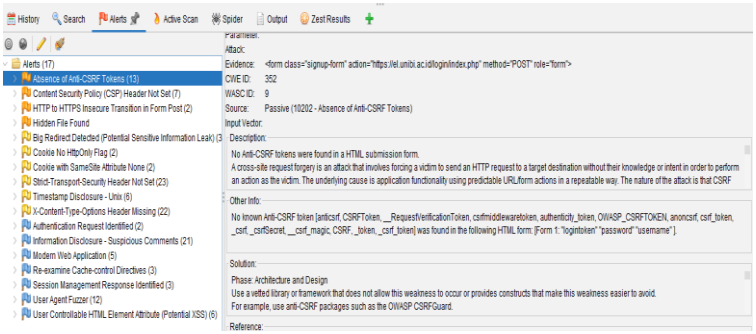
3.2.1 Identifikasi Ancaman

Framework NIST SP 800-30 mengklasifikasikan gangguan terhadap sistem informasi menjadi tiga jenis ancaman utama:

a. Ancaman Alam (*Natural Threat*): Gangguan yang berasal dari alam dan bersifat mendadak, seperti gempa bumi, banjir, atau badai.
b. Ancaman Manusia (*Human Threat*): Gangguan yang disengaja atau tidak disengaja oleh manusia, seperti peretasan, pencurian data, atau kesalahan pengguna.
c. Ancaman Lingkungan (*Environmental Threat*): Gangguan yang diakibatkan oleh perubahan kondisi lingkungan, seperti suhu ekstrem, kelembapan tinggi, atau debu, yang dapat mempermudah terjadinya gangguan lain.

3.2.2 Hasil Indetifikasi Kerentanan

Hasil *scanning* sistem keamanan pada *website e-Learning* Universitas Informatika dan Bisnis Indonesia memiliki kerentanan pada level *Medium*. Sistem berada pada level 3 yang memiliki 17 kriteria kerentanan keamanan, tapi pada gambar 4.1 dapat dilihat bahwa sistem tidak memiliki kerentanan yang tinggi. Dengan demikian, sistem kuliah *online* ini bisa berada pada *level medium*.



Gambar 2 Hasil Scan Menggunakan ZAP

3.2.3 Analisis Pengendalian

Sistem *e-Learning* berbasis *Rocky* 9 Linux dengan *firewall iptables* dan *Uncomplicated Firewall* (UFW). Implementasi ini memudahkan identifikasi dan penanganan masalah keamanan serta stabilitas, membantu administrator meminimalkan gangguan dan waktu henti dalam lingkungan pembelajaran.

3.2.4 Penilaian Kecenderungan Risiko

Tingkat risiko keamanan pada sistem *e-Learning* Universitas Informatika dan Bisnis Indonesia (UNIBI) dapat dianalisis berdasarkan jenis ancaman yang dihadapi, baik terhadap sistem maupun infrastruktur fisik servernya. Berikut adalah penjelasan mengenai kecenderungan risiko UNIBI terhadap berbagai jenis ancaman:

1. *Natural Threat* : Risiko bencana alam di UNIBI rendah karena lokasi aman dan persiapan seperti APAR dan SOP yang memadai. Tingkat kecenderungan dikategorikan rendah (*low*).
2. *Human Threat* : Sistem rentan terhadap peretasan, penyalahgunaan akses, dan sabotase fisik. UNIBI memasang firewall Iptables dan CCTV untuk pencegahan, sehingga risiko ancaman manusia rendah (*low*).
3. *Environmental threat* : Risiko dari suhu, kelembaban, dan debu dikendalikan melalui prosedur pemeliharaan lingkungan server yang optimal. Tingkat kecenderungan dikategorikan rendah (*low*).

3.2.5 Analisis Dampak

Risiko pada sistem *e-Learning* UNIBI dapat mengakibatkan dampak yang beragam, mulai dari kerusakan *hardware*, *software*, hingga kehilangan data dan informasi penting yang tersimpan di server. Dampak yang ditimbulkan tergantung pada jenis dan tingkat keparahan risiko yang terjadi. Beberapa dampak yang bisa terjadi diantaranya :

1. Banjir dan suhu tidak stabil dapat menyebabkan kerusakan fisik pada server, seperti terendam air dan konsleting, mengakibatkan hilangnya data penting karena server tidak dapat digunakan.
2. Kerusakan server dapat memberi akses kepada hacker untuk mengubah dan mencuri informasi, serta merusak sistem yang telah dibangun.
3. Penggunaan melebihi kapasitas dapat merusak perangkat keras server, mengganggu proses kuliah *online*.

3.2.6 Penilaian Tingkat Risiko

Tingkat risiko yang mungkin terjadi terhadap sistem yang ada di Universitas Informatika dan Bisnis Indonesia dapat ditentukan. Tingkat risiko pada Universitas Informatika dan Bisnis Indonesia tersebut, yaitu:

1. Risiko kebakaran di sistem e-Learning UNIBI tinggi (*high*), berdampak pada kerusakan server, kehilangan data, dan kerusakan infrastruktur. Untuk mengurangi risiko, institusi menyediakan APAR, menjalankan prosedur keselamatan, dan meningkatkan keselamatan kerja.
2. *Hacker* adalah ancaman tinggi yang dapat merusak data dan mendapatkan akses ilegal. Untuk pencegahan, institusi memasang *firewall Iptables* dan *Uncomplicated Firewall* (UFW) pada *Rocky* versi terbaru, sehingga risiko serangan *hacker* rendah (*low*).
3. Kerusakan akibat penggunaan melebihi kapasitas sistem dapat terjadi jika lingkungan berkembang tanpa penambahan kapasitas. IT perlu menambah kapasitas secara berkala sesuai kebutuhan, sehingga risiko lingkungan rendah.(*low*).

3.2.7 Rekomendasi Pengendalian

Hasil keamanan sistem kuliah *online* di Universitas Informatika dan Bisnis Indonesia memiliki nilai rata-rata 79,14% (*level 3: Implemented Procedures and Controls*), dengan target level 4 (*Tested and Reviewed Procedures and Controls*). Berdasarkan NIST SP 800-26, untuk mencapai level 4 diperlukan beberapa aktivitas rekomendasi :

1. Mengembangkan program evaluasi efektivitas kebijakan keamanan, prosedur, dan pengendalian.

2. Institusi melakukan kontrol setiap kali terjadi perubahan signifikan pada sistem.
3. Institusi memeriksa kerentanan yang terungkap melalui insiden keamanan atau peringatan keamanan.
4. Rutin menganalisis catatan insiden keamanan untuk aktivitas mencurigakan.
5. Institusi melakukan perpindahan ke PC khusus server.

4. Kesimpulan

Dari hasil penelitian yang telah dilakukan pada sistem *e-Learning* di Universitas Informatika dan Bisnis Indonesia, dapat diambil kesimpulan sebagai berikut : (1) Dampak sistem *e-Learning* terhadap manajemen kontrol sangat positif yaitu 85,04%. (2) *Operational control* 75,6% dan *technical control* 76,8% cukup baik, namun masih perlu pengembangan. (3) Keamanan sistem berada pada level 3 (*implemented procedures and control)* dengan nilai 79,14%. (4) Analisis OWASP ZAP menemukan 17 kriteria kerentanan pada *website* el.unibi.ac.id. (5) Rekomendasi: perbaikan program keamanan, kontrol berkala, analisis insiden rutin, penggunaan server khusus, dan dokumentasi aktivitas pengguna.

Daftar Pustaka

[1] D. Amanda, N. Mutiah and S. Rahmayudha, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan NIST Cybersecurity Framework dan CMMI," *Jurnal Komputer dan Aplikasi*, vol. 11, pp. 291-302, 2023.

[2] S. C. a. K. M. Y. a. K. E. W. a. C. D. K. Hui, "Information security and technical issues of cloud storage services: a qualitative study on university students in Hong Kong," *Library Hi Tech*, 2023.

[3] W. C. H. a. C. C. a. L. J. a. Z. Y. a. L. V. N.-L. a. X. X. Hong, "he influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates," *Education and Information Technologies*, vol. 28, no. 1, pp. 439-470, 2023.

[4] S. C. a. C.-E. V. C. a. O. C. K. a. B. A. O. Eze, "Factors influencing the use of e-learning facilities by students in a private Higher Education Institution (HEI) in a developing economy," *Humanities and social sciences communications*, vol. 7, pp. 1-15, 2020.

[5] M. A. a. S. M. A. a. A. A. Qazi, "Barriers and facilitators to adoption of e-learning in higher education institutions of Pakistan during COVID-19: Perspectives from an emerging economy," *Journal of Science and Technology Policy Management*, vol. 15, no. 1, pp. 31-52, 2024.

[6] A. A. Dimas Adi Prastiyawan and E. Setiawan, "Analisis Manajemen Risiko Layanan Sistem Manajemen Dealer Menggunakan COBIT 5," *Jurnal Matri*, vol. 10, no. 2, pp. 43-49, 2020.

[7] F. A. Hardianto and Y. S. Dharmawan, "Manajemen Risiko TI ISO 31000 Dengan COBIT 5 dan FMEA (PT.XYZ)," *Jurnal Sistem Informasi dan Teknologi*, vol. 4, no. 2, pp. 133-146, 2022.

[8] D. I. Izatri, N. I. Rohmah and R. S. Dewi, "Identifikasi Risiko pada Perpustakaan Daerah Gresik dengan NIST SP 800-30," *Jurnal Riset Komputer*, vol. 7, no. 1, pp. 50-55, Februari 2020.

[9] S. Solihin and H. Hanafiah, "Audit Keamanan dan Manajemen Risiko pada e-learning Universitas Sangga Buana," *Jurnal Manajemen Informatika*, vol. 11, no. 1, pp. 1-14, April 2021.

[10] M. S. Hardani and K. Ramli, "Perancangan Manajemen Risiko Keamanan Sistem Informasi Manajemen Sumber Daya dan Perangkat Pos dan Informatika (SIMS) Menggunakan Metode NIST 800-30," *Jurnal Riset Komputer*, vol. 9, no. 3, pp. 591-599, 2022.

[11] D. Darmawan, Metode Penelitian Kuantitatif, Keti ed., P. Latifah, Ed., Bandung: Remaja Rosdakarya, 2016.

[12] S. Surhayadi and K. Purwanto, Statistika Untuk Ekonomi dan Keuangan Moderen, D. A. Halim, Ed., Jakarta: Salemba Empat, 2016.

[13] Yudiana, A. Elanda and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK ROSMA Dengan Menggunakan OWASP TOP 10," *Journal of Computer Engineering System and Science*, vol. 6, no. 2, pp. 185-191, Juli 2021.

[14] H. Sama and E. , "Pengembangan Website E-Learning Berdasarkan Preferensi Mahasiswa UIB Dengan Metode Research and Development," *Jurnal Sistem Informasi*, vol. 6, no. 1, pp. 1-13, 2024.

[15] D. Sukanto, "Pembelajaran Jarak Jauh Dengan Media E-Learning Sebagai Solusi Pembelajaran Pada Masa Pandemi Corona Virus Disease 2019 (Covid-19)," *Syntax*, vol. 2, no. 11, p. 835, 2020.