JCI
Jurnal Cakrawala Ilmiah
Vol.3, No.10, Juni 2024

EVALUASI KEAMANAN INFORMASI PERGURUAN TINGGI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) VERSI 5.0

Oleh
Muhammad Rizkillah
Prodi S1 Sistem Teknologi dan Informasi, Fakultas Teknik, Universitas Muhammadiyah Mataram
Email: ryzkillah@ummat.ac.id

Article History:
Received: 21-05-2022
Revised: 03-06-2024
Accepted: 24-06-2024

Keywords:
Evaluasi Keamanan Informasi, Indeks Keamanan Informasi, KAMI 5.0, Perlindungan Data, Sistem Elektronik

Abstract: *Dalam era digital yang dipengaruhi oleh sistem informasi, evaluasi keamanan informasi di organisasi menjadi sangat penting untuk mengidentifikasi kerentanan, risiko potensial, memastikan kepatuhan terhadap peraturan, dan mendukung budaya kesadaran keamanan serta keselarasan dengan tujuan strategis organisasi. Indeks KAMI, mengacu pada standar ISO/IEC 27001:2013, terbukti sebagai alat evaluasi yang efektif untuk meningkatkan keamanan informasi di berbagai organisasi. Penelitian ini menggunakan metode studi kasus untuk mengevaluasi tingkat keamanan informasi di perguruan tinggi XYZ melalui berbagai kategori seperti Sistem Elektronik, Tata Kelola Keamanan Informasi, Pengelolaan Risiko, Kerangka Kerja Pengelolaan Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi, Pelindungan Data Pribadi (PDP), dan Suplemen. Hasil evaluasi menunjukkan bahwa keamanan informasi di perguruan tinggi masih banyak berada dalam level Kondisi Awal atau Penerapan Kerangka Kerja Dasar. Upaya lanjutan perlu dilakukan untuk meningkatkan keamanan informasi sesuai standar, demi menjaga integritas, ketersediaan, dan kerahasiaan data sensitif di lingkungan perguruan tinggi.*

PENDAHULUAN

Dalam era digital saat ini, di mana organisasi sangat mengandalkan sistem informasi untuk menjalankan operasional organisasi, pentingnya menilai keamanan informasi organisasi sangatlah besar. Evaluasi keamanan informasi dalam suatu organisasi memiliki kepentingan yang signifikan karena beberapa alasan. Pertama, hal ini membantu dalam mengidentifikasi kerentanan dan potensi risiko yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan informasi sensitif (Tu et al., 2018). Dengan melakukan evaluasi, organisasi dapat secara proaktif mengatasi kelemahan ini dan menerapkan kontrol keamanan yang tepat untuk memitigasi ancaman.

Selain itu, mengevaluasi keamanan informasi organisasi sangat penting untuk memastikan kepatuhan terhadap persyaratan peraturan dan standar industri. Organisasi yang gagal memenuhi standar ini tidak hanya berisiko menghadapi konsekuensi hukum tetapi juga rusaknya reputasi dan hilangnya kepercayaan pelanggan (Muhasin et al., 2022). Oleh karena itu, evaluasi rutin membantu dalam menilai kepatuhan organisasi terhadap

protokol dan pedoman keamanan, sehingga memungkinkan mereka melakukan penyesuaian yang diperlukan agar tetap patuh.

Selain itu, evaluasi keamanan informasi sangat penting untuk menumbuhkan budaya kesadaran keamanan dalam organisasi (Voitsekhovska et al., 2022). Penelitian telah menunjukkan bahwa budaya keamanan informasi karyawan memainkan peran penting dalam menjaga data organisasi (Voitsekhovska et al., 2022). Dengan mengevaluasi budaya keamanan yang ada, organisasi dapat mengidentifikasi area yang perlu ditingkatkan dan menerapkan program pelatihan untuk meningkatkan pemahaman karyawan tentang praktik terbaik keamanan.

Selain itu, mengevaluasi keamanan informasi sangat penting untuk menyelaraskan langkah-langkah keamanan dengan tujuan strategis organisasi (Tu et al., 2018). Hal ini memastikan bahwa kontrol keamanan tidak hanya efektif dalam melindungi data tetapi juga mendukung tujuan organisasi secara keseluruhan. Penyelarasan strategis ini membantu mengoptimalkan alokasi sumber daya dan memprioritaskan inisiatif keamanan berdasarkan kebutuhan spesifik dan profil risiko organisasi.

Salah satu aplikasi dalam mengevaluasi kemanan informasi adalah Indeks KAMI. Indeks KAMI adalah sebuah aplikasi yang digunakan untuk mengevaluasi dan mengukur tingkat kematangan serta kelengkapan keamanan informasi. Aplikasi ini telah disesuaikan dengan standar ISO/IEC 27001:2013 dan dikembangkan oleh Kementerian Komunikasi dan Informatika.

Beberapa penelitian telah dilakukan untuk menerapkan Indeks KAMI dalam berbagai konteks organisasi, diantaranya adalah Prasetyowati et al. (2019) membahas evaluasi manajemen keamanan informasi menggunakan Indeks KAMI berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang. Prasetyowati et al. (2019) menyoroti pentingnya aplikasi ini dalam mengukur keamanan informasi sesuai dengan standar yang berlaku. Sedangkan Rochmadi & Pasa (2021) mengukur risiko dan mengevaluasi keamanan informasi di BKD XYZ dengan menggunakan Indeks KAMI. Rochmadi & Pasa (2021) juga menjelaskan bahwa metode ini efektif sebagai alat untuk mengukur dan mengevaluasi keamanan informasi dalam suatu entitas. Penelitian Pamungkas & Saputra (2020) yang mengevaluasi keamanan informasi di SMAN 1 Sentolo berdasarkan Indeks KAMI dengan menyoroti bahwa penerapan evaluasi ini dapat dilakukan di berbagai instansi dengan mempertimbangkan kategori pertanyaan yang relevan dalam setiap area evaluasi. Wijaya (2021) juga membahas evaluasi keamanan sistem informasi Pasdeal berdasarkan Indeks KAMI. Wijaya (2021) menguraikan kerangka kerja dari Indeks KAMI yang mencakup evaluasi sistem elektronik, tata kelola, risiko, pengelolaan aset, teknologi, dan aspek lain yang relevan dalam manajemen keamanan informasi. Dari berbagai penelitian tersebut, dapat disimpulkan bahwa Indeks KAMI merupakan alat yang efektif dalam mengukur dan mengevaluasi keamanan informasi berdasarkan standar ISO/IEC 27001:2013. Aplikasi ini dapat diterapkan di berbagai jenis organisasi untuk meningkatkan tingkat keamanan informasi.

LANDASAN TEORI

Keamanan Informasi

Keamanan informasi adalah komponen penting dalam organisasi modern, yang

melibatkan langkah-langkah untuk melindungi data sensitif dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah. Berbagai perspektif dan definisi keamanan informasi telah diajukan dalam literatur akademis.

Lundgren dan Möller (2017) memperkenalkan konsep *Appropriate Access* sebagai definisi baru keamanan informasi, menekankan pentingnya memastikan individu memiliki akses yang sesuai terhadap informasi, menyoroti perlunya keseimbangan antara aksesibilitas dan keamanan untuk mencegah pengungkapan atau modifikasi yang tidak sah data.

Selain itu, Ghasemi dkk. (2017) membahas konsep keamanan tanpa syarat dalam konteks skema berbagi multirahasia, dengan fokus pada pemanfaatan teori informasi untuk mendefinisikan keamanan skema dan menekankan kekuatan langkah-langkah keamanan untuk menjaga kerahasiaan dan melindungi informasi dari pelaku jahat.

Veiga dkk. (2020) mengeksplorasi peran budaya keamanan informasi organisasi dalam memitigasi risiko yang terkait dengan faktor manusia dalam perlindungan informasi, menekankan pentingnya menumbuhkan budaya keamanan informasi yang kuat dalam organisasi untuk mengurangi kemungkinan pelanggaran dan insiden data.

Dari penjelasan diatas dapat disimpulkan keamanan informasi melibatkan pendekatan multifaset yang mencakup langkah-langkah teknis, budaya organisasi, manajemen akses, dan kerangka keamanan yang kuat. Dengan mempertimbangkan berbagai definisi dan perspektif, organisasi dapat mengembangkan strategi komprehensif untuk menjaga aset informasi mereka secara efektif.

Indeks KAMI versi 5.0

Indeks KAMI adalah suatu alat evaluasi yang digunakan untuk menganalisis sejauh mana tingkat kesiapan keamanan informasi di sebuah organisasi. Alat evaluasi ini bukan bertujuan untuk menilai apakah bentuk pengamanan yang ada sudah layak atau efektif, tetapi lebih sebagai sarana untuk memberikan gambaran tentang kondisi kesiapan (kompletude dan kedewasaan) kerangka kerja keamanan informasi kepada pimpinan Instansi/Perusahaan. Evaluasi dilakukan terhadap berbagai area yang menjadi fokus implementasi keamanan informasi dengan cakupan pembahasan yang memenuhi semua aspek keamanan yang telah didefinisikan dalam standar ISO/IEC 27001:2013.

Bentuk evaluasi yang diadopsi oleh indeks KAMI didesain untuk dapat diaplikasikan oleh organisasi dari berbagai ukuran, tingkat, dan tingkat kepentingan penggunaan Teknologi Informasi dan Komunikasi (TIK) dalam mendukung berjalannya proses organisasi. Data yang dihasilkan dari evaluasi ini akan memberikan gambaran singkat tentang tingkat kelengkapan dan kedewasaan kerangka kerja keamanan informasi yang diterapkan, dan dapat digunakan sebagai acuan untuk menyusun strategi perbaikan serta menetapkan prioritasnya.

Alat evaluasi ini juga dapat digunakan secara berkala untuk melacak perubahan kondisi keamanan informasi yang disebabkan oleh program kerja yang dilakukan, sambil memberikan informasi tentang peningkatan kesiapan kepada pihak terkait (*stakeholders*).

Indeks KAMI versi 5.0 merupakan versi terbaru dari versi sebelumnya yakni versi 4.2 yang diterbitkan pada Maret 2023. Area evaluasi teknologi informasi pada Indeks KAMI 5.0 meliputi kategori sistem elektronik, tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, teknologi dan keamanan informasi, perlindungan data pribadi, pengamanan keterlibatan

pihak ketiga.

Beberapa aspek dalam pengukuran yang digunakan dalam metode pengukuran Indeks KAMI versi 5.0, adalah :

1. Tata Kelola keamanan informasi mencakup penetapan arah strategis, memastikan tujuan tercapai, dan mengawasi manajemen risiko. Mengevaluasi keamanan informasi dalam kerangka tata kelola memastikan keselarasan antara strategi keamanan dan tujuan organisasi, menetapkan akuntabilitas, mendefinisikan peran, dan mengalokasikan sumber daya secara efektif (Shouran et al., 2019).
2. Manajemen Risiko yang efektif sangat penting untuk mengidentifikasi, menilai, dan memprioritaskan risiko terhadap aset informasi organisasi. Mengevaluasi keamanan informasi dalam manajemen risiko memungkinkan penerapan pengendalian untuk memitigasi risiko yang teridentifikasi, membantu pengambilan keputusan berdasarkan tingkat toleransi risiko dan strategi respons terhadap potensi ancaman (Tristian & Wibowo, 2020).
3. Kerangka Keamanan Informasi menawarkan pendekatan terstruktur untuk menerapkan, mengelola, dan memantau kontrol keamanan. Mengevaluasi keamanan informasi dalam kerangka ini memastikan kepatuhan terhadap standar industri, persyaratan peraturan, dan praktik terbaik, membantu menilai efektivitas langkah-langkah keamanan dan mengidentifikasi area yang perlu ditingkatkan (Singh & Joshi, 2018).
4. Manajemen Aset melibatkan identifikasi, pengklasifikasian, dan pengelolaan aset informasi organisasi. Mengevaluasi keamanan informasi dalam manajemen aset memastikan aset penting terlindungi secara memadai, memahami nilai aset, menilai risiko terkait, dan menerapkan perlindungan yang tepat terhadap potensi ancaman (Febriana et al., 2022).
5. Teknologi dan Keamanan Informasi, teknologi merupakan bagian integral dari keamanan informasi, dan mengevaluasi keamanan solusi teknologi sangat penting untuk menjaga data dan sistem. Menilai keamanan informasi dalam lanskap teknologi melibatkan evaluasi efektivitas kontrol keamanan, mengidentifikasi kerentanan, dan memastikan ketahanan teknologi terhadap ancaman dunia maya (Tristian & Wibowo, 2020).
6. Perlindungan Data Pribadi, melindungi data pribadi sangat penting untuk keamanan informasi. Mengevaluasi keamanan informasi terkait perlindungan data pribadi melibatkan kepatuhan terhadap peraturan perlindungan data, penerapan mekanisme enkripsi, dan memastikan praktik penanganan data yang aman untuk membangun kepercayaan dengan pemangku kepentingan dan mengurangi risiko pelanggaran data (Yu et al., 2016).
7. Menjaga Keterlibatan Pihak Ketiga, hubungan pihak ketiga menimbulkan risiko keamanan bagi organisasi. Mengevaluasi keamanan informasi terkait keterlibatan pihak ketiga mencakup penilaian postur keamanan vendor, mitra, dan penyedia layanan untuk memastikan kepatuhan terhadap standar keamanan, kewajiban kontrak, dan persyaratan perlindungan data (Tristian* & Wibowo, 2020).

METODE PENELITIAN

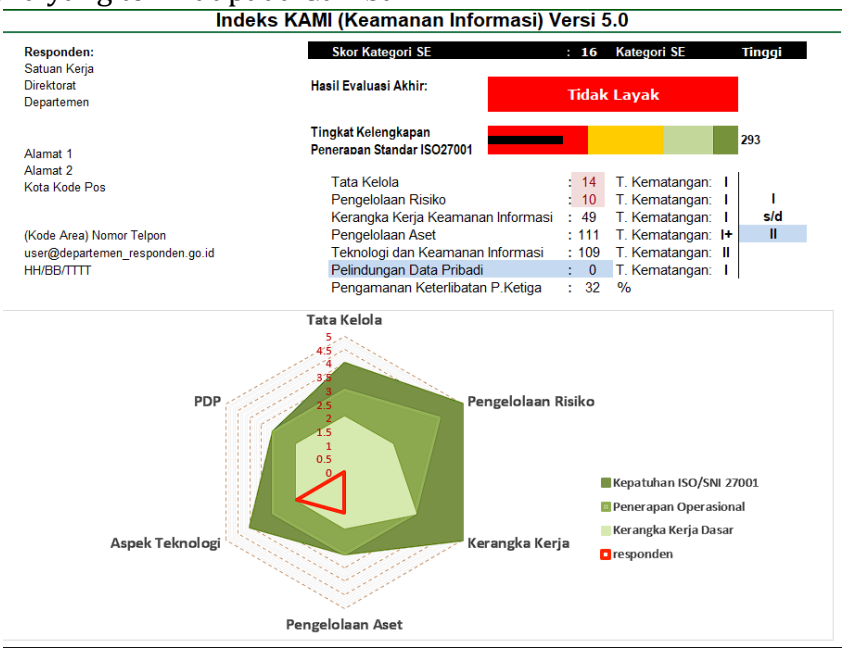
Penelitian ini menggunakan metode studi kasus tingkat keamanan informasi di perguruan tinggi XYZ yang bertujuan untuk memahami fenomena keamanan informasi

secara mendalam. Metode ini dilakukan dengan mengumpulkan data dengan cara wawancara dan observasi dari berbagai sumber yang sesuai dengan penelitian. Data yang terkumpul akan dianalisis untuk menghasilkan pemahaman yang mendalam (Assyakurrohim et al., 2022).

Tim satuan kerja Teknologi Informasi dan Komunikasi (TIK) akan diwawancarai dengan menggunakan panduan dari Indeks KAMI versi 5.0 sebagai acuan, dan evaluasi akan dilakukan sesuai dengan pedoman yang terdapat dalam Indeks KAMI tersebut. Proses penilaian dilakukan melalui pengisian kuesioner yang telah disiapkan, di mana setiap jawaban akan memiliki bobot nilai tertentu sesuai dengan Indeks KAMI. Indeks KAMI menyajikan metode dan rumus untuk menganalisis data yang telah dikumpulkan dan mencerminkan kondisi keamanan informasi perguruan tinggi secara keseluruhan (Faradhiya Aulia Rahmaet al., 2023).

HASIL DAN PEMBAHASAN

Hasil dari perhitungan menggunakan aplikasi Indeks KAMI versi 5.0 terdapat pada halaman Dashboard yang terlihat pada Gambar 1.



Gambar 1. Hasil Penilaian di Halaman Dashboard

Pada Gambar 1 terlihat bahwa Hasil Evaluasi Akhir adalah Tidak Layak dengan nilai 293. Terdapat 9 (sembilan) kategori yang dihitung dalam Indeks KAMI versi 5.0, yaitu

1. Kategori Sistem Elektronik (SE)
   Bagian ini digunakan untuk mengevaluasi tingkat atau kategori SE yang digunakan. Dalam penilaian kategori SE digunakan 3 (tiga) standar yang terlihat pada Gambar 2.

KATEGORI SISTEM ELEKTRONIK				
Rendah		Skor Akhir		Status Kesiapan
10	15	0	247	Tidak Layak
		248	443	Pemenuhan Kerangka Kerja Dasar
		444	760	Cukup Baik
		761	916	Baik
Tinggi		Skor Akhir		Status Kesiapan
16	34	0	387	Tidak Layak
		388	646	Pemenuhan Kerangka Kerja Dasar
		647	828	Cukup Baik
		829	916	Baik
Strategis		Skor Akhir		Status Kesiapan
35	50	0	472	Tidak Layak
		473	760	Pemenuhan Kerangka Kerja Dasar
		761	864	Cukup Baik
		865	916	Baik

Gambar 2. Standar penilaian Kategori Sistem Elektronik

Hasil penilaian keamanan informasi perguruan tinggi XYZ memiliki skor 16 yang berarti bahwa tingkat ketergantungan perguruan tinggi XYZ dalam menjalankan proses bisnis terhadap sistem elektronik termasuk Tinggi dengan Status Kesiapan Tidak Layak yang terlihat dari Skor Akhir 293.

2. Tata Kelola Keamanan Informasi

   Bagian ini digunakan untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi perguruan tinggi XYZ beserta fungsi, tugas dan tanggung jawab pengelola. Pengelompokkan standar penilaian dilakukan berdasarkan tingkat kematangan penerapan keamanan informasi. Tingkat kematangan terbagi atas 5 (lima) tingkat yang terlihat pada Tabel 1.

Tabel 1. Tingkat Kematangan

No	Tingkat	Keterangan
1	Tingkat I	Kondisi Awal
2	Tingkat II	Penerapan Kerangka Kerja Dasar
3	Tingkat III	Terdefinisi dan Konsisten
4	Tingkat IV	Terkelola dan Terukur
5	Tingkat V	Optimal

   Hasil penilaian keamanan informasi perguruan tinggi XYZ dalam kategori Tata Kelola memiliki skor 14 dengan tingkat kematangan I yang artinya masih dalam level Kondisi Awal.

3. Pengelolaan Risiko Keamanan Informasi

   Bagian ini digunakan untuk mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.

   Hasil penilaian keamanan informasi perguruan tinggi XYZ dalam kategori Pengelolaan Risiko memiliki skor 10 dengan tingkat kematangan I yang artinya masih dalam level Kondisi Awal.

4. Kerangka Kerja Pengelolaan Keamanan Informasi

   Bagian ini digunakan untuk mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan dan prosedur) pengelolaan keamanan informasi dan strategi penerapannya.

   Hasil penilaian keamanan informasi perguruan tinggi XYZ dalam kategori Kerangka Kerja memiliki skor 49 dengan tingkat kematangan I yang artinya masih dalam level Kondisi Awal.

5. Pengelolaan Aset Informasi

   Bagian ini digunakan untuk mengevaluasi kelengkapan pengamanan aset informasi,

termasuk keseluruhan siklus penggunaan aset.
Hasil penilaian keamanan informasi perguruan tinggi XYZ dalam kategori Pengelolaan Aset memiliki skor 111 dengan tingkat kematangan I+ yang artinya masih dalam level Kondisi Awal.

6. Teknologi dan Keamanan Informasi
   Bagian ini digunakan untuk mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.
   Hasil penilaian keamanan informasi perguruan tinggi XYZ dalam kategori Teknologi memiliki skor 109 dengan tingkat kematangan II yang artinya masih dalam level Penerapan Kerangka Kerja Dasar.
7. Pelindungan Data Pribadi (PDP)
   Bagian ini digunakan untuk mengevaluasi kelengkapan, konsistensi dan efektifitas penerapan kontrol keamanan terkait PDP.
   Hasil penilaian keamanan informasi perguruan tinggi XYZ dalam kategori PDP memiliki skor 0 dengan tingkat kematangan I yang artinya masih dalam level Kondisi Awal.
8. Suplemen
   Bagian ini digunakan untuk mengevaluasi kelengkapan, konsistensi dan efektifitas penerapan mekanisme keamanan informasi terkait risiko keterlibatan pihak ketiga eksternal.
   Hasil penilaian keamanan informasi perguruan tinggi XYZ dalam kategori Suplemen memiliki skor adalah 32%.

KESIMPULAN

Hasil evaluasi keamanan informasi perguruan tinggi XYZ dengan menggunakan aplikasi Indeks KAMI versi 5.0 dapat disimpulkan bahwa pengelolaan keamanan informasi sangat rendah dimana 5 dari 6 kategori memiliki tingkat kematangan I terutama pada kategori Pelindungan Data Pribadi dan hanya kategori Teknologi dan Keamanan Informasi yang berada pada tingkat kematangan II. Hal ini sangat diperlukan peningkatan pengelolaan keamanan informasi secara signifikan dikarenakan ketergantungan Sistem Elektronik di lingkungan perguruan tinggi XYZ termasuk tinggi.

DAFTAR PUSTAKA

[1] Febriana, H., Ginting, D., & Manik, F. (2022). The applied aproach impact information security for government and company (a review). Data Science Journal of Computing and Applied Informatics, 6(1), 45-54. https://doi.org/10.32734/jocai.v6.i1-7935
[2] Ghasemi, R., Safi, A., & Dehkordi, M. (2017). Efficient multisecret sharing scheme using new proposed computational security model. International Journal of Communication Systems, 31(1). https://doi.org/10.1002/dac.3399
[3] Muhasin, H., Gheni, A., & Yousif, H. (2022). Proposed model for data protection in information systems of government institutions. Bulletin of Electrical Engineering and Informatics, 11(3), 1715-1722. https://doi.org/10.11591/eei.v11i3.3727
[4] Pamungkas, W. and Saputra, F. (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

[5] Prasetyowati, D., Gamayanto, I., Wibowo, S., & Suharnawi, S. (2019). Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (kami) berdasarkan iso/iec 27001:2013 pada politeknik ilmu pelayaran semarang. Joins (Journal of Information System), 4(1), 65-75. https://doi.org/10.33633/joins.v4i1.2429

[6] Rochmadi, T. and Pasa, I. (2021). Pengukuran risiko dan evaluasi keamanan informasi menggunakan indeks keamanan informasi di bkd xyz berdasarkan iso 27001 / sni. Cyber Security Dan Forensik Digital, 4(1), 38-43. https://doi.org/10.14421/csecurity.2021.4.1.2439

[7] Shouran, Z., Rokhman, N., & Priyambodo, T. (2019). System security awareness planning model using the octave method approach. Ijccs (Indonesian Journal of Computing and Cybernetics Systems), 13(3), 231. https://doi.org/10.22146/ijccs.43922

[8] Singh, U. and Joshi, C. (2018). Comparative study of information security risk assessment frameworks. International Journal of Computer Application, 2(8). https://doi.org/10.26808/rs.ca.i8v2.08

[9] Tristian*, R. and Wibowo, A. (2020). Implementing it risk in itsm tools using octave allegro method based at itsmproject. International Journal of Recent Technology and Engineering, 8(6), 111-117. https://doi.org/10.35940/ijrte.e6766.038620

[10] Tu, C., Yuan, Y., Archer, N., & Connelly, C. (2018). Strategic value alignment for information security management: a critical success factor analysis. Information and Computer Security, 26(2), 150-170. https://doi.org/10.1108/ics-06-2017-0042

[11] Veiga, A., Астахова, Л., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—perspectives from academia and industry. Computers & Security, 92, 101713. https://doi.org/10.1016/j.cose.2020.101713

[12] Voitsekhovska, M., Dorosh, M., Grechaninov, V., & Verenych, O. (2022). Functional modeling of the organization's information securityculture state monitoring system development. Herald of Advanced Information Technology, 5(4), 297-308. https://doi.org/10.15276/hait.05.2022.22

[13] Wijaya, Y. (2021). Evaluasi kemananan sistem informasi pasdeal berdasarkan indeks keamanan informasi (KAMI) iso/iec 27001:2013. Jurnal Sistem Informasi Dan Informatika (Simika), 4(2), 115-130. https://doi.org/10.47080/simika.v4i2.1178

[14] Yu, D., Merigó, J., & Xu, Y. (2016). Group decision making in information systems security assessment using dual hesitant fuzzy set. International Journal of Intelligent Systems, 31(8), 786-812. https://doi.org/10.1002/int.21804