

Evaluasi Tingkat Keamanan Indeks KAMI (Studi Kasus : Universitas X)

Muhammad Syaeful Bahry¹, Bambang Sugiantoro²

^{1,2}Program Studi Magister Informatika, Fakultas Sains dan Teknologi, UIN Sunan Kalijaga,
Yogyakarta

Email: ¹saifulbahary37@gmail.com, ²bambang.sugiantoro@uin-suka.ac.id

Abstrak

Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan informasi di Universitas X dengan menggunakan Indeks KAMI, alat yang dikembangkan oleh Badan Siber dan Sandi Negara untuk mengukur kesiapan dan kematangan keamanan informasi berdasarkan standar internasional ISO/IEC 27001:2013. Hasil penelitian menunjukkan bahwa Universitas X memiliki tingkat kesiapan dan kematangan yang baik dengan skor keseluruhan 638. Namun, terdapat beberapa area yang membutuhkan perbaikan lebih lanjut. Evaluasi mencakup berbagai aspek, termasuk tata kelola keamanan informasi, manajemen risiko, kerangka kerja keamanan, manajemen aset, teknologi keamanan, serta perlindungan data pribadi dan keterlibatan pihak ketiga. Berdasarkan temuan ini, diberikan rekomendasi untuk meningkatkan pengelolaan keamanan informasi di Universitas X agar lebih efektif dan efisien.

Kata kunci: Indeks KAMI; tingkat keamanan informasi

Evaluation Of KAMI Index Security Level (Case Study: University X)

Abstract

This study aims to evaluate the level of information security at Universitas X using the KAMI Index, a tool developed by the National Cyber and Crypto Agency to measure the readiness and maturity of information security based on the international standard ISO/IEC 27001:2013. The results indicate that Universitas X has a good level of readiness and maturity with an overall score of 638. However, several areas require further improvement. The evaluation covers various aspects, including information security governance, risk management, security framework, asset management, security technology, as well as data protection and third-party involvement. Based on these findings, recommendations are provided to enhance the information security management at Universitas X to be more effective and efficient.

Keywords: US Index; information security level

1. PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan komunikasi di era Industri 4.0, risiko terhadap keamanan informasi semakin meningkat. Mengingat luasnya sosialisasi nilai-nilai agama, maka pencapaian tujuan bisnis lembaga pendidikan dan pesantren memerlukan teknologi informasi yang tepat guna untuk mengelola data informasi dan menghasilkan layanan yang berkualitas tinggi. Kerentanan aset informasi memungkinkan pihak ketiga yang tidak berkepentingan untuk melakukan intervensi terhadap aktivitas terkait aset pesantren. Oleh karena itu, keamanan informasi diperlukan untuk mencegah risiko terhadap aset informasi lembaga pendidikan. Informasi adalah aset organisasi yang sangat berharga. Oleh karena itu, informasi juga menjadi salah satu sasaran serangan. Saat ini tingkat keamanan informasi menjadi aspek yang sangat penting terutama bagi organisasi dan institusi pendidikan yang menggunakan teknologi pendukung seperti jaringan dan fasilitas lain yang terkait dengan proses pengelolaan informasi.

Universitas X perlu menerapkan standar keamanan informasi resmi seperti ISO/IEC 27001:2013, yang merupakan panduan dan prosedur

IT seperti website untuk mendukung berbagai proses penyediaan informasi.

Keamanan informasi merupakan aspek penting dalam manajemen informasi yang bertujuan melindungi data dari aktivitas pihak yang tidak berwenang seperti pencurian, perubahan, atau penghapusan data tanpa izin. Sayangnya, masalah ini sering diabaikan oleh pimpinan lembaga pendidikan, manajer TI, khususnya dalam konteks web. Di era Industri 4.0, institusi menghadapi ancaman serius terhadap keamanan informasi mereka, menekankan pentingnya perhatian terhadap isu ini.

Keamanan informasi merupakan isu kritis bagi institusi pendidikan ketika menghadapi ancaman seperti pencurian data, penggunaan sistem ilegal, perusakan data, modifikasi data tanpa izin, kegagalan sistem, kesalahan manusia, bencana alam, serta serangan virus dan malware. Manajemen informasi yang efektif memungkinkan lembaga pendidikan untuk mengelola data dengan baik. Keamanan informasi juga mencakup perlindungan aset

terkait keamanan informasi. ISO 27001:2013 adalah pedoman internasional yang paling banyak digunakan untuk manajemen keamanan informasi dan dipublikasikan oleh Badan Siber dan Sandi Negara (BSSN). Peneliti akan memberikan rekomendasi

perbaikan pada area yang masih kurang untuk meningkatkan keamanan informasi. Persyaratan ini harus melengkapi seluruh dokumen Indeks KAMI, termasuk manajemen risiko keamanan informasi, pengelolaan keamanan informasi, struktur kerja keamanan informasi, manajemen aset keamanan informasi, teknologi keamanan informasi, dan pengamanan peranan pihak ketiga penyedia layanan. Penulis berinisiatif untuk melakukan “Evaluasi Keamanan Teknologi Informasi Pada Unit Pelayanan IT Menggunakan Indeks Keamanan Informasi (KAMI)” untuk memastikan kesiapan dan kematangan keamanan informasi di Universitas X.

2. KAJIAN PUSTAKA

2.1. Indeks Keamanan Informasi (KAMI)

Indeks Keamanan Informasi (KAMI) merupakan alat yang berfungsi untuk melakukan asesmen serta evaluasi terhadap tingkat kesiapan kelengkapan dan kematangan keamanan informasi di sebuah organisasi. Indeks KAMI dirancang oleh Badan Siber dan Sandi Negara berdasarkan kriteria pada SNI ISO/IEC 27001 atau dikenal sebagai standar internasional untuk sebuah sistem manajemen keamanan informasi. Sebagaimana diatur dalam Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, ketentuan dan alur pelaksanaan tersebut penting untuk dilaksanakan dalam menjaga keamanan sistem informasi.

Indeks KAMI dalam penggunaannya, bukan digunakan untuk evaluasi dalam menganalisa kelayakan atau efektivitas pengamanan informasi di suatu organisasi, melainkan untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada pimpinan instansi. Evaluasi dilakukan terhadap beragam area yang menjadi fokus implementasi keamanan informasi. Dengan cakupan pembahasan meliputi semua aspek keamanan sebagaimana yang sudah ditetapkan dalam standar ISO/EIC 27001:2022.

Area yang dimaksud dalam proses evaluasi Indeks KAMI adalah sebagai berikut:

- I: Kategori Sistem Elektronik yang digunakan instansi;
- II: Tata kelola keamanan informasi;
- III: Pengelolaan risiko keamanan informasi;
- IV: Kerangka kerja keamanan informasi;
- V: Pengelolaan aset informasi;
- VI: Teknologi dan keamanan informasi;
- VII: Suplemen, area evaluasi untuk aspek pengamanan keterlibatan pihak ketiga penyedia layanan.

Metode yang diterapkan dalam Indeks KAMI dirancang agar dapat diterapkan oleh organisasi dari berbagai ukuran, tingkat kompleksitas, dan tingkat ketergantungan pada teknologi informasi untuk mendukung berbagai proses yang diperlukan. Data dari evaluasi ini akan memberikan gambaran lengkap tentang tingkat kesiapan kelengkapan dan kematangan kerangka kerja informasi yang diterapkan. Hasil evaluasi ini dapat digunakan sebagai dasar untuk menyusun rencana perbaikan serta menetapkan prioritas tindakan yang diperlukan.

2.2. Sistem Manajemen Keamanan Informasi (SMKI)

Badan Siber dan Sandi Negara dalam menyusun Indeks KAMI, berbasis pada kebutuhan bahwa setiap platform informasi harus menerapkan standar keamanan atau disebut Sistem Manajemen Keamanan Informasi (SMKI). SMKI merupakan serangkaian kebijakan dan prosedur yang disusun secara sistematis untuk mengatur data sensitif milik sebuah organisasi. Tujuan utama dari SMKI adalah untuk mengurangi risiko serta memastikan kelangsungan bisnis dengan cara yang proaktif untuk meminimalkan dampak dari pelanggaran keamanan. SMKI juga harus mengacu pada standar nasional atau internasional yang ada guna memastikan tingkat keamanan yang tinggi dan kemampuan untuk mengatasi masalah yang muncul. Pada ISO/IEC 27001, SMKI bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi dengan menerapkan proses manajemen risiko dan memberikan keyakinan kepada pihak-pihak terkait bahwa risiko telah dikelola dengan baik. SMKI merupakan bagian integral dari proses organisasi dan struktur manajemen secara menyeluruh.

2.3. Keamanan Informasi

Keamanan informasi diartikan sebagai upaya untuk melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi, atau penghancuran oleh pihak yang tidak berwenang, guna memastikan kerahasiaan, integritas, dan ketersediaannya bagi pengguna (Nurul, dkk., 2022). Keamanan informasi merupakan isu yang kompleks yang berkaitan dengan menjagakerahasiaan, integritas, dan ketersediaan informasi yang merupakan elemen kunci dalam pengelolaan teknologi informasi. Secara ringkas, keamanan informasi dapat diartikan sebagai usaha untuk melindungi aset informasi dari suatu entitas. Ada beragam jenis informasi yang perlu dilindungi dari akses yang tidak sah atau penyalahgunaan, diantaranya yaitu (Whitman & Mattord, 2013):

- *Physical security*;
- *Personal security*;
- *Operational security*;
- *Communications security*;
- *Network security*.

Keamanan dapat dicapai dengan beberapa cara atau strategi, biasanya dilaksanakan secara bersamaan satu sama lain. Setiap strategi keamanan informasi memiliki fokus dan didasarkan pada tujuan spesifik berdasarkan kebutuhan (Tamsir, dkk., 2022).

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi disebutkan bahwa Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi.

Confidentiality (Kerahasiaan) Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

Integrity (Integritas) Aspek yang menjamin bahwa data tidak diubah tanpa ada ijin pihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.

Availability (Ketersediaan Informasi) Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (Harliana, Perdana, & Prasetyo, 2015).

Dengan demikian, aspek-aspek keamanan informasi dapat digambarkan seperti pada gambar 1 berikut ini.



Gambar 1. Aspek Keamanan Informasi (Sundari &Wella, 2021)

Selain 3 aspek di tersebut, Granfikel dalam Tamsir (2022:3) menyatakan bahwa keamanan informasi mencakup empat elemen, yaitu: perlindungan data, integritas, autentifikasi, dan ketersediaan.

3. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah pendekatan penelitian kualitatif



Gambar 2 Metode Penelitian

Penelitian Pendahuluan adalah langkah untuk peneliti melakukan studi awal dengan melihat kondisi yang ada di Universitas X dalam implementasi tingkat keamanan teknologi informasi.

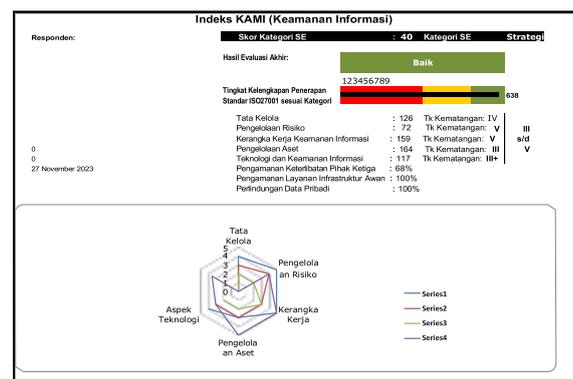
Pengumpulan Data dilakukan dengan melibatkan pengumpulan data melalui wawancara langsung dengan satu responden yang berwenang dan memiliki pemahaman mendalam dalam mengelola tingkat keamanan teknologi informasi. Wawancara ini menggunakan kuisioner tertutup dengan skala Likert yang berbasis Indeks KAMI. Jawaban yang diperoleh dari wawancara tersebut disesuaikan dengan kondisi di lapangan, dengan pilihan jawaban seperti tidak dilakukan, sedang direncanakan, sedang diterapkan sebagian, atau sudah diterapkan secara menyeluruh.

Setelah mengumpulkan data berdasarkan kuisioner Indeks KAMI, tahapan selanjutnya adalah pengolahan data. Data yang telah dikumpulkan akan diolah menggunakan perangkat lunak Indeks KAMI untuk mengevaluasi sejauh mana tingkat kematangan keamanan teknologi informasi sesuai dengan standar ISO 27001.

Analisis Data dan Penarikan Kesimpulan adalah tahapan di mana hasil dari tahapan sebelumnya dianalisis secara mendalam. Tujuannya adalah untuk mengevaluasi apa yang sudah diterapkan dan apa yang perlu diperbaiki dalam tingkat keamanan teknologi informasi di Universitas X untuk masa depan, demi meningkatkan regenerasi penerus bangsa Indonesia.

4. PEMBAHASAN

Hasil evaluasi Indeks KAMI terhadap Universitas X, diketahui gambaran kesiapan kelengkapan dan kematangan keamanan informasi sebagaimana Gambar 3.



Gambar 3 Dashboard Penilaian Indeks KAMI pada Universitas X

Dashboard diatas menggambarkan secara keseluruhan dari penilaian terhadap Universitas X yang telah dilakukan dengan menggunakan indeks KAMI versi 4.2. Dari dashboard tersebut, dapat dilihat bahwa tingkat kesiapan kelengkapan dan kematangan keamanan informasi di Universitas X sudah Baik dengan nilai sebesar 638 dan tingkat kematangan berada pada Tingkat III s/d V.

Untuk penilian skor setiap kategori yaitu:

- I: Kategori Sistem Elektronik yang digunakan instansi memiliki Skor 40;
- II: Tata kelola keamanan informasi memiliki Skor 62;
- III: Pengelolaan risiko keamanan informasi

memiliki Skor 72;

- IV: Kerangka kerja keamanan informasi memiliki Skor 89;
- V: Pengelolaan aset informasi memiliki Skor 74;
- VI: Teknologi dan keamanan informasi memiliki Skor 81;
- VII: Suplemen dengan 68%, skor suplemen bagian pengamanan layanan infrastruktur awam dengan total 95%, dan suplemen bagian perlindungan data pribadi dengan total 94%.

5. KESIMPULAN

Berdasarkan hasil dan pembahasan yang telah dilakukan, berikut beberapa kesimpulan yang dapat diambil:

Tingkat kematangan per area di Universitas X adalah sebagai berikut: Kategori SE dengan skor 40, Tata Kelola dengan skor 62, Risiko dengan skor 72, Kerangka Kerja dengan skor 89, Pengelola Aset dengan skor 74, Teknologi dengan skor 81, dan Suplemen dengan 95%. Skor suplemen untuk pengamanan layanan infrastruktur awam adalah 94%, dan untuk perlindungan data pribadi adalah 94%. Hasil tersebut menunjukkan bahwa sebagian besar proses tingkat keamanan informasi yang ada di Universitas X sudah cukup dilakukan secara rutin dan cukup sesuai standar prosedur yang ada. Berdasarkan standar Indeks KAMI maka pengelolaan tingkat keamanan informasi di Universitas X perlu ditingkatkan.

DAFTAR PUSTAKA

- Badan Siber dan Sandi Negara. 2023. Indeks Keamanan Informasi Versi 5.0. Tim Indeks Kami. <https://www.bssn.go.id/indeks-kami/>
- Nurul, S., Anggrainy, S., & Aprelyani, S. 2022. Faktor-faktor yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review SIM). *Jurnal Ekonomi Manajemen Sistem Informasi*, 3(5):564-573. E-ISSN: 2686-5238, P-ISSN 2686-4916. DOI: <https://doi.org/10.31933/jemsi.v3i5.992>
- Whitman, M. E., & Mattord, H. J. (2013). *Management of information security*, Fourth Edition. Boston: Course Technology.
- Tamsir, N., dkk. 2023. *Keamanan Sistem Informasi*. Bandung: INDIE Press
- Sundari, P. & Wella. 2021. SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR). *Ultima InfoSys : Jurnal Ilmu Sistem Informasi*, 12(1):35-42. ISSN 2085-4579.
- Abdelilah, C., S. Ahriz, K.E. Guemmat, & K. Mansouri. 2024. Implementation of Suitable Information Technology Governance Frameworks for Moroccan Higher Education Institutions. *International Journal of Electrical and Computer Engineering* 14 (3): 3116–26. <https://doi.org/10.11591/ijece.v14i3.pp3116-3126>.
- Ali, T., M. Al-Khalidi, & R. Al-Zaidi. 2024. Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. *Journal of Computer Information Systems*. <https://doi.org/10.1080/08874417.2024.2329985>
- Alip Nur Yanto, Wawan Abdullah, & Muammar Zulfiquri. 2023. Digitalisasi Pesantren Darul Mustafa Lebak Banten. *Tarbiyatuna: Jurnal Pendidikan Islam* 16 (2): 131–44. <https://doi.org/10.54471/tarbiyatuna.v16i2.2601>.
- Badi'ah, Siti, Luthfi Salim, & Muhammad Candra Syahputra. 2021. Pesantren dan Perubahan Sosial pada Era Digital. *Analisis: Jurnal Studi Keislaman* 21 (2): 349–64. <https://doi.org/10.24042/ajsk.v21i2.10244>.
- Baharuddin, A Fahmi. 2019. Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Domain DSS (Deliver, Service, Support). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* 3 (9).
- Berrada, H., J. Boutahar, And S.E.G. El Houssaïni. 2024. MART 23: A Tool to Audit Information Technology Risk Management Maturity. *International Journal of Safety and Security Engineering* 14 (2): 411–19. <https://doi.org/10.18280/ijss.140209>.
- Devanti, Khairunnisa, Wayan Gede Suka Parwita, & I Kadek Budi Sandika. 2019. Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Pada Pt. Bisma Tunas Jaya Sentral. *Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI)* 2 (2): 65–76. <https://doi.org/10.33173/jsikti.59>.
- Dewantara, Rizki, & Bambang Sugiantoro. 2021. Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta). *Jurnal Teknologi Informasi dan Ilmu Komputer* 8 (6): 1137. <https://doi.org/10.25126/jtiik.2021863123>.
- Din, R., R. Bakar, A. Ismail, A. Mustapha, & S. Utama. 2019. Evaluation Review of Effectiveness and Security Metrics Performance on Information Technology Domain. *Indonesian Journal of Electrical Engineering and Computer Science* 16 (2): 1059–64. <https://doi.org/10.11591/ijeecs.v16.i2.pp1059-1064>.
- Erwin, Loso Judijanto, Anggraeni Annisa Fitri, Nurfaidah, Febriyani Damayanti, Herva Emilda Sari, & Novi Indrayani. 2023. *SISTEM INFORMASI MANAJEMEN (Teori, Prinsip Dan Penerapan)*. PT. Sonpedia Publishing Indonesia.
- Ferdiansyah, Pramudhita, Subektiningsih Subektiningsih, & Rini Indrayani. 2019. Evaluasi Tingkat Kesiapan Keamanan Informasi Pada Lembaga Pendidikan Menggunakan

- Indeks Kami 4.0. Mobile and Forensics 1 (2): 53–62. <https://doi.org/10.12928/mf.v1i2.1001>.
- Fernando, E., & J. Gate. 2024. Enhancing IT Risk Management in XYZ Vocational School: Leveraging COBIT 5 Framework with the APO12 Domain. 274–80. <https://doi.org/10.1109/ICETISIS61505.2024.10459513>.
- Habib Saragih, A., S. Ali, E. Suwardi, & H. Utomo. 2024. Finding the Missing Pieces to an Optimal Corporate Tax Savings: Information Technology Governance and Internal Information Quality. *International Journal of Accounting Information Systems* 52. <https://doi.org/10.1016/j.accinf.2023.100665>.
- Laaziri, M., K. Benmoussa, A. El Alaoui El Amrani, & A. Mouchtachi. 2023. A New Approach to University IT Project Portfolio Management Based on Multi-Criteria Methods and the COBIT 5 Governance Framework. *Journal of Systems Science and Information* 11 (5): 636–54. <https://doi.org/10.21078/JSSI-2022-0033>.
- Mayasari. 2021. Laporan Dan Evaluasi Penelitian. *ALACRITY : Journal Of Education* 1 (2).
- Mohamed, A.M.E., N.H.A. Alnor, O.A.A. Mohammed, E.M. Al-Matari, A. Alhebri, & A. Ahmed. 2024. The Impact of Information Technology Governance According to the COBIT on Performance. *International Journal of Advanced and Applied Sciences* 11 (3): 127–36. <https://doi.org/10.21833/ijaas.2024.03.014>.
- Pardosi, Victor Benny Alexsius, Abdul Karim, Rozali Ilham, Hayadi Hamuda, Fernando V Dotulong, Afif Zuhri Arfianto, Leo Sandi, Selly Septiani, Listina Nadhia Ningsih, & Andi Wijaya. 2024. *Sistem Keamanan Komputer*. Batam: Rey Media Grafika.
- Qureshi, K.N., G. O’Keeffe, S. O’Farrell, & G. Costelloe. 2024. Cybersecurity Standards and Policies for CPS in IoE. In *Internet of Things, Part F1832:177–92*. https://doi.org/10.1007/978-3-031-45162-1_11.
- Romadhona, P.F., M.L. Ismail, & Y. Ruldeviyani. 2023. Evaluation of Information Security Management in Crisis Response Using KAMI Index: The Case of Company XYZ. In . Vol. 2508. <https://doi.org/10.1063/5.0115555>.
- Savitri, R., & M.S. Hasibuan. 2024. Information Security Measurement Using INDEX KAMI at Metro City. *Journal of Applied Data Sciences* 5 (1): 33–45. <https://doi.org/10.47738/jads.v5i1.152>.
- Suryanti, Noorhasanah Zainuddin, & Nurfitri Nurfitri. 2023. Evaluasi Keamanan Sistem Informasi Akademik (Siakad) Menggunakan Framework Cobit 5 Pada Universitas Sembilanbelas November Kolaka. *PROSIDING SEMINAR NASIONAL PEMANFAATAN SAINS DAN TEKNOLOGI INFORMASI 2023* 1 (1).
- Susanto, Edy, Lady Antira, Kevin Kevin, Edo Stanzah, & Assyeh Annasrul Majid. 2023. Manajemen Keamanan Cyber Di Era Digital. *Journal of Business And Entrepreneurship* 11 (1): 23. <https://doi.org/10.46273/job.e.v11i1.365>.
- Vaiopoulou, J., S. Papadakis, E. Sifaki, M. Kalogiannakis, & D. Stamovlasis. 2023. Correction to: Classification and Evaluation of Educational Apps for Early Childhood: Security Matters (Education and Information Technologies, (2023), 28, 3, (2547-2578), 10.1007/S10639-022-11289-w). *Education and Information Technologies* 28 (11): 15447–48. <https://doi.org/10.1007/s10639-023-11758-w>.
- Wibowo, A. 2023. Risk Assessment Related To Privacy Information On Electronic Money Server-Based Using Iso 27001 Iso 27005, Iso 27701. *Journal of Theoretical and Applied Information Technology* 101 (3): 1067–77.