ANALISIS KEAMANAN PENGELOLAAN WEB SIMPEL UPN "VETERAN" JAWA TIMUR MENGGUNAKAN ISO 27001:2013

SECURITY ANALYSIS OF SIMPLE WEB MANAGEMENT IN UPN "VETERAN" JAWA TIMUR USING ISO 27001:2013

Lawaahizh Hanifah Pulungan[1*], Radithya Markarito Ariputra[1], Ardilla Firosya[1], Diajeng Putri Widiastuti[1], Reisa Permatasari[1]
*E-mail: 21082010215@student.upnjatim.ac.id

[1]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur

Abstrak

Pada era digital yang terus berkembang saat ini, keamanan informasi dan perlindungan data menjadi faktor kritis yang harus dipertimbangkan dalam pengelolaan laboratorium solusi. Keamanan informasi yang digunakan pada Web SIMPEL berupa ISO 27001:2013. Tujuan penelitian ini untuk mengidentifikasi dan melakukan pemahaman yang lebih baik terhadap risiko keamanan informasi yang ada, serta menyediakan rekomendasi untuk peningkatan sistem keamanan pada Web SIMPEL. Untuk mencapai tujuan penelitian ini, pengumpulan data dilakukan menggunakan metode kualitatif dengan melakukan wawancara kepada Kepala Ruangan Laboratorium Solusi Universitas Pembangunan Nasional "Veteran" Jawa Timur. Berdasarkan hasil analisis dengan menggunakan ISO 27001:2013, Web SIMPEL belum memenuhi standar keamanan sistem informasi ISO 27001:2013. Hal tersebut diperoleh dari beberapa domain yang belum sesuai standar ISO 27001:2013 dijabarkan pada tabel *Gap Analysis* yang menunjukkan bahwa masih belum adanya kebijakan dalam keamanan sistem informasi, autentikasi pengguna, hingga belum adanya prosedur yang jelas. Hasil analisis yang ada pada tabel *Gap Analysis* berupa rekomendasi untuk memenuhi domain yang belum sesuai standar. Dengan adanya rekomendasi tersebut, diharapkan dapat membantu pengembangan Web SIMPEL dalam mencapai standar ISO 27001:2013 khususnya dalam hal *information security*.
Kata Kunci: *ISO 27001:2013, keamanan informasi, peningkatan sistem*

Abstract

In today's ever-evolving digital era, information security and data protection are critical factors that must be considered in managing solution laboratories. The information security used on the SIMPEL Web is ISO 27001:2013. The purpose of this study is to identify and make a better understanding of existing information security risks, as well as provide recommendations for improving the security system on the SIMPEL Web. To achieve the objectives of this study, data collection was carried out using qualitative methods by conducting interviews with the Head of the Solutions Laboratory Room at the National Development University "Veteran" East Java. Based on the results of the analysis using ISO 27001:2013, SIMPEL Web does not meet ISO 27001:2013 information system security standards. This was obtained from several domains that were not following the guidelines outlined in the ISO 27001: 2013 standard described in the Gap Analysis table which shows that there is still no policy in information system security, user authentication, so that there are no clear procedures. The results of the analysis in the Gap Analysis table are in the form of recommendations to fulfill domains that are not in accordance with standards. With these recommendations, it is hoped that they can help SIMPEL Web development achieve ISO 27001:2013 standards, especially in terms of information security.
Keywords: *ISO 27001:2013, information security, system improvement*

1. PENDAHULUAN

Penelitian dan pengembangan sesuatu hal umumnya dilakukan pada sebuah tempat bernama laboratorium. Laboratorium sendiri secara bahasa dapat diartikan sebagai tempat kerja untuk melakukan sebuah bentuk rangkaian, penelitian, atau pengukuran disertai dengan adanya peralatan pendukung. Laboratorium Solusi UPN "Veteran" Jawa Timur memegang peranan penting untuk mendukung kegiatan akademik dan penelitian di bidang teknologi informasi. Laboratorium Solusi tersebut merupakan tempat di mana mahasiswa dan staf fakultas dapat melakukan eksperimen, pengembangan, dan pengujian solusi sistem informasi. Pokok penelitian atau makalah yang akan ditulis, tujuan, wawasan, dan rencana pengembangan disebutkan dalam pendahuluan karya ilmiah.

Pada era digital yang terus berkembang saat ini, keamanan informasi dan perlindungan data menjadi faktor kritis yang harus dipertimbangkan dalam pengelolaan Laboratorium Solusi. Bentuk ancaman terhadap keamanan informasi dapat datang dari berbagai sumber, seperti serangan siber, akses tidak sah, kehilangan data, atau kebocoran informasi. Terdapat tiga pilar dalam keamanan informasi, yaitu kerahasiaan yang memastikan bahwa informasi diakses oleh orang yang berwenang, integritas yang menjaga perusakan atau pengubahan informasi secara ilegal, dan ketersediaan yang memastikan bahwa informasi sudah akurat [1].

Sistem informasi adalah kombinasi aktivitas dan teknologi informasi yang digunakan oleh pelaku untuk mendukung operasi dan manajemen [2]. Kegunaan sistem informasi yaitu sebagai metode atau alat yang dapat menjadi pendukung proses pengolahan data sehingga dapat menghasilkan informasi yang berguna bagi organisasi [3]. Sistem Informasi Peminjaman Laboratorium (SIMPEL) merupakan suatu sistem yang meliputi *input*, proses, dan *output* di mana data yang diolah dari Laboratorium Solusi.

Untuk menjaga keamanan pengelolaan SIMPEL, implementasi standar keamanan seperti ISO 27001:2013 menjadi hal yang penting. Standar ISO 27001 adalah standar keamanan yang dapat dijadikan sebagai pedoman dalam peningkatan kesadaran pengguna, pengurangan risiko kemanan, dan penetapan tindakan saat celah keamanan ditemukan [4]. Pada ISO ini, terdapat 133 kontrol keamanan informasi kemudian dari kontrol tersebut perusahaan dapat memilih kontrol yang sesuai dengan kondisi di lapangan untuk diterapkan [5]. Standar ISO 27001 dapat diterapkan pada perusahaan untuk menciptakan serta mempertahankan *information security management system* (ISMS) [6]. ISMS terdiri dari berbagai komponen yang saling berhubungan dan dapat digunakan untuk melakukan pengelolaan dan pengendalian ancaman keamanan informasi serta untuk melindungi CIA. [6].

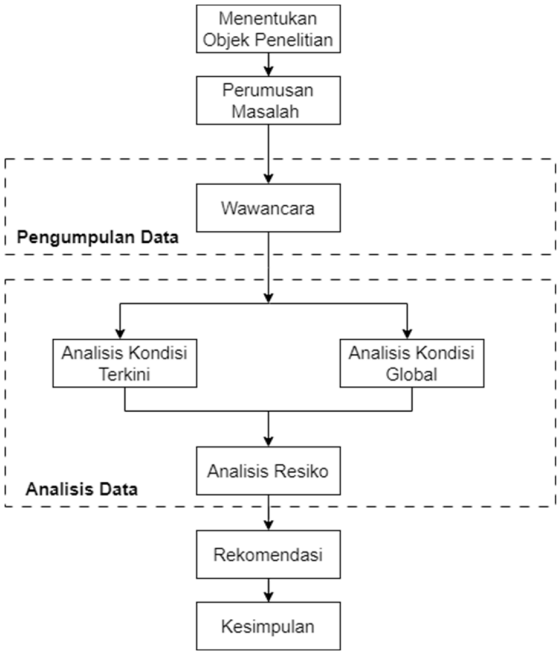
ISO 27001:2013 merupakan standar global untuk ISMS yang menetapkan aturan guna membentuk, menerapkan, mengaplikasikan, mengamati, meninjau, mengelola, dan peningkatan dalam Sistem Manajemen Keamanan Informasi (SMKI) [7]. Dalam ISO 27001:2013 telah dibuat agar dapat disesuaikan dengan pengguna di organisasi kecil, menengah, dan besar di semua bidang untuk melindungi aset informasi yang penting bagi organisasi itu sendiri [8]. Badan Siber dan Sandi Negara (BSNN) mengeluarkan pedoman internasional yang umum untuk melakukan manajemen keamanan data yaitu ISO 27001:2013 [9].

Namun penerapan ISO 27001 sebagai standar keamanan sistem informasi memiliki batasan standar di antaranya persetujuan dari direksi perusahaan di mana sering kali perusahaan menolak menggunakan standar keamanan ini karena beberapa perusahaan merasa kesusahan dalam menerapkan ISO 27001, kendala anggaran yang sebisa mungkin memaparkan keuntungan dari investasi ISO 27001 agar mendapatkan persetujuan anggaran, ketersediaan SDM yang cukup yang bisa memahami penerapan ISO 27001, dan memiliki rencana yang matang agar dapat mencapai target yang diinginkan [10].

Dengan begitu, diperlukan analisis untuk meningkatkan keamanan pengelolaan SIMPEL melalui identifikasi dan pemahaman yang lebih baik terhadap risiko keamanan informasi yang ada, serta menyediakan rekomendasi untuk peningkatan sistem keamanan.

2. METODOLOGI

Metode dalam penelitian adalah teknik yang harus dilakukan guna memperlancar tindakan dalam pengambilan hasil. Standar ISO 27001 adalah metode yang sepadan dalam analisis keamanan informasi [11]. Standar ISO 27001 adalah standar keamanan seri ISO 27001 yang dapat dijadikan sebagai pedoman dalam peningkatan kesadaran pengguna, pengurangan risiko kemanan, dan penetapan tindakan saat celah keamanan ditemukan [4]. Standar ini akan diimplementasikan pada penelitian ini dengan dilakukan beberapa langkah seperti pada Gambar 1.



Gambar 1. Langkah-langkah penelitian

2.1 Pengumpulan data

Pada penelitian ini menggunakan metode kualitatif melalui wawancara kepada Kepala Laboratorium Solusi Universitas Pembangunan Nasional "Veteran" Jawa Timur. Metode penelitian kualitatif berguna untuk melakukan penelitian pada masalah yang ada, dengan peneliti sebagai instrumen kuncinya yang melakukan teknik pengumpulannya secara terhubung dan dengan menggunakan metode kualitatif yang berfokus pada hasil yang didapat dari wawancara [12]. Teknik wawancara merupakan cara untuk memperoleh informasi dengan memberikan pertanyaan-pertanyaan lisan terkait proyek atau kejadian pada masa yang akan datang, kini, bahkan masa lalu secara terstruktur [13]. Teknik wawancara berfokus pada jawaban narasumber yang kemudian akan dianalisis dan dijabarkan menjadi sebuah deskripsi yang berguna untuk menghasilkan pandangan dari sudut pandang narasumber [14].

2.2 Analisis Data

Pada penelitian ini dibuat tabel *gap analysis* berdasarkan hasil wawancara langsung dengan Kepala Laboratorium Solusi untuk mendapatkan data yang akan dianalisis menggunakan tabel *gap analysis*. Tabel *gap analysis* merupakan tabel yang berfungsi untuk melakukan komparasi

antara kondisi keamanan informasi pada Laboratorium Solusi dengan ketentuan standar keamanan ISO 27001:2013 [15]. Terdapat beberapa domain pada ISO 27001:2013 [16] yang dapat dijadikan dasar untuk membuat tabel *gap analysis*, yaitu seperti pada Gambar 2.

Table 1 ISO 27001:2013 Annex Control Domain (ISO/IEC 27001:2013, 2013)

A.5. Information Security Policies	A.13. Communication security
A.6. Organization of Information Security	A.14. System acquisition, development and maintenance
A.7. Human Resource Security	A.15. Supplier relationships
A.8. Asset Management	A.16. Information security incident management
A.9. Access Control	A.17. Information security aspects of business continuity management
A.10. Cryptography	A.18. Compliance
A.11. Physical and environmental security	
A.12. Operation Security	

Gambar 2. Domain ISO 27001:2013 (Anton Purba, Mohammad Soetomo)

3. HASIL DAN PEMBAHASAN

Dari adanya 13 domain yang ada pada ISO 27001:2013, penelitian ini mengambil beberapa domain yang berkaitan dengan penelitian yang dilakukan. Sebaliknya, domain lain tidak digunakan karena adanya ruang lingkup yang terbatas serta batasan sistem yang ada. Berdasarkan hasil wawancara langsung bersama Kepala Laboratorium Solusi UPN "Veteran" Jawa Timur, terdapat sejumlah domain ISO 27001:2013 [17] yang dapat dijadikan dasar untuk membuat tabel *gap analysis*. Beberapa domain yang dimaksud adalah seperti pada Tabel 1.

Table 1. Domain ISO yang digunakan

Domain	Proses Implementasi
A.5	Kebijakan keamanan informasi
A.8	Manajemen aset
A.9	Kontrol akses
A.11	Keamanan fisik dan lingkungan
A.16	Manajemen insiden keamanan informasi

Setelah domain yang diimplementasikan ditentukan, selanjutnya adalah penyusunan pertanyaan yang diajukan kepada narasumber untuk mendapatkan hasil yang digunakan untuk pengolahan data. Daftar pertanyaan yang diajukan adalah seperti pada Tabel 2.

Tabel 2. Pertanyaan Wawancara

Domain	Pertanyaan
A.5 Kebijakan Keamanan Informasi	Bagaimana cara mengelola keamanan pada Web SIMPEL? Apakah Web SIMPEL memiliki kebijakan keamanan informasi? Apa standar keamanan yang digunakan pada Web SIMPEL untuk menjaga kemanan data peminjam?
A.8 Manajemen Aset	Bagaimana cara mengelola kebijakan terhadap penggunaan Web SIMPEL?
A.9 Kontrol Akses	Apa saja batasan yang ada pada Web SIMPEL?
A.11 Keamanan Fisik dan Lingkungan	Apakah ada kemanan fisik yang diterapkan pada Web SIMPEL?
A.16 Manajemen Insiden Keamanan Informasi	Apa yang menjadi kendala dalam mengelola Web SIMPEL?

	Apakah Web SIMPEL pernah mengalami kebocoran data?

Selesai dilakukan analisis yang berlandaskan pada ISO 27001:2013, dari wawancara yang telah dilakukan menggunakan pertanyaan tersebut dapat dihasilkan beberapa temuan menggunakan beberapa domain sebagai berikut ini.

A.5 Kebijakan Keamanan Informasi

Berdasarkan domain tersebut, pada Web SIMPEL belum memiliki kebijakan keamanan informasi. Hal ini juga dipengaruhi karena belum pernah dilakukannya autentikasi sistem serta tidak adanya fitur login pada Web SIMPEL bagi *user* dan pengunjung.

A.8 Manajemen Aset

Berdasarkan domain manajemen aset, data dan informasi Web SIMPEL dikelola langsung oleh admin. User atau pengunjung hanya dapat melakukan inputan peminjaman lab serta melihat tabel daftar peminjam. Penghapusan dan modifikasi data hanya dapat dilakukan admin untuk menjaga konsistensi data.

A.9 Kontrol Akses

Berdasarkan domain kontrol akses, hanya admin yang memiliki akses khusus pada Web SIMPEL dengan melakukan autentikasi berupa *username* dan *password*. Web SIMPEL ini merupakan web yang sifatnya terbuka untuk umum sehingga pengunjung dari luar lingkungan kampus juga dapat melakukan peminjaman lab melalui Web SIMPEL.

A.11 Keamanan Fisik dan Lingkungan

Berdasarkan domain tersebut, Web SIMPEL telah melakukan bentuk keamanan fisik dengan cara penguncian server. Pengamanan fisik server ini dilakukan secara ganda dengan penguncian tempat server dan penguncian ruangan letak server serta adanya pemantauan server melalui kamera CCTV.

A.16 Manajemen Insiden Keamanan Informasi

Berdasarkan domain manajemen insiden keamanan informasi, Web SIMPEL belum terdapat bentuk manajemen insiden keamanan informasi secara terstruktur. Hal ini dikarenakan belum adanya kendala dalam pengelolaan Web SIMPEL serta tidak adanya kebocoran data hingga saat ini.

Selanjutnya, dibentuk rekomendasi tata kelola yang dibuat berdasarkan hasil tabel *gap analysis* dan temuan-temuan pada Web SIMPEL yang belum memenuhi standar ISO 27001:2013 seperti pada Tabel 3.

Tabel 3. *Gap Analysis* Domain Kebijakan Keamanan Informasi

Domain	Klausul	Kondisi		Risiko
		Terkini	Global	
A.5	A.5.1.1	Belum adanya aturan keamanan informasi.	Adanya ketetapan keamanan informasi.	Apabila belum terdapat kebijakan keamanan informasi, memungkinkan terjadinya kebocoran data dan terganggunya kinerja web.

Rekomendasi Tabel 3 :

Berdasarkan domain kebijakan keamanan informasi, Web SIMPEL membutuhkan kebijakan yang dapat membantu pengendalian keamanan informasi.

Tabel 4. *Gap Analysis* Domain Manajemen Aset

Domain	Klausul	Kondisi Terkini	Global	Risiko
A.8	A.8.1.3	Tidak terdapat aturan dalam penggunaan Web SIMPEL, melainkan baru terdapat SOP mengenai pengelolaan laboratorium solusi.	Adanya ketetapan dalam penggunaan Web SIMPEL	Apabila belum terbentuk kebijakan tersebut maka akan memungkinkan terjadinya penyalahgunaan penggunaan informasi.

Rekomendasi Tabel 4 :
Berdasarkan domain manajemen aset, Web SIMPEL memerlukan kebijakan yang dapat berupa prosedur serta peraturan dalam penggunaan informasi. Peraturan dan prosedur tersebut dipergunakan untuk menjaga informasi yang dimiliki Web SIMPEL.

Tabel 5. *Gap Analysis* Domain Kontrol Akses

Domain	Klausul	Kondisi Terkini	Global	Risiko
A.9	A.9.1.1	Belum adanya autentikasi dan otorisasi kepada *user*.	Adanya autentikasi dan otorisasi kepada *user*.	Apabila belum adanya autentikasi dan otorisasi kepada *user*, memungkinkan adanya pihak yang tidak bertanggung jawab yang bisa menyebabkan penyalahgunaan penggunaan web.

Rekomendasi Tabel 5 :
Berdasarkan domain kontrol akses, Web SIMPEL perlu memiliki proses autentikasi dan otorisasi kepada *user* sehingga admin dapat mengenali apakah *user* merupakan pihak internal (dalam kampus) atau pihak eksternal.

Tabel 6. *Gap Analysis* Domain Keamanan Fisik dan Lingkungan

Domain	Klausul	Kondisi Terkini	Global	Risiko
A.11	A.11.1.3	Belum adanya pengamanan secara fisik selama 24 jam (security).	Adanya pengamanan secara fisik selama 24 jam (security).	Kemungkinan akan terjadi kerugian, kerusakan, pencurian, atau penguasaan tanpa hak akses, dan operasi organisasi dapat terganggu.

Rekomendasi Tabel 6 :
Berdasarkan keamanan fisik dan lingkungan, Lab Solusi perlu menerapkan pengamanan pada Web SIMPEL agar dapat mencegah hak akses yang tidak berwenang. Dengan begitu, keamanan perangkat keras dapat terjaga dan operasi organisasi dapat berjalan dengan lancar.

Tabel 7. ***Gap Analysis*** **Domain Manajemen Insiden Keamanan Informasi**

Domain	Klausul	Kondisi		Risiko
		Terkini	Global	
A.16	A.16.1.2	Tidak adanya proses pemberitahuan terkait keadaan keamanan dalam informasi kepada pihak berwenang	Adanya metode pelaporan terkait keadaan keamanan dalam informasi kepada pihak berwenang	Insiden keamanan informasi belum dapat diproses.
	A.16.1.3	Tidak adanya pelaporan dari pengguna Web SIMPEL mengenai kecurigaan kelemahan keamanan terhadap informasi yang digunakan.	Adanya proses pelaporan dari pengguna Web SIMPEL mengenai kelemahan keamanan informasi yang digunakan.	Kelemahan keamanan informasi akan terus dialami organisasi.
	A.16.1.4	Tidak adanya penilaian serta pengambilan keputusan mengenai pengkategori-an insiden keamanan dalam informasi.	Adanya pengukuran dan pengambilan keputusan mengenai pengklasifikasian peristiwa keamanan dalam informasi.	Pengklasifikasian insiden keamanan informasi akan terus mengalami kerancuan
	A.16.1.5	Tidak adanya prosedur mengenai tanggapan terhadap keamanan informasi	Adanya proses mengenai tanggapan terhadap keamanan informasi	Tidak ada acuan untuk menghadapi insiden ke-amanan informasi selanjutnya bagi organisasi.
	A.16.1.6	Belum dilakukannya analisis dan pencegahan mengenai insiden keamanan informasi.	Dilakukannya analisis dan pencegahan mengenai peristiwa keamanan informasi guna meminimalisir peluang atau akibat	Keamanan informasi tidak dapat ditingkatkan berdasarkan insiden keamanan yang pernah dialami karena tidak dilakukannya proses dokumentasi oleh organisasi.

		kejadian pada waktu mendatang.	
A.16.1.7	Belum dilakukannya proses dokumentasi yang dapat digunakan sebagai bukti.	Dilakukannya proses dokumentasi yang dapat digunakan sebagai bukti	Karena belum terdapat proses dokumentasi maka organisasi tidak memiliki bukti untuk menangani segala insiden keamanan yang terjadi.

Rekomendasi Tabel 7 :
Berdasarkan domain manajemen insiden keamanan informasi, diharapkan Web SIMPEL memiliki bentuk manajemen insiden keamanan informasi yang dapat membantu dalam pengelolaan web serta menjaga keamanan data pada Web SIMPEL.

4. KESIMPULAN DAN SARAN

Berdasarkan data yang telah dianalisis menggunakan ISO 27001:2013, Web SIMPEL belum memenuhi standar keamanan informasi ISO 27001:2013. Dengan adanya temuan yang diperoleh, beberapa domain yang belum sesuai standar ISO 27001:2013 dijabarkan pada tabel *gap analysis*. Tabel *gap analysis* ini berisikan kondisi web saat ini lalu kondisi global yang diharapkan serta risiko yang mungkin terjadi apabila domain tidak diterapkan. Hasil analisis ini dibentuk menjadi perancangan tata kelola berupa rekomendasi. Rekomendasi tersebut berupa saran pembuatan kebijakan keamanan informasi, manajemen risiko, serta kontrol akses. Dengan adanya rekomendasi tersebut, diharapkan dapat membantu pengembangan Web SIMPEL dalam mencapai standar ISO 27001:2013 khususnya dalam hal keamanan informasi.

Saran untuk penelitian selanjutnya yaitu dapat melakukan penjabaran pada klausul dalam domain sehingga dapat memperluas penelitian dan sumber data. Adanya perluasan sumber data dapat membantu peneliti selanjutnya menemukan data yang tidak hanya dari pengelolaan keamanan sistem informasi.

5. DAFTAR RUJUKAN

[1] M. R. Hamzah, "Audit Keamanan Sistem Informasi dengan Menggunakan Standar ISO/IEC 27002: 2013 dan ISO/IEC 27001: 2013 pada Sub Bagian Data dan Informasi Direktorat Jenderal Kebudayaan Republik Indonesia," *Skripsi,* p. 29, 2018.

[2] Ramadhani, S. R., & Wijaya, L. V. (2020). Journal of Applied Informatics and Computing (JAIC). *Journal of Applied Informatics and Computing (JAIC) Sistem Informasi Peminjaman Laboratorium pada Cross-Platform dengan Metode Prototyping (Studi Kasus: Politeknik Caltex Riau)*, 1.

[3] Tuga, M. A., Wasum, & Aziz, A. (2019). Seminar Nasional FST 2019 ~ Universitas Kanjuruhan Malang. *ANALISIS MANAJEMEN KEAMANAN SISTEM INFORMASI AKADEMIK UNIVERSITAS KANJURUHAN MALANG MENGGUNAKAN STANDAR ISO 27001:2013*, *2*.

[4] Rutanaji, D., Kusumawardani, S. S., & Winarno, W. W. (2017). Prosiding Seminar Nasional XII Rekayasa Teknologi Industri dan Informasi. *ISO 27001 Sebagai Metode Alternatif Bagi Perancangan Tata Kelola Keamanan Informasi (Sebuah Usulan Untuk Diterapkan di Arsip Nasional RI)*.

[5] Bakri, M., & Irmayana, N. (2017). Jurnal TEKNOKOMPAK. *ANALISIS DAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI SIMHP BPKP MENGGUNAKAN STANDAR ISO 27001*, *11*.

[6] Darmawan, Y. (2017). *Analisis Tata Kelola Keamanan Laboratorium Fakultas Teknologi Informmasi Universitas Kristen Satya Wacana Menggunakan Standart ISO 27001:2013*.
[7] Nasser, A. A. (2017). *Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen. International Journal of Scientific Research in Multidisciplinary Studies*, 3(11), 4-13.
[8] Basyarahil, F. A. (2017). Security management using indeks keamanan informasi (KAMI) based on ISO/IEC 27001:2013 at direktorat pengembangan teknologi dan sistem informasi (DPTSI) ITS Surabaya. 393.
[9] Muahidin, Z., Kusrini, & Nasiri, A. (2022). *Analisis Manajemen Keamanan Informasi Menggunakan Indeks Keamanan,* Volume 12 *No 2*, 2.
[10] PT Integra Teknologi Solusi, 2023. *Apa Saja Kesulitan Penerapan ISO 27001 dalam Perusahaan?* [Online] Available at: https://integrasolusi.com/blog/apa-saja-kesulitan-penerapan-iso-27001-dalam-perusahaan/ [Accessed 2 April 2023]
[11] Dicky Rutanaji, Sri Suning Kusumawardani, Wing Wahyu Winarno, "ISO 27001 SebagaiMetode Alternatif Bagi Perancangan Tata Kelola Keamanan Informasi (Sebuah Usulan Untuk Diterapkan di Arsip Nasional RI)," p. 169, 2017.
[12] Prasanti, D. (2018). JURNAL LONTAR. *PENGGUNAAN MEDIA KOMUNIKASI BAGI REMAJA PEREMPUAN DALAM PENCARIAN INFORMASI KESEHATAN*, 6, 16.
[13] PUJAASTAWA, I. B. G. (2016). *TEKNIK WAWANCARA DAN OBSERVASI UNTUK PENGUMPULAN BAHAN INFORMASI*.
[14] Azizi Algi, Agus H. S. Reksoprodjo, Rudy Agus G. Gultom3, "ANALISIS STANDAR ISO/IEC 27001: 2013 SEBAGAI STRATEGI KEAMANAN," *Jurnal Peperangan Asimetris* , vol. Volume 6 Nomor 2, p. 161, 2020.
[15] Sitta Rif'atul Musyarofah, Rahadian Bisma, "Analisis kesenjangan sistem manajemen keamanan informasi (SMKI)," *Jurnal Ilmiah Sistem Informasi* , 2021.
[16] Anton Purba, Mohammad Soetomo, "Assessing Privileged Access Management (PAM) using ISO 27001:2013 Control," *Proceedings of Annual Conference on Management and Information Technology (ACMIT),* p. 60, 2018.
[17] Yulianti, A., Rudianto, C., & Wijaya, A. F. (2018). Jurnal Sistem Informasi Indonesia (JSII). *Analisis dan Perancangan Tata Kelola Persandian Pengamanan Informasi Menggunakan Standar ISO 27001:2013 (Studi Kasus di Diskominfo Kota Salatiga)*, *3*.