NARATIF(Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika)
Vol. 02 No. 02 Desember 2020
P-ISSN: 2656-7377 || E-ISSN: 2714-8467

# MENGUKUR KESIAPAN KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN INDEK KAMI

## STUDI KASUS PADA UNIVERSITAS XYZ

Saepudin
Program Studi Teknik Informatika
Sekolah Tinggi Teknologi Bandung, Jl. Soekarno Hatta No. 378 Bandung
saepudin@sttbandung.ac.id

**Abstrak**

Sistem informasi sudah banyak diadopsi oleh berbagai organisasi pemerintahan dan juga institusi pendidikan, mulai dari sekolah menegah atas sampai pergururuan tinggi. Begitu pentingnya sistem informasi bagi perguruan tinggi mengakibatkan rentannya sistem informasi tersebut kalau tidak dilakukan peninjauan dalam masalah keamanan, keamanan menjadi masalah yang sangat penting mengingat sistem informasi dapat di akses kapan pun dan oleh siapa pun. Keamanan informasi sangat penting untuk itu harus ada bebrapa kebijakan baik teknis dan non teknis. Kebijakan tentang kamanan informasi harus baik dan harus mencakup beberapa prosedur seperti prosedur pengelolaan aset, prosedur pengelolaan sumber daya manusia, prosedur pengamanan fisik dan lingkungan, prosedur pengamanan logical security, prosedur pengamanan operasional teknologi informasi dan prosedur penanganan insiden dalam pengamanan informasi. Untuk itu perlu dilakukan pengukuran keamanan sistem informasi untuk memastikan keamanan informasi diterapkan sesuai dengan prosedur. ISO/IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha mengimplementasikan konsep-konsep keamanan informasi pada Universitas XYZ dari aspek keamanan sistem informasi berdasarkan standar ISO 27001. Perguruan tinggi perlu dilakukan pengukuran keamanan sistem informasi untuk mendapatkan gambaran kondisi kesiapan dan kematangan keamanan informasi. Indeks Keamanan Informasi disingkat KAMI adalah alat evaluasi yang dirilis oleh Kementerian Komunikasi dan Informasi yang berfungsi untuk menganalisa tingkat kesiapan pengamanan informasi di instansi pemerintah dan dapat digunakan untuk non pemerintahan.

Kata Kunci :
ISO/IEC 27001, pengukuran, evaluasi, indek KAMI, keamanan sistem informasi, SMKI.

***Abstract***

*Information systems have been widely adopted by various government organizations and educational institutions, ranging from high schools to universities. Once the importance of information systems for universities results in the vulnerability of the information system if a review is not carried out in security issues, security becomes a very important issue considering that information systems can be accessed anytime and by anyone. Information security is very important, so there must be several policies, both technical and non-technical. Information security policies must be sound and must include several procedures such as asset management procedures, human resource management procedures, physical and environmental security procedures, logical security procedures, information technology operational security procedures and incident handling procedures for information security. For this reason, it is necessary to measure the security of information systems to ensure information security is implemented in accordance with procedures. ISO / IEC 27001 is a standard document for Information Security Management Systems (ISMS) in general regarding what should be done in an effort to implement information security concepts at XYZ University from the aspect of information system security based on ISO 27001 standards. information to get a picture of the condition of readiness and maturity of information security. The Information Security Index, abbreviated as KAMI, is an evaluation tool released by the Ministry of Communication and Information which functions to analyze the readiness level of information security in government agencies and can be used for non-governmental organizations.*

*Keywords :*
*ISO / IEC 27001, measurement, evaluation, WE index, information system security, ISMS.*

## I. PENDAHULUAN

Universitas XYZ merupakan perguruan tinggi yang sudah menggunakan sistem informasi akademik yang yang dapat diakses oleh dosen dan mahasiswa dalam kegiatan belajar mengajar di universitas xyz. Keamanan informasi pada sistem akademik universitas xyz sangat penting terutama menyangkut data baik mahasiswa, dosen dan juga pegawai non pendidik. Data tersebut merupakan salah satu aset bagi institusi perguruan tinggi yang harus di jaga baik dari aspek confidenciality, integrity dan availability. Mengingat pentingnya keamanan informasi, maka kebijakan tentang keamanan informasi harus baik dan harus mencakup beberapa prosedur seperti prosedur pengelolaan aset, prosedur pengelolaan sumber daya manusia, prosedur pengamanan fisik dan lingkungan, prosedur pengamanan logical security, prosedur pengamanan operasional teknologi informasi dan prosedur penanganan insiden dalam pengamanan informasi. Untuk mengukur keamanan informasi tersebut penulis akan melakukan wawancara dengan kunci pemegang sistem informasi untuk memastikan keamanan informasi diterapkan sesuai dengan prosedur. ISO/IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi pada sebuah organisasi[1][2][3][4]. ISO/IEC 27001 dipilih karena standar ini sangat fleksibel dikembangkan karena sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai dan ukuran struktur organisasi. Perguruan tinggi perlu dilakukan evaluasi keamanan sistem informasi untuk mendapatkan gambaran kondisi kesiapan dan

kematangan keamanan informasi. Indeks Keamanan Informasi disingkat KAMI adalah alat evaluasi yang dirilis oleh Kementerian Komunikasi dan Informasi yang berfungsi untuk menganalisa tingkat kesiapan pengamanan informasi di instansi pemerintah dan dapat digunakan untuk non pemerintahan[5][6].

## II. TINJAUAN PUSTAKA

Keamanan informasi merupakan aspek penting dalam usaha melindungi aset informasi dari seoluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimasi risiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis dalam sebuah organisasi. Keamanan informasi mempunyai tiga aspek yang sangat mendasar adalah[7]:

a. Kerahasiaan
   Memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.
b. Ketersediaan
   Informasi belum mengalami perubahan karena kesalahan secara sengaja maupun tidak
c. Keutuhan
   Ketersediaan sumber informasi ketika dibutuhkan. Ketersediaan ini dapat terpengaruh oleh faktor teknis, faktor alam, dan faktor manusia

Definisi Keamanan Informasi menurut (ISO 27001 dalam Sarno dan Iffano, 2009: 27) adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (business continuity), meminimasi risiko bisnis (reduce business risk) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis. Definisi lain keamanan informasi menurut (SMKI dalam Sarno dan iffano, 2009:45) adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Maka keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi risiko-risiko yang terjadi, mengoftimalkan pengembalian investasi (return on investment). Bahwa ini berarti Kemanan informasi berkaitan upaya perlindungan atau mengamankan aset yang berharga terhadap kehilangan, pengungkapan penyalahgunaan, atau kerusakan yang mungkin terjadi upaya dalam menjamin kelangsungan bisnis (business continuity), meminimalkan risiko bisnis (reduce business risk) dan memaksimalkan pengembalian investasi dan peluang[8].

1. SMKI ( sistem manajemen keamanann informasi)

   Pengertian Sistem manajemen keamanan informasi (SMKI) atau information security management system (ISMS). (SMKI dalam sarno dan iffano, 2009:46) merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan (plan), mengimplementasikan dan mengoperasikan (Do), memonitor dan meninjau ulang (Check) serta memelihara dan meningkatkan atau mengembangkan (Act) terhadap keamnan informasi perusahaan[9].

   Keamanan Informasi ditujukan untuk menjaga aspek kerahasiaan, keutuhan, dan ketersediaan dari informasi Sistem manajemen keamanan informasi yang diterapkan perusahaa atau instansi adalah dalam upaya mengamankan aset informasi terhadap ancaman yang mungkin terjadi. Ole sebab itu, kemanan informasi secara tidak langsung menjamin kelangsungan bisnis perusahaan. Sistem manajemen keamanan informasi menjadi penting diterapkan agar informasi yang beredar di perusahaan dapat dikelola dengan benar sehingga perusahaan dapat mengambil keputusan berdasarkan informasi yang ad dengan benar pula dalam rangka memberikan layanan yang terbaik kepada pelanggan.

   Tujuan dari SMKI sendiri adalah untuk meminimalisir risiko dan menjamin kelangsungan bisnis secara proaktif untuk membatas dampak dari pelanggaran keamanan, dan keamanan informasi ditujukan yaitu untuk menjaga aspek Kerahasiaan (confidentiality), keutuhan (Integrity), dan ketersediaan (availability) dari informasi. Sistem Manajemen Keamanan Informasi juga harus mengacu pada standar nasional atau internasional yang ada agar kualitas pengamanan yang diberikan tinggi dan mampu menanggulangi adanya masalah. Standar internasional yang telah direkomendasikan untuk penerapan SMKI adalah SNI ISO/IEC 27001:2013. Standa berjalan berbasis risiko sehingga mampu mengurangi ancaman dan menanggulangi masalah dengan cepat dan tepat. Dimana Implementasi dari SMKI ini meliputi kebijakan, proses, prosedur, struktur organisasi, sert fungsi dari software dan hardware[6].

   Indonesia sendiri melalui BSN ( Badan Standar Nasioanal ) kenapa mengadopsi pada standar ISO karen indonesia merupakan satu anggota bahkan menjadi anggota Dewan sehingga memiliki peran aktif dan penting dalam organisasi internasional tersebut, sehingga dengan demikian indonesia harus menjalankan kebijakan dan standar yang diterbitkan oleh ISO.

   SMKI adalah suatu pendekatan proses maka dalam mengimplementasikannya perlu dukungan mangemen yaitu [3]:

   a. Perencanaan (Planing) : yaitu melakukan kegiatan meliputi proses pernacangan, pembuatan dan implementas untuk mencapai tujuan SMKI, tipe perancangan dalam SMKI antara lain:
      a. Strategic planning
      b. Tactical palnning
      c. Operational planning

b. Kebijakan yaitu : peran dukungan kebijakan dari manajemen akan memberikan arahan dan dukungan sumber daya untuk mencapai tujuan SMKI, tanpa ada dukungan kebijakan dari pihak managemen organisasi SMKI tidak dapat dilakukan
c. Program, dalam penyusunan SMKI didukung dengan pembangunan suatu prosedur dan proses secara detail tentang operasi-operasi dalam SMKI salah satunya adalah program pelatihan Keamanan Informasi
d. Penilaian Risiko yaitu : organisasi harus memahami seberapa besar dampak yang akan diterima oleh organisasi jika terjadi insiden keamanan Informasi. Penilaian risiko dilaksanakan berdasarkan serangkaian manajemen risiko meliputi Penilaian risiko (risk asessment).
e. Sumber Daya Manusia yaitu keamanan personil secara individu pada saat bekerjadan keamanan personil dalam organisasi
f. Tanggung Jawab yaitu tanggung jawab manajemen dalam penerapan SMKI, baik individu maupun tanggung jawab seluruh sumber daya organisasi untuk menjalankan dan memelihara SMKI.

Secara praktis memang tidak ada ketentuan bahwa menerapan terhimpuan teknik keamanan saja menjamin 100% aman. Meskipun teknik-teknik keamanan secara menyeluruh, belum cukup untuk memberikan jaminan keamanan. Penerapan SMKI tidak bisa dilakukan secara terpisah yang berarti Keamanan Informasi adalah penerapan secara menyeluruh baik teknik keamanan yang terhimpun Teknologi Keamanan Informasi serta penjagaa aspek keamanan Informasi melalui prosesproses yang terhimpun dalam SMKI. Dengan demikian bahwa penerapan SMKI sangatlah penting karena ancaman terhadap aspek Keamanan Informasi semakin meningkat. Organisasi menghadapi ancaman terhadap informasi yang dimilikinya sehingga diperlukan langkahlangkah yang tepat untuk mengamankan dalam SMKI[6].

2. ISO 27001:2013

ISO (International Organization for Standardization) adalah pengembang terbesar di dunia standar international secara sukarela. Standar international memberikan keamanan yang lebih spesifik, layanan yang baik, membantu industri lebih efisien dan efektif. ISO/IEC 27001 merupakan standar keamanan informasi yang diterbitkan pada bulan Oktober 2005 oleh ISO dan IEC ( The International Electrotechnical Commission ). implementasi ISO/IEC 27001 mencakup pada semua organisasi seperti perusahaan swasta, lembaga, pemerintahan dan lembaga nirlaba. ISO/IEC 27001 adalah sebuah metode khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasional. ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi atau Information Securit Management Syestem, biasa disebut ISMS, yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahan dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi diperusahan berdasarkan “best practise” dalam pengamanan informasi Standar ini menjelaskan syarat untuk membuat, menerapkan, memonitor, menganalisa dan memelihara serta mendokumentasikan SMKI dalam kontek risiko keamanan informasi organisasi keseluruhan. Standar ini menjelaskan pula bagaimana mendidkripsikan menetapkan, mengimplementasikan, mengoprasikan mengamati, meninjau memelihara dan mengembangkan sistem.

ISO/IEC 27001 mendefinisikan pula keperluankeperluan untuk SMKI, sehingga SMKI yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang penting agar terhindar dari risiko dan kegagalan pengamanan sistem informasi, serta memberikan jaminan pemulihan operasi bisnis akibat kerugian yang timbulkan. ISO/IEC 27001 diterapkan tidak selalu harus digunakan dari keseluruhan kontrol melainkan disesuaikan dengan kebutuhan kontrol dari organisasi masing-masing. Beberapa alasan yang patut dijadika pertimbangan kenapa dipilih standar SNI ISO/IE 27001:2013 diantaranya[10]:

a. Sudah diadopsi oleh Indonesia melalui BS (Badan Standardisasi Nasional)
b. Sudah ditetapkan oleh Kementrian Komunikasi dan Informatika mengenai standar dengan diterbitkan Permen (Peraturan Kementrian).
c. Menyediakan model lengkap terkait bagaimana melakukan : membangun, implementasi, operasional, memonitor, mengkaji ulang, memelihara dan mengembangkan SMKI.
d. SNI ISO/IEC 27001:2013 Implementasi SMKI didesain menjadi fleksibel karena tergantung dari : kebutuhan organisasi, tujuan organisasi yang dicapai, persyaratan keamanan yang diperlukan, proses bisnis yang ada, jumlah pegawai dan ukuran struktur organisasi. Dengan kata lain bahwa menggunakan SNI ISO/IEC 27001:2013 dalam implementasinya bisa sangat tergantung kebutuhan organisasi.
e. SNI ISO/IEC 27001:2013 menyedikan sertifikat implementasi SMKI yang diakui secara internasional yang disebut ISMS Sertification.

Dalam membangun SMKI menggunaka standar SNI ISO/IEC 27001:2013 perlu diperhatikan dan dipahami bahwa struktur organisasi SNI ISO/IEC 27001:2013 memiliki dua bagian yaitu;

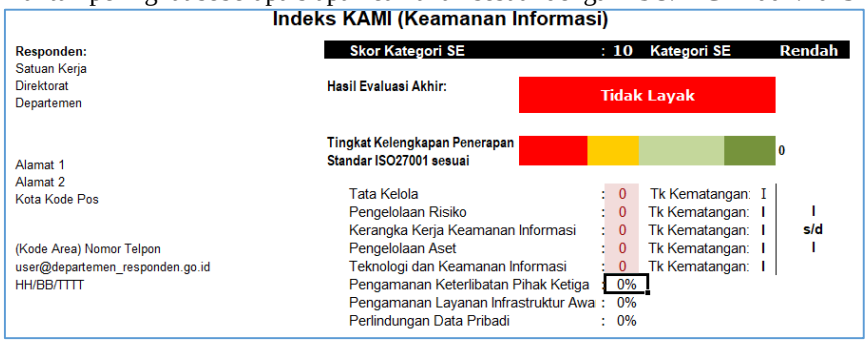
a. Kalusul : Mandatori Proses, kalusul (pasal) adalah persaratan yang harus dipenuhi oleh organisasi
b. Annex A: Sequrity Control, yaitu dokumen referensi yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol keamanan yang perlu diimplementasikan didalam SMKI yang terdiri dari 14 Kalusul kontrol Keamanan, 13 objektif Kontrol dan 114 Kontrol.

3. Indek KAMI

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi perguruan tinggi. Evaluasi pada indek KAMI dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2013. Hasil evaluasi indeks KAMI menggambarkan tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2013 dan peta area tata kelola keamanan sistem informasi di instansi perguruan tinggi. Penilaian dalam Indeks KAMI dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2013, yang disusun kembali menjadi 5 (lima) area di bawah ini[8][10][9][4][7][2][4][10]:

a. Tata Kelola Keamanan Informasi – Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
b. Pengelolaan Risiko Keamanan Informasi – Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
c. Kerangka Kerja Keamanan Informasi – Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
d. Pengelolaan Aset Informasi – Bagian ini mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut
e. Teknologi dan Keamanan Informasi – Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Ada dua metode dalam indek KAMI yaitu peniliaina lima area yang telah di sebutkan di tas dan penilaian kematangan untuk peringkat seberapa siapa keamanan sesuai dengan ISO/IEC 27001:2013




Gambar 1 Tampilan keluaran Indek KAMI

## III. METODE

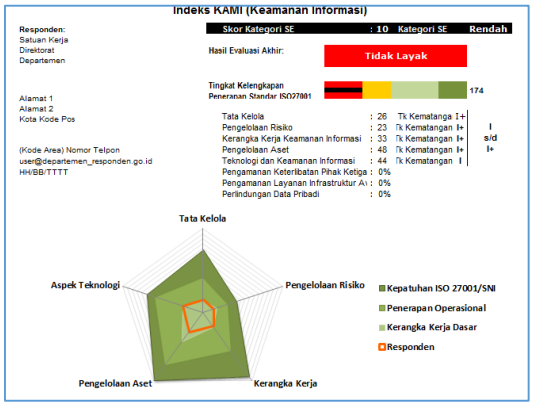
Metode penelitian ini menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO/IEC 27001:2013 sebagai kerangka penelitian untuk mengolah hasil analisa dari wawancara tentang keamanan informasi. Indeks KAMI merupakan alat yang digunakan untuk menilai tingkat kematangan, tingkat kelengkapan penerapan serta gambaran tata kelola keamanan informasi pada suatu instansi perguruan tinggi maupun perusahaan. Langkah penelitian sebagai berikut:

a. Mendefinisikan ruang lingkup
b. Menetapkan peran atau tingkat kepentingan
c. Menilai lima area dalam indek KAMI
d. Hasil akan di gambarkan dalam bentuk jaring laba-laba

## IV. PEMBAHASAN

Hasil evaluasi keamanan sistem informasi pada Universitas XYZ menggunakan indek KAMI sesuai ISO 27001:2013 dengan melakukan wawancara dan observasi kepada staf ICT-SIM Universitas XYZ adalah sebagai berikut :

TABEL I
HASIL KESIAPAN DARI INDEK KAMI




| **Bagian I: Kategori Sistem Elektronik** | | |
|---|---|---|
| Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan | | |
| **[Kategori Sistem Elektronik]** Rendah; Tinggi; Strategis | | **Status** |
| # | **Karakteristik Instansi/Perusahaan** | |
| 1.1 | Nilai investasi sistem elektronik yang terpasang<br>[A] Lebih dari Rp.30 Miliar<br>[B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar<br>[C] Kurang dari Rp.3 Miliar | C |
| 1.2 | Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik<br>[A] Lebih dari Rp.10 Miliar<br>[B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar<br>[C] Kurang dari Rp.1 Miliar | B |
| 1.3 | Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu<br>[A] Peraturan atau Standar nasional dan internasional<br>[B] Peraturan atau Standar nasional<br>[C] Tidak ada Peraturan khusus | B |
| 1.4 | Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik<br>[A] Teknik kriptografi khusus yang disertifikasi oleh Negara<br>[B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri<br>[C] Tidak ada penggunaan teknik kriptografi | B |
| 1.5 | Jumlah pengguna Sistem Elektronik<br>[A] Lebih dari 5.000 pengguna<br>[B] 1.000 sampai dengan 5.000 pengguna<br>[C] Kurang dari 1.000 pengguna | B |
| 1.6 | Data pribadi yang dikelola Sistem Elektronik<br>[A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya<br>[B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha<br>[C] Tidak ada data pribadi | B |
| 1.7 | Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi<br>[A] Sangat Rahasia<br>[B] Rahasia dan/ atau Terbatas<br>[C] Biasa | B |
| 1.8 | Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi<br>[A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik<br>[B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung<br>[C] Proses yang hanya berdampak pada bisnis perusahaan | B |
| 1.9 | Dampak dari kegagalan Sistem Elektronik<br>[A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara<br>[B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih<br>[C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih | C |

| | | |
|---|---|---|
| 1.10 | Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme)<br>[A] Menimbulkan korban jiwa<br>[B] Terbatas pada kerugian finansial<br>[C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial) | C |
| | **Skor penetapan Kategori Sistem Elektronik** | **17** |

Tingkat ketergantungan terhadap sistem elektronik sangat tinggi yaitu bernilai 17, Hasil pengukuran Bagian II, III, IV, V dan VI menunjukan bahwa tingkat kematangan keamanan informasi di universitas xyz berada pada Level I+ dan II yaitu Penerapan Kerangka Kerja Dasar, sementara untuk bagian V tingkat kematangan keamanan informasi masih berupa Kondisi Awal.

## V. KESIMPULAN

Kesimpulan berdasarkan hasil pengukuran keamanan sistem informasi dengan indek KAMI masih kurangnya kesiapan untuk melakukan sertifikat ISO/IEC 27001:2013, untuk kedepan penelitian selanjutnya bisa melakukan pengukuran dengan menggunkana framework yang lain seperti Cobit 2019 terbaru dengan menggunakan area domain khusus keamanan.

## REFERENSI

[1] T. Informatika, U. Sam, R. Manado, J. Kampus, and U. Bahu, "Implementasi Indeks Kami Di Universitas Sam Ratulangi," *J. Tek. Inform.*, vol. 12, no. 1, 2017, doi: 10.35793/jti.12.1.2017.17869.

[2] E. L. Putra, B. C. Hidayanto, and H. M. Astuti, "Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI)," *J. Tek. Pomits*, vol. 3, no. 2, pp. 228–233, 2014, [Online]. Available: http://ejurnal.its.ac.id/index.php/teknik/article/view/8289.

[3] B. A. Firzah, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi ( Kami ) Berdasarkan Iso / Iec 27001 : 2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi ( Dptsi ) Its Surabaya Evaluating Information Security Management Using Ind," vol. 6, no. 1, 2017.

[4] D. D. Prasetyowati, I. Gamayanto, S. Wibowo, and S. Suharnawi, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang," *JOINS (Journal Inf. Syst.*, vol. 4, no. 1, pp. 65–75, 2019, doi: 10.33633/joins.v4i1.2429.

[5] B. Sutara, "Pengukuran Keamanan Informasi PDAM Titra Medal Menggunakan Indeks KAMI Untuk Analisis Tingkat Kematangan Keamanan Informasi," vol. 17, no. 2, pp. 34–41, 2018, [Online]. Available: https://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/32.

[6] E. R. Pratama, Suprapto, and A. R. Perdanakusuma, "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001: Studi Kasus KOMINFO Provinsi Jawa Timur," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 5911–5920, 2018, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465.

[7] M. P. Mokodompit and N. Nurlaela, "Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000 (Studi Kasus Pada Peguruan Tinggi X)," *J. Sist. Inf. Bisnis*, vol. 6, no. 2, p. 97, 2017, doi: 10.21456/vol6iss2pp97-104.

[8] M. R. Ridho, K. Ghozali, and B. C. Hidayanto, "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus: Bidang Aplikasi dan Telematika Dinas Komunikasi Dan Informatika Surabaya," *J. Tek. POMITS (Publikasi Online ITS)*, vol. 1, no. 1, pp. 1–6, 2012.

[9] F. T. Informasi, "Indeks Keamanan Informasi ( Kami ) Berdasarkan Iso / Iec 27001 : 2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi ( Dptsi ) Its Surabaya Evaluating Information Security Management Using Indeks Keamanan Informasi ( Kami ) Based on Iso / Iec," 2013.

[10] W. C. Pamungkas and F. T. Saputra, "Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013," *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 101, 2020, doi: 10.30865/json.v1i2.1924.

.