CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 4, No. 1, Mei 2021, hlm. 38-43

PENGUKURAN RISIKO DAN EVALUASI KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI DI BKD XYZ BERDASARKAN ISO 27001 / SNI

Tri Rochmadi[1], Ike Yunia Pasa[2]

[1]Sistem Informasi, Fakultas Komputer, Universitas Alma Ata
[2]Teknologi Informasi, Fakultas Teknik, Universitas Muhammadiyah Purworejo
Email: [1]trirochmadi@almaata.ac.id, [2]ikeypasa@umpwr.ac.id

(Naskah masuk: 02 Mei 2021, diterima untuk diterbitkan: 31 Mei 2021)

Abstrak

Digitalisasi tidak bisa dihindari di era revolusi industri 4.0 termasuk di pemerintahan. Selain memberikan manfaat yang luar biasa pada sisi efisiensi dan efektiftas kerja, namun juga meninggalkan ancaman tentang data privasi atau keamanan informasi. Atas dasar ancaman yang dimungkinkan banyak terjadi akibat digitalisasi tersebut, maka perlu adanya pengukuran bagaimana keamanan informasi pada BKD XYZ agar bisa dijadikan evaluasi dan perbaikan. Hal ini dimaksudkan agar BKD XYZ bisa melindungi asset data dan informasi atau mencegah adanya serangan dari ancaman-ancaman yang mungkin saja terjadi. Metode yang digunakan dalam penelitian ini adalah dengan menggunakan Indeks KAMI sebagai tool pengukuran dan evaluasi keamanan informasi di BKD XYZ. Dari hasil penelitian yang dilakukan, bahwasanya BKD XYZ masih berada pada tingkat tidak layak untuk benar-benar bisa menerapkan keamanan informasi yang ideal. Sehingga dibutuhkan tindak lanjut sesuai rekomendasi perbaikan, agar BKD XYZ bisa mencapai kesiapan sertifikasi ISO 27001/SNI.

Kata kunci: *Indeks Keamanan Informasi, ISO 27001/SNI, Manajemen Risiko*

MEASUREMENT OF RISK AND EVALUATION OF INFORMATION SECURITY USING THE INFORMATION SECURITY INDEX IN BKD XYZ BASED ON ISO 27001 / SNI

Abstract

Digitalization is inevitable in the era of industrial revolution 4.0, including in government. Apart from providing tremendous benefits in terms of work efficiency and effectiveness, it also leaves threats about data privacy or information security. Based on threats that may occur due to digitalization, it is necessary to measure how the information in BKD XYZ can be used as evaluation and improvement. This is an alarm so that BKD XYZ can protect asset data and information or prevent attacks from possible threats. The method used in this study is to use the WE Index as a means of measuring and evaluating information in BKD XYZ. From the results of the research conducted, that BKD XYZ is still at an inadequate level to be able to implement ideal information security. So a follow-up recommendation for improvement is needed so that BKD XYZ can achieve ISO 27001 / SNI certification readiness.

Keywords: *Information Security Index, ISO 27001 / SNI, Risk Management*

1. PENDAHULUAN

Revolusi industri 4.0. saat ini sedang berkembang di Indonesia, selain itu untuk transparansi dan efisiensi kerja (Kohar & Putro, 2014). Adanya digitalisasi akibat dari revolusi industri 4.0 selain banyak manfaat, tentu juga harus dipertimbangkan dari sisi keamanan informasinya, terlebih BKD memiliki data pribadi yang sensitif jika sampai bocor. Belakangan ini kasus kejahatan siber marak terjadi, sehingga evaluasi keamanan informasi sangat diperlukan agar bisa memberikan gambaran tentang kesiapan dalam hal keamanan informasi tersebut dan juga untuk mencapai tata kelola (governance) yang baik (Riadi, Riyadi Yanto, & Handoyo, 2020). Diharapkan dengan evaluasi menggunakan Indeks Keamanan Informasi (KAMI) ini dapat memberikan kerangka kerja keamanan informasi bagi instansi sehingga meminimalkan kejahatan siber dan jika sampai terjadi kejahatan siber tersebut dapat dilakukan investigasi forensik digital dengan mudah dari kerangka kerja yang ada.

Keamanan informasi yang ada ini menyangkut unsur *CIA (Confidentiality, Integrity dan Availibility)* yaitu data yang telah diserahkan pegawai ke BKD haruslah dijamin kerahasiannya, data terjaga originalitasnya tanpa perubahan sepihak dan mudah diakses kembali karena tersedia dalam sistem yang baik (Pamungkas & Saputra, 2020). Unsur *CIA* dalam keamanan informasi tersebut haruslah dipatuhi, karena kajahatan siber sangat luas, seperti *ARP Spoofing* yang bisa digunakan oknum untuk mencuri data akun wifi yang ingin terhubung ke jaringan instansi (Sugiantoro, 2017).

Tujuan penelitian ini dilakukan untuk mengevaluasi tingkat keamanan informasi menggunakan Indeks Keamanan Informasi (KAMI) versi 4.1 yang dikeluarkan oleh (BSSN, 2019b). Evaluasi keamanan informasi dengan Indeks KAMI ini juga mengukur penerapannya jika ada insiden dapat dilakukan investigasi forensik digital yaitu proses investigasi jika terjadi kerancuan atau insiden kejahatan dalam perangkat komputer (Rochmadi, Wicaksono, & Nisa, 2020) dari identifikasi digital (Rochmadi, 2019). Selain itu evaluasi ini tidak hanya dalam hal teknis atau teknologi, namun juga dalam hal perilaku pengguna itu sendiri, karena jika fokus pada teknologinya saja investasi yang dikeluarkan tidak akan signifikan (Glaspie & Karwowski, 2018). Menurut (Katadata Insight Center & KOMINFO, 2020), Indonesia juga masih perlu literasi digital dan keamanan informasi, karena sering kita mendengar kasus pencurian, hoaks itu juga tidak luput dari unsur pengguna pada kategori kerangka kerja keamanan informasi. Hasil dari penelitian juga dapat diterapkan pada instansi lain terutama yang menyimpan data pribadi dan transaksi sensitif seperti keuangan, kesehatan dan lainnya yang menjadi landasan bisnis utamanya.

2. LANDASAN TEORI

2.1. Keamanan Informasi

Keamanan informasi mengacu pada proses dan metode bagaimana melindungi informasi terkait data privasi yang ada dari segala bentuk kejahatan siber (Matondang, Isnainiyah, & Muliawatic, 2018). Prinsip utama keamanan informasi terdiri dari *confidentiality* (kerahasiaan), *integrity* (integritas) pertimbangan yang sistematis dari (a) Hal yang dan *availability* (ketersediaan) atau sering disingkat *CIA* seperti pada gambar 1. Dalam keamanan informasi tersebut berusaha untuk menghindari dari berbagai serangan atau ancaman yang mungkin bisa terjadi dalam sistem elektronik.

Gambar 1. Prinsip Keamanan Informasi
Sumber : (Rizky, 2020)

2.2. Ancaman Serangan Siber

Jenis ancaman serangan siber sangat beragam dan banyak terjadi pada masa pandemic covid 19. Beberapa serangan yang sering terjadi adalah virus, *social engineering*, *hacker* atau bisa juga bencana (Siagian, 2016). Pada pola serangan *social engineering*, umumnya model lama yaitu melalui *phising* untuk mencuri data atau informasi yang kemudian bisa dilakukan *eksploitasi* dari informasi yang didapatkan (Afif, 2020).

2.3. Manajemen Risiko

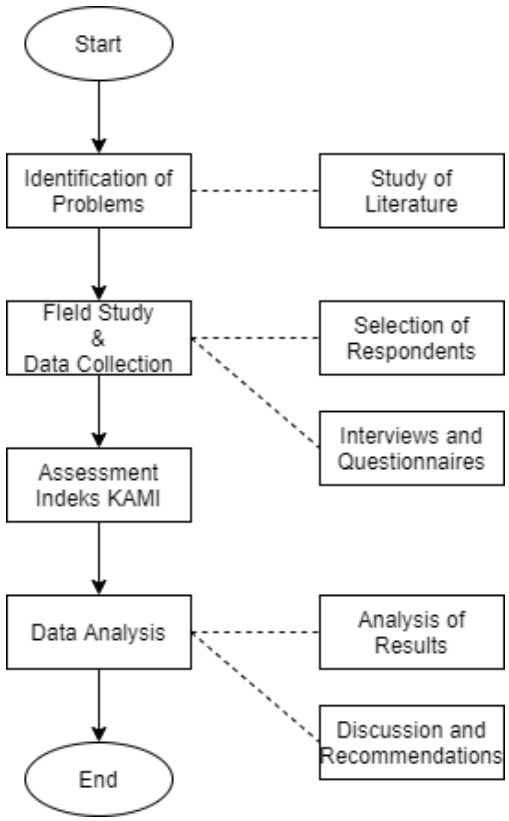
Dengan semakin masifnya kejahatan siber atau jenis serangan siber yang terjadi di berbagai lini termasuk pemerintahan, sehingga perlu adanya manajemen risiko yang diterapkan agar bisa meminimalkan kerugian atau kehilangan data yang vital. Ada beberapa jenis tahapan yang digunakan untuk manajemen risiko yang salah satunya adalah dimulai dengan penilaiain risiko, yang bisa juga menggunakan Indeks KAMI. Penilaian risiko merupakan sebuah pertimbangan yang sistematis dari hal-hal yang membahayakan bisnis mungkin akibat dari kegagalan keamanan informasi (Matondang et al., 2018).

2.4. Indeks KAMI

Indeks Keamanan Informasi (KAMI) adalah sebuah tool yang digunakan untuk membantu mendapatkan informasi terkait dan untuk mengukur tingkat kesiapan dari segi kelengkapan sampai dengan kematangan dalam penerapan keamanan informasi. Indeks keamanan informasi (KAMI) juga berdasarkan kriteria SNI ISO/IEC 27001, yaitu Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, Aspek Teknologi dengan suplemen Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan dan Perlindungan Data Pribadi. Penggunaan Indeks KAMI bisa digunakan sebagai tool dalam memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi (BSSN, 2019a).

3. METODE PENELITIAN

Penelitian ini dilakukan dalam 4 langkah yang meliputi: Identifikasi masalah dan studi literatur; studi lapangan dan pengumpulan data; penilaian Indeks KAMI; analisis hasil, pembahasan dan saran rekomendasi. Alur dari penilitian tersebut seperti yang terlihat pada gambar 2 di bawah.



Gambar 2. Metodologi Penelitian

Identifikasi masalah dilakukan pada BKD XYZ yang mana instansi tersebut sudah menerapkan digitalisasi atau sistem elektornik dalam hal penyimpanan sampai ke pengolahan data untuk mendukung kinerja yang lebih efektif dan efisien. BKD XYZ merupakan Badan Kepegawaian Daerah asli milik pemerintah yang menjadi objek penelitian ini sengaja dirahasiakan agar lebih privacy terutama bagi SDM TI yang ada pada BKD tersebut. Sejak pertama kali menerapkan sistem elektronik untuk kegiatan operasionalnya, BKD XYZ belum pernah menerapkan evaluasi terhadap keamanan informasi, sehingga peneliti melakukan studi literatur yang tepat untuk mengukur dan mengevaluasi keamanan informasi di BKD XYZ menggunakan pedoman Indeks KAMI.

Tahap studi lapangan dan pengumpulan data, pada tahap ini dengan melakukan observasi lapangan dan pengisian kuesioner yang berisi variable-variabel tentang keamanan informasi dari Indeks KAMI yang diisi oleh responden dari pejabat IT di lingkungan BKD tersebut. Pemilihan responden adalah pejabat IT agar informasi yang didapatkan valid dan bisa sebagai rekomendasi yang tepat atas apa yang ada di lingkungan BKD terkait sistem elektronik di BKD tersebut.

Tahap penilaian dengan pedoman Indeks KAMI meliputi Sistem Elektronik, Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Pengelolaan Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi dan Suplemen. Dari masing-masing kategori tersebut berisi variable-variable yang juga diselaraskan dengan ISO/IEC 27001.

Terakhir adalah tahap analisis hasil yang dilanjutkan dengan pembahasan dan saran rekomendasi dari hasil penilaian dan analisis, agar BKD memiliki kerangka kerja yang lebih baik untuk keamanan informasi di lingkungan BKD yang tentu riskan akan adanya data yang bersifat krusial karena data pribadi dan keuangan.

4. HASIL DAN PEMBAHASAN

Pada proses penilaian ini terbagi menjadi 3 kategori yaitu kategori sistem elektronik, kategori 5 area keamanan informasi dan kategori suplemen.

4.1. Hasil Penilaian Sistem Elektronik

Proses penilaian pada kategori sistem elektronik di BKD XYZ diperoleh hasil dengan nilai skor 19. Skor tersebut menurut Indeks KAMI bahwa sistem elektronik berada pada posisi tinggi, sebagaimana ditunjukkan pada tabel 1.

Tabel 1. Skor Kategori Sistem Elektronik

Kategori Sistem Elektronik	Skor
Rendah	10 – 15
Tinggi	16 – 34
Strategis	35 – 50

4.2. Hasil Penilaian 5 Area Keamanan Informasi

Penilaian pada 5 area keamanan informasi meliputi: tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan aset informasi serta teknologi dan keamanan informasi. Hasil penilaian didapatkan skor terendah pada kategori pengelolaan risiko keamanan informasi dengan nilai 13 dan paling tinggi pada kategori pengelolaan aset informasi dengan nilai 46. Sedangkan skor penilaian di BKD XYZ pada kategori yang lain dan detail keseluruhan skor penilaian ditunjukkan pada tabel 2.

Tabel 2. Penilaian Kategori 5 Area Keamanan Informasi di BKD XYZ

No	Kategori Area Keamanan Informasi	Nilai
1	Tata kelola keamanan informasi	**30**
2	Pengelolaan risiko keamanan informasi	**13**
3	Kerangka kerja pengelolaan	**33**

No	Kategori Area Keamanan Informasi	Nilai
	keamanan informasi	
4	Pengelolaan aset informasi	**46**
5	Teknologi dan keamanan informasi	**39**

4.3. Hasil Penilaian Suplemen

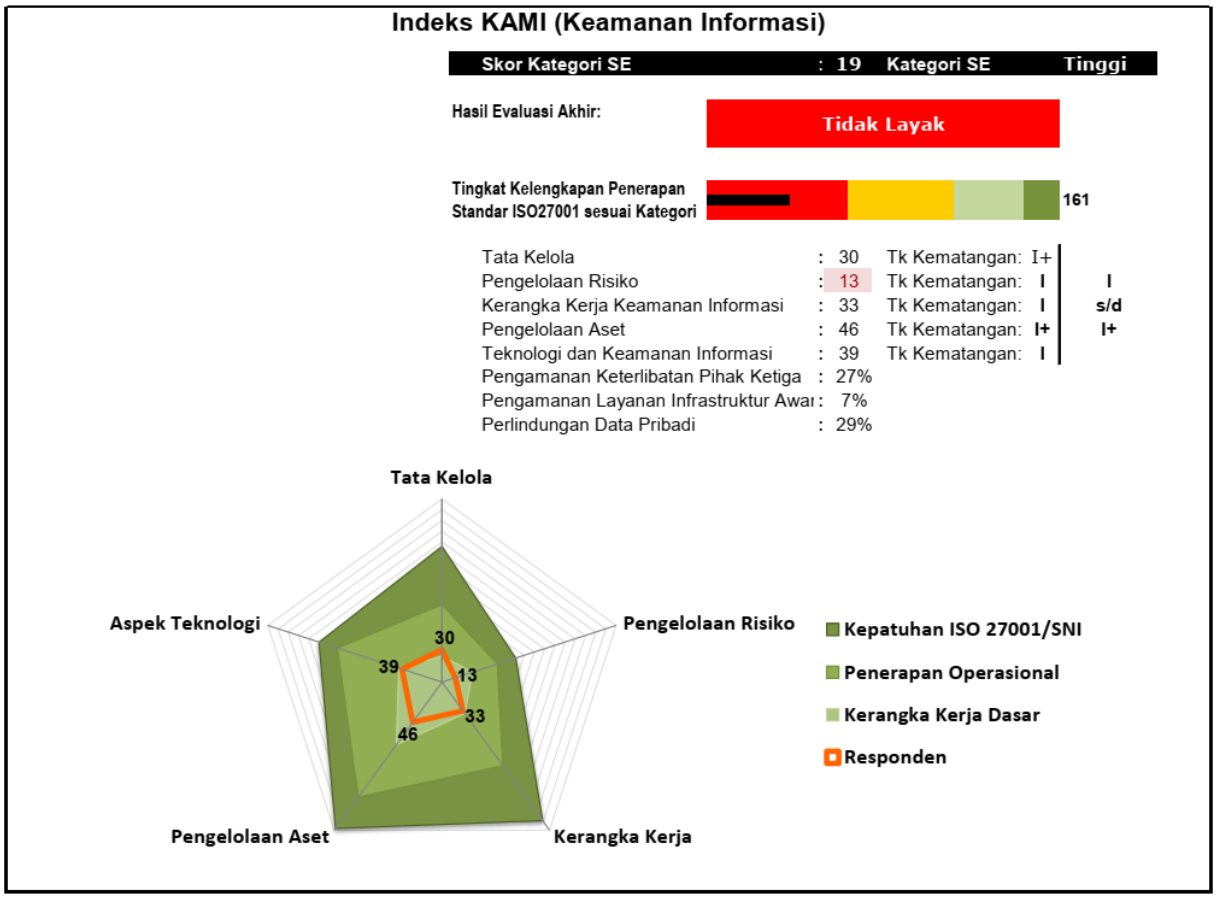
Kategori suplemen terdapat 3 bagian yang dinilai, yaitu: pengamanan keterlibatan pihak ketiga penyedia layanan, pengamanan layanan infrastruktur awan (*cloud service*) dan perlindungan data pribadi. Dari hasil penilaian pada kategori suplemen diperoleh skor 27% pada keterlibatan pihak ketiga, 7% pada layanan infrastruktur awan dan 29 % pada perlindungan data pribadi.

Tabel 3. Penilaian Kategori Suplemen

No	Kategori Suplemen	Nilai
1	Pengamanan keterlibatan pihak ketiga penyedia layanan	**27%**
2	Pengamanan layanan infrastruktur awan (cloud service)	**7%**
3	Perlindungan data pribadi	**29%**

4.4. Hasil Akhir Penilaian

Hasil evaluasi akhir yang diperoleh pada BKD XYZ menggunakan Indeks KAMI yang juga berdasarkan pada ISO 27001/SNI berada pada level tidak layak. Hal tersebut didasarkan pada penilaian lebih banyak berada pada level tingkat kematangan I sebanyak 3 kali dan tingkat kematangan pada level I+ lebih sedikit yaitu 2 kali. Hasil analisa dari tingkat kematangan tersebut diperoleh nilai 161 yang artinya adalah tidak layak dalam hal status kesiapan penerapan keamanan informasi yang ada di BKD XYZ, seperti pada gambar 3.



Gambar 3. Hasil Penilaian BKD XYZ pada Dashboard Indeks KAMI

Penjelasan terkait hasil analisa pada dashboard Indeks KAMI, berdasarkan pada pengelompokan pada tabel 4.

Tabel 4. Tabel Penilaian Indeks KAMI

Rendah		Skor Akhir		Status
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Kerja
		313	535	Cukup Baik
		536	645	Baik
Tinggi		**Skor Akhir**		**Status**
16	34	0	272	Tidak Layak
		273	455	Pemenuhan

				Kerangka Kerja
		456	583	Cukup Baik
		584	645	Baik
Strategis		**Skor Akhir**		**Status**
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja
		536	609	Cukup Baik
		610	645	Baik

Hasil analisa sebagaimana pada dashboard gambar 3, didapatkan kategori sistem elektronik pada level tinggi di antara range nilai 16-34 yaitu memiliki nilai 19. Dengan menggunakan acuan pada tabel 4, BKD XYZ masih dikategorikan tidak layak dalam pemenuhan keamanan informasi, karena hasil skor akhir dari 5 kategori area keamanan informasi diperoleh range skor 0-272 yaitu skornya 161.

4.5. Rekomendasi Perbaikan

Berdasarkan hasil penilaian yang diperoleh sesuai dengan gambar 3, bahwa BKD XYZ masih dikategorikan tidak layak, sehingga perlu banyak perbaikan yang harus dipenuhi supaya naik statusnya menjadi cukup baik di antaranya:

1. Instansi memberikan update kemampuan dan pemahaman kepada SDM terkait seputar keamanan informasi.
2. SDM penanggungjawab membuat kerangka kerja yang baik dan didokumentasikan, serta diterapkan secara berkala di masing-masing unit.
3. SDM melakukan kajian terhadap *business impact analysis (BIA)* yaitu suatu proses menentukan dan mendokumentasikan dampak bisnis dari gangguan terhadap kegiatan yang mendukung produk dan layanan utama.
4. Instansi harus mendukung dan menyegerakan dari kerangka kerja yang sifatnya masih dalam perencanaan.
5. Instansi secara rutin mendorong SDM penanggungjawab melakukan analisa minimal per tahun sekali terkait semua konfigurasi yang ada.
6. SDM membuat tata tertib, peraturan dan ketetapan terkait dengan asset infrastruktur, perangkat lunak dan standarisasi *backup* data.
7. Melakukan analisa log yang dihasilkan dari semua proses yang terjadi pada sistem di BKD XYZ untuk memastikan amannya data dan sebagai bukti dari insiden respon, jika forensik digital diperlukan.

5. KESIMPULAN DAN SARAN

Hasil penilaian instansi BKD XYZ dalam pengukuran risiko dan penilaian keamanan informasi berada pada level tidak layak, yang mana pada kategori sistem elektronik 19 atau tinggi. namun pada kategori tinggi tersebut, BKD XYZ belum mengimbangi pada 5 area keamanan informasi yaitu di nilai 161. Dari 5 area keamanan informasi yang sudah pada level kematangan I+ hanya di tata kelola dan pengelolaan aset, lainnya masih di level kematangan I. Sehingga disarankan BKD XYZ untuk segera melakukan banyak perbaikan sesuai dengan saran rekomendasi yang telah diberikan atau bisa langsung menyesuaikan dengan pedoman indeks keamanan informasi pada tingkat III agar mencapai kesiapan sertifikasi ISO 27001/SNI.

Rekomendasi perbaikan tersebut juga bisa menjadi perhatian bagi pengelola TI pada instansi lain. Perbaikan-perbaikan perlu dievaluasi dan dikaji terutama untuk instansi yang menyimpan data atau informasi pribadi ataupun yang bersifat kritis seperti transaksi, keuangan dan kesehatan.

Penelitian selanjutnya perlu adanya evaluasi kembali menggunakan indeks keamanan informasi jika rekomendasi telah diterapkan. Evaluasi tersebut bisa dengan membandingkan framework lain seperti NIST ataupun COBIT untuk mendapatkan hasil dan rekomendasi perbaikan yang lebih baik.

DAFTAR PUSTAKA

AFIF, M. N. (2020). KEAMANAN INFORMASI DI RUMAH SAKIT. *Jurnal Sabhanga*, *2*(1), 18–29. Retrieved from http://e-journal.stikessatriabhakti.ac.id/index.php/sbn1/article/view/21/21

BSSN. (2019a). *Indeks KAMI Versi 4*.

BSSN. (2019b). INDEKS KEAMANAN INFORMASI (KAMI). Retrieved from Bagian Komunikasi Publik, Biro Hukum dan Hubungan Masyarakat – BSSN website: https://bssn.go.id/indeks-kami/

GLASPIE, H. W., & KARWOWSKI, W. (2018). Human factors in information security culture: A literature review. *Advances in Intelligent Systems and Computing*, *593*, 267–280. https://doi.org/10.1007/978-3-319-60585-2_25

KATADATA INSIGHT CENTER, & KOMINFO. (2020). *Status Literasi Digital Indonesia 2020*.

KOHAR, A., & PUTRO, H. P. (2014). Ancaman Keamanan pada Sistem Informasi Manajemen Rumah Sakit. *Seminar Nasional Informatika Medis (SNIMed)*, 114–120.

MATONDANG, N., ISNAINIYAH, I. N., & MULIAWATIC, A. (2018). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *2*(1), 282–287. https://doi.org/10.29207/resti.v2i1.96

PAMUNGKAS, W. C., & SAPUTRA, F. T. (2020).

Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *1*(2), 101. https://doi.org/10.30865/json.v1i2.1924

RIADI, I., RIYADI YANTO, I. T., & HANDOYO, E. (2020). Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI). *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *5*(4), 1–9. https://doi.org/10.22219/kinetik.v5i4.1083

RIZKY, M. (2020). Confidentiality, Integrity and Availability – The CIA Triad. Retrieved from CV. Garuda Sarana Sejahtera (GSS) website: https://klikgss.com/2020/12/18/confidentiality-integrity-and-availability-the-cia-triad/

ROCHMADI, T. (2019). Deteksi Bukti Digital Pada Adrive Cloud Storage Menggunakan Digital Evidence Detection in Adrive Cloud Storage Using Live. *CyberSecurity Dan Forensik Digital*, *2*(2), 21–24.

ROCHMADI, T., WICAKSONO, Y., & NISA, N. D. (2020). Digital Evidence Identification of Android Device using Live Forensics Acquisition on Cloud Storage (iDrive). *International Journal of Computer Applications*, *175*(26), 40–43. https://doi.org/10.5120/ijca2020920815

SIAGIAN, S. (2016). Analisis ancaman keamanan pada sistem informasi manajemen di rumah sakit rimbo medica jambi 2015. *SCIENTIA JOURNAL*, *4*(04), 371–375. Retrieved from https://www.neliti.com/id/publications/286618/analisis-ancaman-keamanan-pada-sistem-informasi-manajemen-di-rumah-sakit-rimbo-m%0Ahttp://www.academia.edu/download/57094957/163-Article_Text-265-1-10-20180417.pdf

SUGIANTORO, B. (2017). *Analisis Tingkat Keamanan pada Dinas XYZ Terhadap Serangan Pengguna Wifi*. 18–19.