JURNAL ILMIAH SAINS TEKNOLOGI DAN INFORMASI
Vol.1, No.3 Juli 2023
e-ISSN: 2964-3104; p-ISSN: 2964-3090, Hal 01-13
DOI: https://doi.org/10.59024/jiti.v1i3.192

AUDIT SISTEM INFORMASI BERBASIS COBIT 2019 MENGGUNAKAN STANDAR ISO 27001 : 2005

Muhamad Sidik
Universias Sains Teknologi dan Komputer Semarang
mgcn.sidik@gmail.com

Abstrak Penting bagi semua perguruan tinggi untuk mempelajari dan mengevaluasi manajemen teknologi informasi agar dapat mencapai efektivitas dan efisiensi dalam manajemen bisnis. Keamanan teknologi informasi dianggap sebagai langkah pengendalian guna mengurangi risiko dan ancaman terhadap keamanan, terutama karena pembelajaran umum dan kuliah, teknologi informasi digunakan dalam proses manajemen. inspeksi untuk menentukan keamanan teknis kemudian diperlukan untuk memastikan bahwa semuanya berfungsi dengan baik. standar yang digunakan adalah organization for standardization (iso) 27001: 2005. dipilih karena kerangka dapat dimodifikasi dengan alat penelitian yang digunakan dalam organisasi. setelah itu akan dikembangkan lebih lanjut dan disesuaikan dengan sistem manajemen keamanan informasi (smki) terfokus akibatnya, semua memiliki hasil jpa = pa1: pa10, na=jpa/10 memberikan rata-rata 65%. but, itu memiliki tingkat positif, tetapi masih memenuhi persyaratan pendidikan tinggi, yang memerlukan evaluasi terus menerus dan peningkatan kontrol keamanan yang direkomendasikan. kata
Kunci: Manajemen, Teknologi Keamanan Informasi, Iso 27001 : 2005

LATAR BELAKANG

Kemungkinan tumbuhnya masalah keamanan berkorelasi negatif dengan pesatnya pertumbuhan teknologi informasi. Teknologi informasi digunakan dalam manajemen data untuk menyediakan layanan berkualitas tinggi untuk tujuan dan prosedur bisnis dalam upaya memenuhi tujuan bisnis universitas. Untuk memanfaatkan teknologi secara maksimal untuk pembelajaran, universitas harus memastikan keamanan dan kerahasiaan semua data yang diproses. Mereka juga harus memastikan integrasi, dan kinerja sistem informasi merupakan faktor penting yang harus dikendalikan secara efektif. [1]

Kontribusi terkomputerisasi digunakan di universitas untuk pemrosesan teknologi informasi yang relatif kompleks. Manajemen keamanan TI telah diterapkan dengan hasil yang relatif sangat baik. Namun, masih ada konflik data tertentu yang tidak dapat diselesaikan di seluruh sistem, misalnya: B. Pengguna memiliki akses mudah ke data atau informasi di luar izin mereka dan kurangnya personel untuk mengawasi keamanan TI. Audit diperlukan agar manajemen keamanan teknologi gosip berfungsi dengan sukses. [2].
Karena tidak ada kerangka kerja yang diperlukan untuk proses kontrol manajemen keamanan TI, audit menggunakan standar atau kerangka kerja yang sesuai dengan persyaratan.[3] Karena ISO 27001:2005 adalah standar yang relatif fleksibel yang dapat

Received Mei 3, 2023; Revised Mei 22, 2023; Juli 22, 2023
*Corresponding author, e-mail address

disesuaikan sesuai dengan permintaan, persyaratan keamanan, tujuan, dan operasi bisnis institusi, dipilih untuk pengujian keamanan TI. [4]

Masalahnya adalah bagaimana menawarkan alat uji yang sesuai untuk arsitektur jaringan yang digunakan, serta bagaimana merancang manajemen keamanan infrastruktur di dalam perusahaan secara lebih efektif dan efisien. Penelitian ini bertujuan untuk mengembangkan suatu audit manajemen keamanan teknologi informasi yang didasarkan pada infrastruktur universitas, melakukan evaluasi terhadap keamanan infrastruktur TI dengan menggunakan standar ISO 27001:2005, dan menyajikan suatu instrumen audit manajemen keamanan TI yang relevan dengan tujuan dan proses bisnis yang terkait dengan topologi infrastruktur tersebut.

KAJIAN TEORITIS

Audit didefinisikan sebagai pemeriksaan yang ketat dan metodis atas kesimpulan atau dokumentasi pendukung oleh spesialis internal dan/atau eksternal yang tidak memihak di bidang pelaporan dan dokumentasi pendukung dengan tujuan untuk menentukan keandalan laporan dan dokumentasi pendukung serta mengembangkan rekomendasi yang lebih kuat. Seluruh infrastruktur TI dipantau dan dikendalikan oleh audit TI [5].

Penilaian teknologi, seperti perangkat lunak dan perangkat keras, serta infrastruktur yang digunakan oleh universitas untuk memastikan apakah mereka berhasil mencapai tujuan bisnis adalah nama lain dari audit teknologi informasi.[6] Standar keamanan informasi ISO 27001: 2005 mencakup pedoman mendasar untuk SMKI. Sebagai metodologi untuk membuat, menerapkan, mengoperasikan, memantau, memverifikasi, memelihara, dan terus meningkatkan SMKI berdasarkan pengukuran tingkat pencapaian target, standar ini dibuat dengan menggunakan pendekatan proses.. [7]

Dalam mencapai tujuan bisnis, penting untuk memilih klausul dengan bijak. [6] Standar ISO 27001:2005, yang merupakan standar keamanan informasi, mencakup konsep dasar Sistem Manajemen Keamanan Informasi (SMKI). Standar ini didesain dengan pendekatan proses sebagai model untuk mengatur, melaksanakan, mengoperasikan, memantau, memverifikasi, memelihara, dan meningkatkan secara berkelanjutan SMKI. Hal ini dilakukan dengan menggunakan pengukuran yang didasarkan pada analisis dan perencanaan hasil pengamatan terhadap tingkat pencapaian tujuan. [7]. Memilih klausul dengan bijak dapat membantu Anda mencapai tujuan bisnis. [6] Standar keamanan informasi ISO 27001: 2005 mencakup pedoman dasar untuk SMKI. Standar ini dibuat dengan menggunakan metodologi berbasis proses sebagai model untuk pengoperasian fasilitas, pemantauan, verifikasi, pemeliharaan, dan peningkatan berkelanjutan SMKI berdasarkan alat ukur berdasarkan evaluasi dan penyusunan hasil observasi kontrol akses dan penerapan manajemen keamanan informasi di sesuai dengan standar ISO untuk meningkatkan efisiensi dan pengelolaan dokumen, yang kemudian digunakan sebagai panduan untuk mengatasi keamanan informasi. ISSN:2301-9271.[10]

B. Pemrosesan data atau opsi online yang terikat secara hukum dengan TI dan disebut KORA hanyalah beberapa contoh bagaimana Simic et al. menunjukkan bagaimana evaluasi keamanan TI konvensional dimasukkan ke dalam perangkat lunak. Penilaian keamanan TI yang komprehensif dan konsisten dengan persyaratan hukum: integrasi standar KORA, IT-Grundschutz, dan ISO 27001. IGI Global, 2013, Jurnal Internasional Keamanan dan Privasi Informasi. [11] Selain menggunakan 10 klausul ISO

27001: 2005 sebagai alat, pendekatan audit yang digunakan berbeda dari penelitian sebelumnya karena temuan audit disediakan sebagai diagram radar untuk kenyamanan universitas. Persentase Pemeriksaan (PA) yang dalam penelitian ini berjumlah 10 keterangan pemeriksaan, merupakan hasil persentase keterangan pemeriksaan. Total Control Percentage (JPA) yang meliputi pertanyaan, ruang lingkup, dan 88 instrumen, memiliki 10 klausul. Skor Akhir (NA) adalah hasil pembagian persentase total JPA dengan jumlah klausa pada tes akhir. NA = JPA/10.

METODE PENELITIAN

Penelitian ini adalah penelitian kualitatif yang bertujuan untuk mendeskripsikan tingkat pengukuran atau evaluasi Sistem Manajemen Keamanan Informasi (SMKI) di Perguruan Tinggi XYZ di Kota Semarang. Melalui pendekatan kualitatif, penelitian ini akan menganalisis dan mendeskripsikan bagaimana SMKI di perguruan tinggi tersebut diukur atau dievaluasi. Tujuan dari analisis ini adalah untuk memberikan gambaran tentang sejauh mana perguruan tinggi tersebut telah mengimplementasikan SMKI dan seberapa efektif pengukuran atau evaluasi tersebut dalam memastikan keamanan informasi yang adekuat.[12].

Adapun tahapan dalam penelitian ini dapat dilihat pada Gambar 1.

Gambar 1. Metode Penelitian[13]

1. Penelitian ini menggunakan metode yang terdiri dari empat tahap, yaitu perencanaan audit, persiapan audit, pelaksanaan audit, dan pelaporan audit.

1. Untuk memastikan bahwa definisi proses bisnis sejalan dengan persyaratan dan tujuan manajemen keamanan informasi di perguruan tinggi, perencanaan pemeriksaan dilakukan melalui definisi proses dan tujuan bisnis, yang ditentukan dengan bantuan literatur review, observasi, dan studi literatur.
2. Pembuatan tes untuk dijadikan instrumen tes 10 klausul SMKI dengan 88 soal ujian, dimana setiap soal disesuaikan dengan tahapan perencanaan audit tujuan perusahaan dan

proses bisnis yang dirumuskan secara objektif. Menurut alat evaluasi yang dipilih sesuai dengan rekomendasi implementasi saat ini dalam standar ISO 27001: 2005, yang disesuaikan dengan keadaan perguruan tinggi, setiap pernyataan dievaluasi..

2. Setelah review, dosen, Ka, ES, Ka, jejaring, penjaminan mutu, dan sesuai kesepakatan, observasi di lokasi studi, dipekerjakan untuk tahap pengumpulan dan verifikasi data.

3. Pelaporan inspeksi adalah fase terakhir dari proses, di mana laporan ditulis dan disusun menggunakan pengetahuan yang diperoleh dari data industri dan menyertakan ide atau rekomendasi untuk meningkatkan institusi..

Tabel 1. Penilaian Hasil Audit.

Prosentasi	Keterangan	Implementasi
0 – 35 %.	Sangat Rendah	Diimplementasikan untuk mencapai tujuan bisnis
36 – 50 %.	Rendah	Proses diimplementasikan, dikelola serta hasilnya ditetapkan dan dikontrol
51 – 85 %	Baik	Proses didokumentasi dan dikomunikasikan
86 – 100 %	Sangat Baik	Proses diprediksikan, ditingkatkan dan dikembangkan untuk tujuan yang akan datang.

Peringkat rata-rata semua instrumen menurut rumus JPA = PA1:

PA10 T/A=JPA/10 T/A:
Hasil akhir PA:
Tingkat pemeriksaan, JPA:
Jumlah persentase pemeriksaan. Hasil uji total negatif bila nilainya 0 sampai 50%, hasil uji total positif bila nilai rata-ratanya 51 sampai 100%.

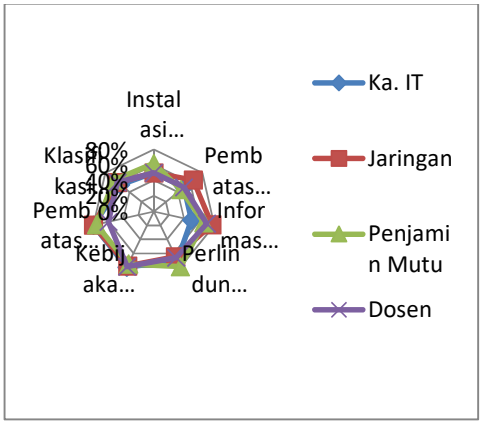
.

HASIL DAN PEMBAHASAN

Ketika melakukan perencanaan audit, penting untuk memahami proses bisnis yang akan diaudit serta teknologi informasi yang terkait. Salah satu wawasan yang ingin dicapai adalah dengan memeriksa laporan dan dokumen yang ada, serta mencari informasi apakah perguruan tinggi tersebut telah memiliki proses audit internal di masa lalu. Dalam konteks topologi jaringan dan infrastruktur di perguruan tinggi, terdapat tiga server utama yang meliputi Foundation Server, server dosen, dan server mahasiswa. Jaringan pada ruang server utama ini kemudian dibagi menjadi beberapa switch eksternal. Untuk distribusi jaringan, terdapat switch di setiap ruangan dan laboratorium yang dihubungkan oleh switch eksternal.
Kontribusi penelitian adalah:

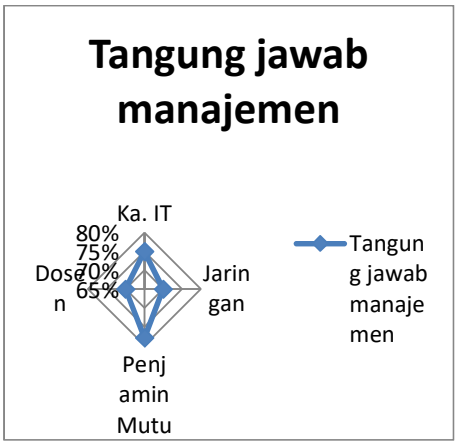
1. Membuat instrumen spesifik baru untuk arsitektur atau topologi jaringan pada skala tertentu, audit manajemen keamanan TI dengan 10 pernyataan audit dengan 88 pertanyaan audit.
2. Membuat indikator baru untuk mengukur data jaringan, persyaratan keamanan IT dari sistem yang akan dibangun dan formula instrumen khusus.

Hasil Audit Dengan Menggunakan Diagram Radar



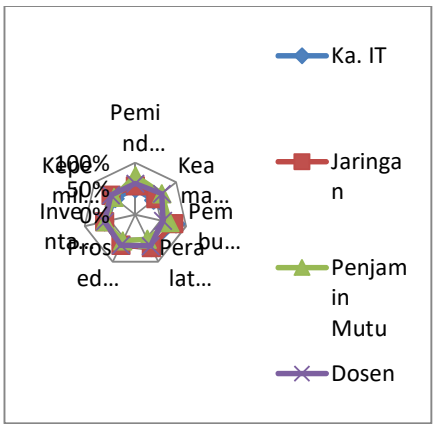
Gambar 2. Representasi Sistem Manajemen Keamanan Teknologi Informasi.

Berikut adalah gambaran persentase penginstalan perangkat lunak di sistem operasi (53%), pembatasan penginstalan perangkat lunak (53%), analisis dan definisi persyaratan keamanan informasi (66%), perlindungan untuk aplikasi layanan acara (70%), praktik pengembangan yang dilindungi (78%), pembatasan modifikasi paket perangkat lunak (74%), dan klasifikasi data (60%) yang relevan. Hasil tersebut didapatkan melalui penggunaan Kuesioner Uji Lapangan Kinerja Baik yang mengindikasikan bahwa manajer laboratorium teknis dan akademis memiliki rata-rata pencapaian sebesar 53% dalam hal menginstal perangkat lunak dan membatasi aplikasi.



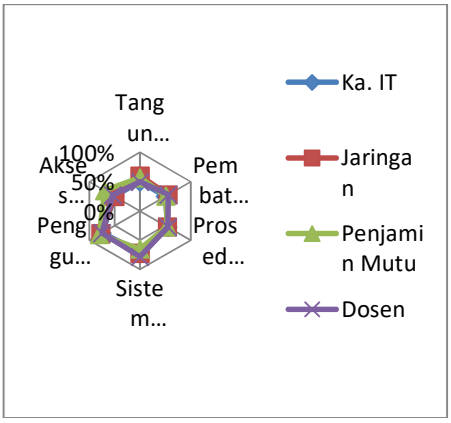
Gambar 3.Representasi Tanggung Jawab Manajemen.

Berdasarkan temuan rata-rata responden yang mengatakan bahwa tanggung jawab manajemen secara keseluruhan sangat baik (73%), tanggung jawab manajemen dapat dipelajari dalam diagram pada Gambar 3..



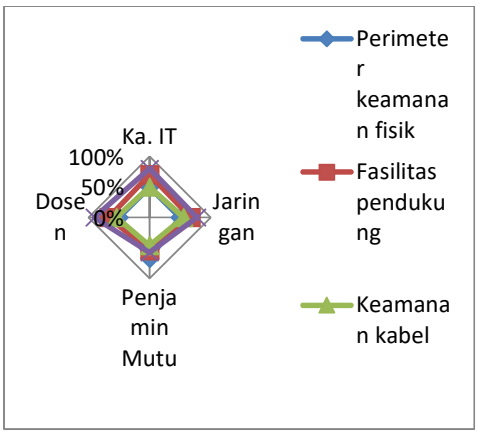
Gambar 4.Representasi Manajemen Aset.

Gambar 4 menunjukkan bahwa pembuangan atau penggunaan kembali peralatan atau perangkat yang aman adalah 69%, kas keluar dan pembuangan aset yang aman adalah 60%, dan penggunaan peralatan tanpa pengawasan adalah 65%. basis aset (61%), prosedur operasional yang ditetapkan (63%) dan kepemilikan aset (56%). Perguruan tinggi harus melakukan proses pengelolaan secara aktif agar dapat melaksanakan tugasnya dalam pemeliharaan dan optimalisasi pemanfaatan..



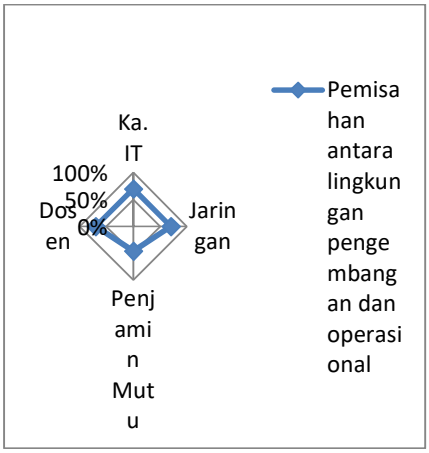
Gambar 5.Representasi *Human Resource Security.*

Hal ini ditunjukkan oleh grafik pada Gambar 5. Program kode sumber kontrol akses (56%), pembatasan akses informasi (53%), tindakan keamanan login (55%), sistem manajemen kata sandi (71%), dan penggunaan utilitas sistem (77%), semuanya dikaitkan dengan karyawan. Persentase rata-rata kendala hak akses yang lemah dan kewajiban penyelesaian adalah 53%, menunjukkan keterlambatan dalam penyelesaian tugas..



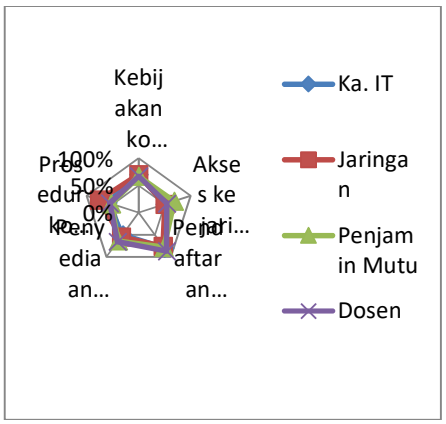
Gambar 6. Diagram keamanan fisik dan lingkungan.

Diagram Gambar 6 menunjukkan cakupan proteksi fisik sebesar 54%, infrastruktur pendukung sebesar 65%, proteksi kabel sebesar 54%, dan pemeliharaan peralatan sebesar 74%. Jelas bahwa tidak setiap ruang memiliki perlindungan fisik yang terkoordinasi..



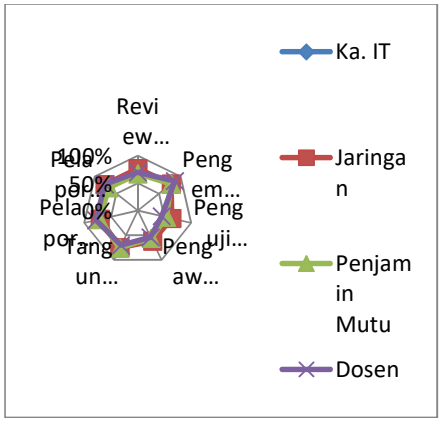
Gambar 7. Ilustrasi manajemen operasional dan komunikasi.

Pemisahan pengaturan operasional dan pengembangan pada diagram Gambar 7 menunjukkan nilai yang rendah, dengan rata-rata 64% responden, menunjukkan bahwa hal itu harus ditangani di perguruan tinggi..



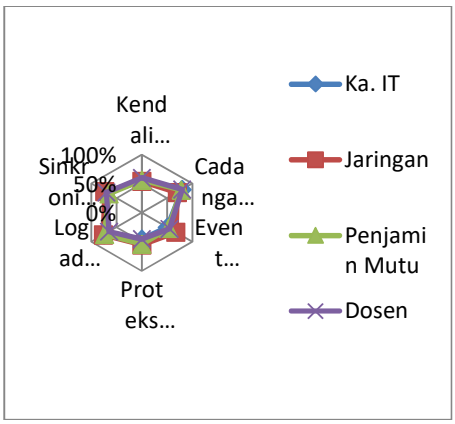
Gambar 8. Representasi Akses Kontrol.

Kebijakan kontrol akses mencapai 69% dari grafik pada Gambar 8, diikuti oleh akses jaringan dan layanan online (59%), pendaftaran pengguna (80%), pemberian hak akses kepada pengguna (59%), dan kontrol perubahan sistem saat ini pengukuran (61%). Jelas bahwa rata-rata 59% pengguna memiliki akses ke hak pengguna dan layanan online.



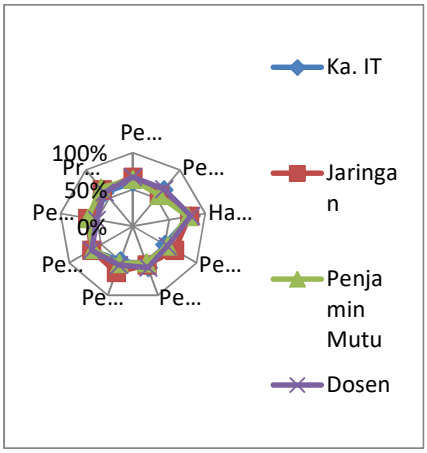
Gambar 9. Presentasi, pengembangan dan pemeliharaan sistem informasi.

Menurut diagram Gambar 9, statistik berikut menonjol: 71% tinjauan teknis aplikasi setelah beralih sistem operasi, 81% pengembangan perangkat lunak outsourcing, 58% tinjauan sistem keamanan, 73% pelaporan kasus pelanggaran data, 74% dari pelaporan kelemahan privasi, dan 69% penilaian dan keputusan pelanggaran privasi.



Gambar 10. Representasi proses manajemen sistem keamanan.

Gambar 10 menunjukkan statistik berikut: 56% untuk manajemen malware, 77% untuk cadangan data, 56% untuk log peristiwa, 50% untuk perlindungan data log, 73% untuk manajemen dan log operator, dan 70% untuk perlindungan waktu sistem untuk sinkronisasi referensi kepemimpinan..



Gambar 11. Representasi Manajeman Kelanjutan Proses.

Berdasarkan data yang diberikan, terdapat persentase kontrol jaringan sebesar 65%, segregasi jaringan sebesar 59%, prosedur dan kebijakan distribusi informasi sebesar 63%, pembelajaran tentang pelanggaran keamanan informasi sebesar 65%, perencanaan keamanan informasi berkelanjutan sebesar 60%, hak kekayaan intelektual (HKI) sebesar 79%, perlindungan data dan informasi pribadi rahasia sebesar 56%, inspeksi kepatuhan teknis sebesar 57%, dan pemantauan sistem informasi sebesar 57%. Data tersebut menunjukkan tingkat pencapaian dalam bidang-bidang tersebut.

Hasil modifikasi menggunakan alat yang disesuaikan dengan lokasi studi ditunjukkan di bawah ini, beserta temuan penilaian terhadap keseluruhan prosedur..

Tabel 2. Penilaian Klausul Audit.

No	Klausul Audit	Prosentasi Audit
1	Sistem manajemen keamanan teknologi informasi	65%
2	Tanggung jawab manajemen	73%
3	Manajemen aset	61%
4	*Human resource security*	61%
5	Keamanan fisik dan lingkungan	62%
6	Manajemen operasi dan komunikasi	64%
7	Akses kontrol	66%
8	Sistem informasi, pengembangan dan pemeliharaan	70%
9	Manajemen pengolahan sistem keamanan	64%
10	Manajeman kelanjutan proses	62%

Mendampingi penilaian manajemen keamanan TI, kriteria berikut dicatat sesuai dengan standar ISO 27001:

1. Di perguruan tinggi, ada pedoman keamanan teknologi informasi.
2. Anda telah menetapkan kebijakan kontrol akses pengguna dengan kriteria keamanan informasi tertentu.
3. Sistem harus memenuhi kriteria keamanan teknologi informasi sebelum dapat dibangun

KESIMPULAN DAN SARAN

Penilaian kemampuan manajemen keamanan TI telah meningkatkan efektivitas, efisiensi, dan relevansi perencanaan infrastruktur dengan tujuan dan prosedur perusahaan saat ini. Perguruan Tinggi XYZ di Kota Semarang telah menggunakan alat audit manajemen keamanan TI yang sesuai dengan kerangka kerja ISO 27001:2005, serta arsitektur jaringan yang digunakan di lembaga tersebut.

Hal ini membantu mereka dalam mengidentifikasi dan mengelola risiko keamanan informasi, serta memastikan bahwa infrastruktur TI mereka mendukung tujuan bisnis dan memenuhi standar keamanan yang relevan. Dengan adanya penilaian manajemen kemampuan keamanan TI, Perguruan Tinggi XYZ dapat meningkatkan keamanan informasi mereka dan mengoptimalkan penggunaan teknologi informasi secara keseluruhan.

10 frase yang digunakan dalam penelitian ini menghasilkan kesimpulan umum JPA = PA1: PA10 N/A=JPA/10 N/A: PA. Hasil akhir: Tingkat inspeksi, JPA: rata-rata 65% dari keseluruhan inspeksi diselesaikan. Perlu dilakukan perbaikan atas temuan-temuan yang penting dan bernilai tinggi, dan perbaikan tersebut harus diwujudkan dengan penilaian yang berkelanjutan.

Saran lain adalah agar universitas menggunakan alat audit Keamanan TI ISO 27001:2005 yang tersedia untuk melakukan audit manajemen keamanan TI setiap 12 bulan untuk menjaga keamanan infrastruktur tetap terkendali, menerapkan standar kinerja kerja, dan menginventarisasi semua aset. Diharapkan lebih banyak studi akan dibuat untuk perbandingan sehubungan dengan penilaian akhir model %..

DAFTAR REFERENSI

[1] Y. C. N. Bless, G. Made, A. Sasmita, and A. A. K. A. Cahyawan, "Audit Keamanan SIMAK Berdasarkan ISO 27002 (Studi Kasus : FE UNUD)," *Merpati*, vol. 2, no. 2, pp. 157–166, 2014.

[2] J. Vol and J. Vol, "ISSN 2338-137X Audit Keamanan Sistem Akuntansi Enterprise PT . Gresik Cipta Sejahtera Berdasarkan Standar ISO 27002 : 2005," vol. 5, no. 8, pp. 1–7, 2016.

[3] M. Utomo, A. Holil, N. Ali, and I. Affandi, "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I," *Inst. Teknol. Sepuluh Nop.*, vol. 1, no. 1, pp. 2–7, 2012.

[4] D. Simić-Draws, S. Neumann, A. Kahlert, P. Richter, R. Grimm, M. Volkamer, and A. Roßnagel, "Holistic and Law Compatible IT Security Evaluation," *Int. J. Inf. Secur. Priv.*, vol. 7, no. 3, pp. 16–35, 2013.

[5] Mehdi Kazemi, "Evaluation of information security management system success factors: Case study of Municipal organization," *African J. Bus. Manag.*, vol. 6, no. 14, 2012.

[6] A. Goeritno and A. H. Hendrawan, "Implementasi Iso / Iec 27001 : 2013 Untuk Sistem Manajemen Keamanan Informasi (Smki) Pada Fakultas Teknik Uika-Bogor," *Semin. Nas. Sains dan Teknol. Fak. Tek. Univ. Muhammadiyah Jakarta*, vol. 8, no. November, pp. 1–5, 2016.

[7] S. Zakwan, S. Ratnawati, and N. A. Hidayah, "Audit Tata Kelola Sumber Daya Teknologi Informasi Dengan Kerangka Kerja Cobit 4.1 Untuk Evaluasi Manajemen Pada Badan Pengawasan Keuangan Dan Pembangunan," *Stud. Inform. J. Sist. Inf.*, vol. 7, no. 2014, pp. 1–16, 2014.

[8] Juliandarini and S. Handayaningsih, "Audit Sistem Informasi Pada Digilib Universitas XYZ Menggunakan Kerangka Kerja Cobit 4.0," *J. Sarj. Tek. Inform.*, vol. 1, no. 1, pp. 276–286, 2013.

[9] A. C. Dewi, E. Nugroho, and R. Hartanto, "PENYUSUNAN TATA KELOLA KEAMANAN INFORMASI PADA PRODUKSI FILM ANIMASI (Kasus di PT. XX)," *Pros. SNATIF*, pp. 297–302, 2017. S. Ariyani and M. Sudarma, "Implementation Of The ISO / IEC 27005 In Risk Security Analysis Of Management Information System," vol. 6, no. 8, pp. 1–6, 2016.

10] T. Kristanto, R. Arief, and N. F. Rozi, "Perancangan Audit Keamanan Informasi Berdasarkan Standar Iso 27001 : 2005 (Studi Kasus : Pt Adira ...," *Semin. Nas. Sist. Inf. Indones. 22 Sept. 2014*, vol. 2005, no. October 2015, pp. 1–6, 2014.

[11] Sugiyono. P.D, *Metode penelitian pendidikan pendekatan kuantitatif.pdf*. 2014.

[12] H. A. D. Afandi, "Audit Kemanan Informasi Menggunakan Iso 27002 Pada Data Center Pt.Gigipatra Multimedia," *J. TIM Darmajaya*, vol. 01, no. 02, pp. 175–191, 2015.