ISSN: 2548-8082 / E-ISSN 2615-6350
Vol.3 No.2 Edisi 2019

AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK STIKES JENDERAL ACHMAD YANI MENGGUNAKAN SNI ISO/IEC 27001:2013

Saepudin[1], M. Hendayun[2], Arief Zulianto[3]

[1,2,3] *Program Pendidikan Magister Program Studi Teknik Informatika*
Jln. Karapaitan No. 116, Bandung Jawa Barat
E-mail: Saepudinst@gmail.com[1)], mhendayun@gmail.com[2)], madzul@stei.itb.ac.id[3)]

Abstraksi

Sistem informasi akademik yang ada di STIKES (Sekolah Tinggi Ilmu Kesehatan) telah diimplementasikan dan digunakan untuk memudahkan dalam mengelola akademik. Kurangnya kesadaran keamanan infomasi pengguna, pengelolaan hak akses yang tepat, pemeliharaan keamanan jaringan, keamanan fisik dan operasional menyebabkan resiko terganggunya sistem informasi akademik oleh orang yang tidak bertanggung jawab. Untuk melihat kelemahan-kelemahan yang ada pada sistem informasi akademik harus dilakukan audit dengan menggunakan standar ISO/IEC 27001:2013. Tahapan untuk melakukan audit yaitu: merencanakan, melaksanakan, menganalisis hasil temuan. Ruang lingkup yang akan diaudit adalah klausul keamanan sumber daya manusia, klausul keamanan kontrol akses, klausul keamanan fisik dan lingkungan, klausul keamanan operasional, klausul kemanan komunikasi, dengan tujuan dilakukan audit adalah untuk membuat perancangan kontrol keamanan pada sistem informasi akademik. Hasil dari audit kepatuhan terhadap ISO/IEC 27001:2013 dengan rumus jumlah pertanyaan yang sesuai dengan penerapan ISO/IEC 27001:2013 dibagi dengan total jumlah soal yang diberikan pada auditee. Klausul keamanan sumber daya manusia dengan nilai 14,3 % , klausul keamanan kendali akses dengan nilai 33.3 %, klausul keamanan fisik dan lingkungan dengan nilai 46.6 %, klausul keamanan operasional dengan nilai 26.6 %, dan klausul keamanan komunikasi dengan nilai 66.6 %. Untuk melakukan perbaikan dilakukan perancangan kontrol keamanan sistem informasi akademik yang nilainya dibawah 50 %, dengan membuat kebijakan, prosedur dan formulir sehingga didapatkan kontrol keamanan yang lebih baik.

Kata kunci :

Audit, keamanan informasi, sistem informasi, SNI ISO/IED 27001:2013, rekomendasi

Abstract

The academic information system in STIKES (Sekolah Tinggi Ilmu Kesehatan) has been implemented and used to facilitate academic management. Lack of security awareness of user information, management of appropriate access rights, maintenance of network security, physical and operational security causes the risk of disruption of academic information systems by people who are not responsible. To see weaknesses in academic information systems, an audit must be conducted using the ISO / IEC 27001: 2013 standard. Stages for conducting audits are: planning, implementing, analyzing findings. The scope to be audited is a human resource security clause, an access control security clause, a physical and environmental security clause, an operational security clause, a communication security clause, with the aim of conducting an audit to create a security control design on academic information systems. The results of the compliance audit on ISO / IEC 27001: 2013 with the formula for the number of questions in accordance with the application of ISO / IEC 27001: 2013 divided by the total number of questions given to the auditee. Human resource security clause with a value of 14.3%, access control security clause with a value of 33.3%, physical and environmental security clause with a value of 46.6%, operational security clause with a value of 26.6%, and communication security clause with a value of 66.6%. To make improvements, the design of academic information system security controls is designed with a value below 50%, by making policies, procedures and forms to obtain better security controls.

***Keywords** :*

Audit, information security, information system, SNI ISO/IED 27001:2013, recommendation

Pendahuluan

Penerapan Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi keharusan dan kebutuhan di setiap instansi penyelenggara pelayanan publik mengingat peran TIK yang semakin penting bagi upaya meningkatkan kualitas layanan. Dalam menyelenggarakan TIK, faktor keamanan informasi merupakan aspek penting yang harus diperhatikan mengingat pengelolaan TIK akan terganggu jika informasi sebagai salah satu objek utama dalam pengelolaan TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (confidentiality), keutuhan (integrity), ketersediaan (availability).

STIKES (Sekolah Tinggi Ilmu Kesehatan) sudah menerapkan hak akses yang telah disesuaikan dengan tugas dan tanggung jawabnya masing-masing, akan tetapi masih sering mengalami gangguan seperti kecerobohan pengguna karena sering sharing hak akses kepada orang lain yang menyebabkan hak akses tersebut dapat digunakan oleh orang yang tidak bertanggung jawab, kurangnya pemeliharaan keamanan fisik yang ada di ruang server mengakibatkan pernagkat server kehilangan pasokan listrik, layanan terganggu disebabkan karena kurangnya pemeliharaan jaringan, pengelolaan sistem informasi akademik masih ada yang salah input dan menyebabkan data keluaran menjadi salah.

Sistem informasi akademik perlu dilakukan pengamanan agar tidak terganggu, kalau dibiarkan dan tidak ada tindak lanjut untuk perbaikan dikhawatirkan akan mengganggu dan timbulnya rasa ketidakpercayaan pengguna [2]. Untuk itu perlu dilakukan audit untuk melihat gambaran bagaimana kontrol keamanan sistem informasi yang sedang berjalan sudah sesuai dengan standar dan tujuan bisnis [3]. Ketidaksesuaian memungkinkan terjadinya kesalahan praktek dan tidak adanya kesempatan untuk mengembangkan atau memperbaiki keamanan sistem informasi.

Ada beberapa praktek terbaik yang dikembangkan peneliti untuk melakukan audit keamanan informasi diantaranya adalah COBIT 5 dan ISO/IEC 27001:2013. COBIT 5 merupakan kerangka komprehensif yang membantu perusahaan dalam mencapai tujuan dan menghasilkan nilai melalui tata kelola dan manajemen teknologi informasi yang efektif. Pemilihan ISO/IEC 27001:2013 sangat tepat karena standar ini fokus pada Sistem Manajemen Keamanan Informasi (SMKI), bertujuan membantu organisasi untuk membangun, mengembangkan, mempertahankan, dan terus meningkatkan keamanan sistem informasi [12] [4] [13].

Rumusan masalah yang akan dilakukan dalam penelitian ini seberapa patuh keamanan sistem informasi yang telah diterapkan sesuai dengan ISO/IEC 27001:2013 dan bagaimana cara memperbaiki kontrol keamanan yang sudah diterapkan berdasarkan hasil audit. Tujuan yang akan dicapai adalah mengetahui kepatuhan dan merancang keamanan sistem informasi akademik sesuai dengan ISO/IEC 27001:2013.

Tahapan untuk melakukan audit mengacu pada Forum ISO 27K [18] yaitu: menetukan ruang lingkup dan tujuan audit, perencanaan audit, pelaksanan audit, analisis hasil audit dan hasil outcame merancang keamanan sistem informasi akademik.

Metode Penelitian

A. Metode Penelitian

Dalam penelitian ini akan melakukan audit dimana lokasi permasalahan yang dipilih adalah kasus yang ada di instansi pendidikan STIKES, mengenai masalah keamanan pada sistem informasi akademik dan akan diselesaikan dengan melakukan audit. Hasil audit berupa temuan yang nantinya akan dianalisis untuk dicarikan solusinya berupa rekomendasi yang bersifat deskripsi atau gambaran untuk melakukan perbaikan.

B. Teknik Pengumpulan Data

Dalam melakukan audit harus ada lembar kerja sebagai panduan untuk melakukan wawancara atau pemeriksaan kemudian memverifikasinya. Perolehan data dalam audit ini berdasarkan wawancara karena audit yang dilakukan peneliti adalah audit secara manual tidak melakukan audit berbantuan komputer. Teknik pengumpulan data dilakukan dengan melakukan wawancara dan hasil wawancara akan dianalisis. Wawancara yang akan dilakukan adalah wawancara personal kepada *auditee* dimana *auditee* adalah orang yang bertanggung jawab terhadap pekerjaannya. Wawancara dilakukan dengan tatap muka dan tempat wawancara dilakukan di STIKES Pemilihan responden atau bertindak sebagai *auditee* harus mempunyai informasi yang diinginkan oleh peneliti dalam hal ini disebut *auditor* atau pewawancara. *Auditee* harus mau bekerja sama untuk memberikan informasi yang dibutuhkan oleh *auditor* atau pihak pewawancara.

C. Tahapan Penelitian

Menjelaskan tahapan dan prosedur dalam merancang sistem manajemen keamanan informasi mengacu pada panduan audit ISO/IEC 27001 disesuaikan dengan kebutuhan penelitian, adapun langkah dan prosedur dapat dijabarkan sebagai berikut:

1. Menentukan ruang lingkup dan tujuan audit, ruang lingkup kendali kontrol keamanan secara teknikal.

2. Persiapan dan perencanaan audit, membuat instrumen dan persiapan penentuan jadwal dan pihak auditee harus dipersiapkan
3. Pelaksanaan audit, melakukan wawancara ke lapangan dengan panduan pertanyaan sesuai dengan instrumen audit yang telah dibuat.
4. Analisis hasil audit, menganalisis hasil temuan audit untuk dicarikan solusinya.
5. Perancangan perbaikan kontrol keamanan untuk melakukan perbaikan, jika ada ketidaksesuaian dengan ISO/IEC 27001:2013

Hasil dan Pembahasan

A. Menentukan Ruang Lingkup dan Tujuan Audit

Ruang lingkup berdasarakan permasalahan yang ada, sesuai dengan hasil wawancara awal, adapun dari hasil wawancara awal bahwa kesadaran keamanan informasi sangat kurang, kontrol akses belum maksimal, banyaknya insiden keamanan karean kurangnya pemeliharaan keamanan fisk dan jaringan dan kurangnya keamanan operasional. Pemetaan kontrol keamanan pada ISO/IEC 27001:2013 dapat dipetakan menjadi A.7 keamanan sumber daya manusia, A.9 keamanan kendali akses, A.11 keamanan fisik, A.12 keamanan operasional dan A.13 keamanan komunikasi.

B. Pelaksanaan Audit

Dalam melaksanakan audit harus ada persetujuan dari pihak yang diaudit adapun persetujuannya ada pada lampiran. Setelah persetujuan audit yang di dalamnya dijelaskan tujuan dilakukan audit dan klausul mana saja yang akan diaudit, serta hasil dari audit berupa perancangan kontrol keamanan untuk meminimalisir resiko.

C. Analisis dan Rekomendasi Keamanan Sumber Daya Manusia

Setelah melakukan audit keamanan sumber daya manusia pada saat ini dan rekomendasi untuk perbaikan kontrol keamanan dapat dilihat pada tabel berikut :

Tabel C Hasil Analisis dan Rekomendasi Keamanan Sumber Daya Manusia

Analisis A.7.1.1:
Bagian kepegawaian sudah melakukan proses seleksi sesuai dengan aturan dan ketentuan yang berlaku di lingkungan STIKES, mulai dari proses Pengumuman lowongan pekerjaan, Seleksi dokumen dengan kelengkapan seperti KTP, surat berkelakuan baik dari kepolisian, surat lamaran, ijazah, daftar riwayat hidup Pemanggilan untuk interviu Pemanggilan untuk menjadi pegawai Belum ada formulir untuk perjanjian kerahasiaan kepada calon pegawai untuk menghindari pelanggaraan keamanan informasi Harus ada kebijakan dari pimpinan bahwa setiap pegawai yang diterima harus mengisi dan menandatangani surat perjanjian kerahasiaan Dibuat surat perjanjian kerahasiaan sesuai dengan ketentuan yang ada dan berlaku di STIKES
Rekomendasi :
Kebijakan : Pegawai yang diterima di lingkungan STIKES wajib mengisi perjanjian kerahasiaan dengan formulir yang telah disediakan
Analisis A.7.2.1:
Pimpinan belum berkomitmen untuk mengarahkan dan mewajibkan untuk menerapkan keamanan informasi, salah satu jalan untuk menerapkan keamanan sistem informasi dengan mewajibkan pelatihan kesadaran keamanan informasi minimal tiga bulan sekali
Rekomendasi :
Kebijakan : semua pegawai diwajibkan untuk pelatihan kesadaran keamanan informasi minimal tiga bulan sekali
Analisis A.7.2.2:
Pimpinan belum komitmen untuk meningkatkan pengetahuan pegawai tentang kesadaran keamanan informasi, untuk itu perlu dilakukan pelatihan minimal tiga bulan sekali , dan prosedur pelatihan harus dibuat dan hasil pelatihan harus dievaluasi.
Rekomendasi :
Kebijakan : bahwa setiap pegawai yang telah melakukan pelatihan harus dievaluasi dan mengisi formulir evaluasi pelatihan Dibuat prosedur pengajuan pelatihan Dibuat formulir untuk evaluasi hasil pelatihan
Analisis A.7.2.3:

Pelanggaran keamanan informasi seperti sering terjadinya sharing password antara pengguna, belum dilakukan tindakan atau sanksi, disebabkan belum adanya aturan dan kebijakan
Rekomendasi :
Harus ada kebijakan bahwa pegawai yang melanggar keamanan informasi akan diberikan sanksi berupa teguran dan pemecatan. Membuat aturan atau sangsi berupa formulir yang disatukan dengan formulir perjanjian kerahasiaan
Analisis A.7.3.1:
Penghentian dan perubahan tanggung jawab pegawai telah diatur sesuai dengan aturan yang ada di STIKES, pegawai yang keluar dari STIKES masih membawa hak akses, karena belum ada prosedur untuk penghapusan hak akses
Rekomendasi :
Kebijakan : semua pegawai yang telah keluar atau diberhentikan atau ada perubahan peran dan tanggung jawab (mutasi) maka hak akses tersebut harus: Dicabut untuk pegawai yang keluar Disesuaikan untuk pegawai yang dipindahtugaskan
Nilai kepatuhan : Jumlah total jawaban yang sesuai = 1 Jumlah total pertanyaan = 7 1/7X100% = 14,3 %
Perancangan kebijakan keamanan sumber daya manusia Formulir perjanjian kerahasiaan Formulir evaluasi pelatihan Formulir data pegawai Prosedur pelatihan kesadaran keamanan informasi

D. Analisis dan Rekomendasi Keamanan Kendali Akses

Setelah melakukan audit keamanan kendali akses pada saat ini dan rekomendasi untuk perbaikan kontrol keamanan dapat dilihat pada tabel berikut:

Tabel D Hasil Analisis dan Rekomendasi Keamanan Kendali Akses

Analisis A.9.1.1:
Kebijakan kendali akses belum terdokumentasi, membatasi akses sesuai dengan peran dan tanggung jawab. Mahasiswa, dosen dan administrator mempunyai tugas dan tanggung jawab yang berbeda-beda
Rekomendasi :
Semua kebijakan kontrol akses harus dituangkan dalam kebijakan pimpinan STIKES.
Analisis A.9.2.1 :
Ada proses pendaftaran ke admin akan tetapi tidak diketemukan prosedur dan alur permohonan / penghapusan hak akses yang didokumentasikan.
Rekomendasi :
Harus dibuat prosedur permohonan dan penghapusan hak akses Mahasiswa, dosen, karyawan dan pengelola harus mendaftar sebelum masuk ke sistem informasi akademik
Analisis A.9.2.2:
Sebelum mendapatkan hak akses pengguna harus mendapatkan ijin dan pemilik sistem sesuai dengan proses registrasi yang telah ditetapkan dan tingkatan hak akses disesuaikan dengan peran sebagai mahasiswa, dosen dan administrator.
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013
Analisis A.9.2.3 :
Hak akses istimewa diberikan kepada Kepala PUSISFO, hak akses istimewa ini hanya digunakan oleh orang yang benar-benar mengerti.
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013
Analisis A.9.2.4 :
Belum adanya kebijakan yang mengharuskan kata sandi harus diamankan untuk menghindari penggunaan oleh orang yang tidak bertanggung jawab
Rekomendasi :
Setiap pengguna wajib mengamankan kata sandi yang telah diberikan supaya terhindar dari penggunaan yang tidak sah oleh orang yang tidak bertanggung jawab Semua pegawai harus menggunakan password yang kuat, tidak boleh sama dengan user ID, tidak boleh menggunakan password yang mudah ditebak, tidak menggunakan password sesuai dengan tahun kelahiran

Analisis A.9.2.5:
Hak akses sama sekali belum direviu untuk menjamin hak akses yang diberikan sesuai dengan tugas dan perannya seharusnya direviu secara berkala.
Rekomendasi :
Administrator harus sering mereviu hak akses pengguna secara berkala
Analisis A.9.2.6 :
Penghapusan dilakukan untuk pemegang hak akses yang sudah keluar dan akan disesuaikan hak aksesnya jika pegawai dipindahtugaskan, tidak terdapat dokumentasi proses tersebut
Rekomendasi :
Hak akses harus dicabut untuk pegawai yang sudah keluar dari STIKES dan hak akses akan disesuaikan jika pegawai dipindahtugaskan
Analisis A.9.3.1:
Pengguna belum mengikuti aturan yang ada untuk mengamankan kata sandi sesuai denagn standar yang ditetapkan, pengguna belum memastikan bahwa perangkat pengolah informasi yang digunakan mendapat perlindungan pada saat ditinggalkan, pengguna sudah melakukan perlindungan agar informasi rahasia tidak diketahui oleh orang yang tidak berhak
Rekomendasi :
Pegawai harus mengamankan user- ID dan password yang dimilikinya supaya terhindar dari penggunaan yang tidak sah Pegawai tidak diperbolehkan mencatat user-ID dan password di kertas, media elektronik dan tempat lain. Pegawai harus bertanggung jawab untuk mengamankan user ID dan password yang dimilikinya Pegawai harus memastikan perangkat untuk mengakses informasi akademik yang digunakannya mendapatkan perlindungan, terutama pada saat ditinggalkan. Pegawai harus melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.
Analisis A.9.4.1:
Pada aplikasi informasi akademik sudah ada menu untuk mengelola hak akses sesuai dengan peran dan tanggung jawab. Peran sebagai mahasiswa hanya bisa mengedit profil dan melihat jadwal, nilai dan melakukan perwalian. Dosen hanya bisa merubah profil dan membuat penilaian terhadap mahasiswa. Administrator mempunyai hak akses dengan tingkatan yang tertinggi, pengelola hanya bisa digunakan terbatas untuk mengelola akademik saja
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013
Analisis A.9.4.2:
Semua pengguna baik dosen, mahasiswa dan admin untuk masuk ke aplikasi informasi akademik harus memasukan user ID dan password , user ID mahasiswa menggunakan nomor induk mahasiswa, user ID dosen menggunakan nomor induk karyawan, user ID administrator menggunakan nomor induk karyawan, tidak menampilkan apapun pada aplikasi informasi akademik sampai proses log on selesai. Peringatan akan tampil jika mahasiswa, dosen dan admin melakukan kesalahan memasukan user ID atau password. Tidak ada pesan apapun sampai proses log on selesai.
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013
Analisis A.9.4.3:
Aplikasi informasi akademik sudah menerapkan user ID dan password untuk menjaga akuntabilitas, pada aplikasi ini pengguna baik dosen, mahasiswa dan admin dapat merubah password masing-masing sesuai dengan ketentuan yang ada di STIKES. Pada saat penggantian password diwajibkan untuk membuat password yang kuat dengan menggunakan gabungan beberapa karakter huruf, angka dan lain-lain. Pada saat penggantian harus menggunakan password yang lain yang belum pernah dimasukkan sebelumnya. Penggantian password belum dilakukan secara berkala, password yang dikirim ke database sudah terenkripsi dengan baik menggunakan teknik kriptografi.
Rekomendasi :
Kebijakan : Pegawai yang memiliki hak akses, penggantian password harus selalu dilakukan secara periodik minimal 3 bulan sekali
Nilai kepatuhan : Jumlah total yang sesuai = 4 Jumlah total pertanyaan = 12 3/14 x 100 = 33,3 %
Perancangan kebijakan keamanan kendali akses Prosedur pencabutan hak akses pegawai keluar/dipindahtugaskan Prosedur mereviu hak akses Prosedur pendaftaran /penghapusan hak akses Formulir pendaftaran hak akses

E. Analisis dan Rekomendasi Keamanan Fisik dan Lingkungan

Setelah melakukan audit keamanan fisik dan lingkungan pada saat ini dan rekomendasi untuk perbaikan kontrol keamanan dapat dilihat pada tabel berikut:

Tabel E Hasil Analisis dan Rekomendasi Keamanan Fisik dan Lingkungan

Analisis A.11.1.1:
Sudah ada dinding pembatas dengan menggunakan tembok dalam ruangan seluas duabelas meter persegi
Rekomendasi ;

Sudah sesuai dengan ISO/IEC 27001:2013
Analisis A.11.1.2 :
1.Orang tidak bisa masuk sembarangan
2.Tidak ada buku tamu untuk masuk ke ruangan server, dan tidak pernah didampingi oleh petugas yang bertanggung jawab terhadap server. Dikhwatirkan akan mengganggu perangkat yang sedang berjalan tanpa PUSISFO ketahui Tidak bisa masuk sembarangan karena terkunci
Rekomendasi :
1. Sesuai dengan ISO/IEC 270012013 2.Setiap ada pekerjaan dalam ruang server harus mengisi buku tamu dan didampingi oleh salah satu petugas penangung jawab server untuk mengawasi jalannya pekerjaan sehingga tidak mengganggu jalannya operasional. 3.Harus membuat buku tamu
Analisis A.11.1.3 :
Sudah memperkirakan bahwa dulu pernah kebanjiran tapi belum menimpa server tapi area lain, untuk itu dipindahkan ke lantai dua. Untuk keamanan pencurian dipasang kunci.
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013
Analisis A.11.1.4 :
Alat pemadam kebakaran sudah disiapkan untuk menghindari kebakaran
Rekomendasi :
Sesuai ISO/IEC 27001:2013
Analisis A.11.1.5 :
Sudah ada CCTV untuk mengetahui kejadian atau hal yang tidak diinginkan
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013
Analisis A.11.2.1 :
Peralatan terpasang dalam rak yang kokoh, adanya grounding untuk anti petir, grounding tidak dilindungi dari ancaman orang yang tidak bertanggung jawab
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013
Analisis A.11.2.2 :
UPS selalu dicek dengan baik
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013
Analisis A.11.2.3 :
Kabel power dan jaringan sudah dipisahkan di ruangan server, akan tetapi masih ada temuan di tempat lain kabel jaringan dan power ada yang disatukan, untuk itu perlu konsistensi untuk pemisahan tersebut
Rekomendasi
Dilakukan pemeriksaan secara menyeluruh untuk memastikan bahwa kabel jaringan dengan kabel power sudah terpisah.
Analisis A.11.2.4 :
Tidak ada daftar pengecekan, sehingga tidak ada pelaporan kepada atasan bahwa pengecekan sudah dilakukan
Rekomendasi :
Setiap sebulan sekali harus ada laporan dari masing-masing pemilik aset ke Kepala PUSISFO untuk pengecekan semua peralatan dengan baik
Analisis A.11.2.5 :
Pemindahan aset dari ruang server ke luar selalu minta ijin kepada Kepala PUSISFO. Tetapi tidak melakukan dokumentasi berupa berita acara
Rekomendasi :
Setiap barang yang keluar atau masuk harus ada berita acara untuk dokumentasi
Analisis A.11.2.6 :
Keluar masuk aset yang tidak didokumentasikan akan menyebabkan hilangnya aset tertentu, untuk itu berita acara harus tetap dibuat
Rekomendasi :

Harus membuat berita acara untuk setiap aset yang masuk atau keluar Formulir untuk berita acara serah terima barang harus tersedia
Analisis A.11.2.7:
Kebijakan harus ada karena aset informasi seperti komputer yang sudah tidak terpakai akan digunakan kembali baik oleh PUSISFO atau oleh divisi lain, untuk menghindari hal yang tidak diinginkan bahwa dalam komputer terdapat media penyimpanan seperti hardisk yang dapat menyimpan data mungkin data bersifat rahasia.
Rekomendasi :
Membuat kebijakan bahwa setiap aset yang mau digunakan kembali baik untuk keperluan PUSISFO atau oleh divisi lain, data sensitif atau data rahasia harus dibuang seperti memformat hardisk secara permanen.
Analisis A.11.2.8 :
Orang PUSISFO sangat mengerti benar bahwa di komputer atau laptop selalu di password dan menggunakan screen saver pada windows, akan tetapi tidak menyeluruh untuk semua pengguna lain untuk itu perlu adanya kebijakan
Rekomendasi :
Setiap perangkat pengguna yang digunakan untuk mengakses informasi akademik harus di password dan untuk windows menggunakan screen saver agar pada saat ditinggalkan otomatis log out
Analisis A.11.2.9 :
Kebijakan harus ada untuk memastikan bahwa semua informasi rahasia yang ada di flashdisk, hardisk harus diamankan dan disimpan dalam laci yang terkunci, laptop selalu log-out ketika tidak dipakai dan ditinggalkan
Rekomendasi :
Ada kebijakan tentang mengamankan peralatan yang berisi informasi rahasia seperti hardisk atau flashdisk disimpan di laci dan dalam keadaan terkunci Untuk peralatan seperti laptop harus log-out jika ditinggalkan atau tidak digunakan lagi
Nilai kepatuhan : Jumlah total yang sesuai = 7 Jumlah total pertanyaan = 15 Jadi 7/15 x 100 = 46,6 %
Perancangan kebijakan keamanan fisik dan lingkungan Membuat Formulir berita acara serah terima barang

F. Analisis dan Rekomendasi Keamanan Operasional

Setelah melakukan audit keamanan operasional pada saat ini dan rekomendasi untuk perbaikan kontrol keamanan dapat dilihat pada tabel berikut:

Tabel F Hasil Analisi dan Rekomendasi Keamanan Operasional

Analisis A.12.1.1 :
Panduan untuk masuk ke sistem informasi akademik sudah ada dan bisa didownload disitus resmi www.stikesayani.ac.id,
Rekomendasi :
Dua pertanyaan Sesuai dengan ISO/IEC 27001:2013
Analisis A.12.1.2 :
Belum adanya manajemen perubahan pada STIKES yang didalamnya terkait rencana, langkah mitigasi jika ada yang salah harus dibuat dan dikendalikan
Rekomendasi :
PUSISFO harus mengendalikan perubahan terhadap perangkat pengolah informasi.
Analisis A.12.1.3 :
Sudah ada manajemen kapasitas bandwidth
Rekomendasi :
Sesuai ISO/IEC 27001:2013
Analisis A.12.1.4 :
Sudah ada pemisahan antara pengembangan, pengujian dan operasional, setiap ada penambahan fasilitas atau perubahan fasilitas, developer selalu meng update-nya ke pihak STIKES
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013

Analisis A.12.2.1 :
Belum ada kebijakan yang melarang mendownload atau memasang perangkat lunak yang berbahaya, meskipun sudah ada antivirus akan tetapi antivirus yang terpasang masih versi trial.
Rekomendasi :
Melarang mendownload dan memasang perangkat lunak berbahaya seperti keylogger Memasang antivirus yang bukan versi trial Pegawai harus diberikan pelatihan kesadaran untuk dapat mengidentifikasi wabah dan untuk menjaga terhadap beberapa serangan vektor, seperti lampiran email yang mencurigakan.
Analisis :
Supaya himbauan bisa dipatuhi oleh pegawai, harus dibuat kebijakan yang disetujui dan didokumentasikan oleh pimpinan STIKES dan bagi yang melanggar harus ditindak dan diberi sanksi.
Rekomendasi :
Pegawai dilarang mendownload dan memasang penggunaan perangkat lunak yang berbahaya di komputer yang digunakan untuk mengakses informasi akademik
Analisis :
Petugas PUSISFO telah melakukan pengecekan dan pembersihan virus sampai bersih dan dapat digunakan untuk mengakses informasi akademik.
Rekomendasi :
Setiap perangkat pengguna untuk mengakses sistem informasi akademik harus bebas dari virus
Analisis A.12.3.1 :
PUSISFO telah melakukan cadangan dua minggu sekali yang dicadangakan hanya data saja, aplikasi dan konfigurasi tidak dilakukan. Cadangan dilakukan atas kesadaran PUSISFO karena tidak ada kebijakan dan prosedur yang disetujui oleh pimpinan, cadangan tidak dilakukan dengan menggunakan enkripsi juga belum pernah ada pengujian terhadap hasil cadangan tersebut. Ada beberapa kelemahan jika cadangan tidak diuji akan menyebabkan kegagalan pada saat restore dan mudahnya diakses oleh orang yang tidak bertanggung jawab jika hasil cadangan tidak dienkripsi dan cadangan harus disimpan di tempat yang jauh.
Rekomendasi :
Bahwa semua data, konfigurasi dan aplikasi harus dicadangkan sesuai dengan prosedur yang ditetapkan oleh pimpinan. Cadangan harus dienkripsi, diuji dan disimpan di tempat yang jauh Membuat prosedur cadangan dan *restore* data
Analisis A.12.5.1 :
Seharusnya dilakukan oleh staf PUSISFO yang berpengalaman untuk menginstal perangkat lunak harus mengikuti prosedur standar yang disetujui.
Rekomendasi
Instalasi perangkat lunak pada lingkungan operasional sistem harus dilaksanakan sesuai prosedur
Analisis A.12.6.1:
Memiliki program manajemen kerentanan dapat menjadi sangat penting untuk belajar tentang individu kerentanan dan resiko di sekitarnya. Ukuran proaktif ini dapat memungkinkan PUSISFO untuk lebih cepat menanggapi ancaman baru dan menerapkan langkah-langkah mitigasi untuk mengurangi risiko
Rekomendasi :
PUSISFO harus dapat memperoleh informasi mengenai kerentanan teknis dari sistem yang akan digunakan secara tepat waktu, ekspos organisasi terhadap kerentanan teknis tersebut harus dievaluasi, dan langkah-langkah yang tepat harus diambil untuk mengatasi risiko terkait.
Analisis A.12.7.1:
PUSISFO belum pernah melakukan audit, setiap penyelidikan dan audit sistem informasi harus direncanakan dan cakupan disepakati. Audit tidak boleh mengubah informasi apapun yang ditinjau dan akses auditor harus dipantau dan dicatat. Idealnya auditor harus memiliki akses hanya baca dan hanya menjalankan skrip audit mereka di luar jam kerja untuk meminimalkan gangguan.
Rekomendasi :
Aktivitas dan kebutuhan audit, termasuk verifikasi terhadap sistem operasional, harus secara hati-hati direncanakan dan disepakati untuk meminimalkan gangguan pada proses bisnis.
Nilai kepatuhan : Jumlah total yang sesuai = 4 Jumlah total pertanyaan = 15 4/15x 100 = 26.6 %

Perancangan Kebijakan keamanan Operasional

G. Analisis dan Rekomendasi Keamanan Komunikasi

Setelah melakukan audit keamanan komunikasi pada saat ini dan rekomendasi untuk perbaikan kontrol keamanan dapat dilihat pada tabel berikut:

Tabel G Hasil Analisis dan Rekomendasi Keamanan Komunikasi

Analisis A.13.1.1 :
PUSISFO sudah melakukan pengelolaan jaringan dengan baik, dipasangnya firewall dengan menggunakan mikrotik, semua akses dari luar ke dalam jaringan akan ditolak kecuali web aplikasi informasi akademik.
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013
Analisis A.13.1.2 :
Belum menerapkan manajemen resiko, terbukti banyak jaringan yang sangat riskan sekali untuk kegagalan koneksi seperti wifi dan switch yang tidak tertata rapih
Rekomendasi :
Semua jaringan harus rapi dan memudahkan untuk pengelolaan dan terhindar dari resiko
Analisis A.13.1.3 :
VLAN untuk memisahkan jaringan dalam wireless dan kabel, media kabel digunakan untuk internal staf dan admin dan Dosen. Mahasiswa diberikan akses wireless untuk mengakses internet dan informasi akademik. Untuk menjaga keamanan dari serangan luar yang akan mengganggu sistem informasi akademik maka akses wireless tidak dihubungkan dengan jaringan kabel. Jaringan kebel akses terbatas dan hanya bisa digunakan oleh Staf, dosen dan admin.
Rekomendasi :
Sesuai dengan ISO/IEC 27001:2013
Nilai kepatuhan : Jumlah total yang sesuai = 2 Jumlah total pertanyaan = 3 2/3x 100 =66,6 %
Hasil perancangan keamanan komunikasi tidak dilakukan karena sudah melebihi 50 %

Kesimpulan

A. Kesimpulan

Setelah dilakukan audit kepatuhan pada sistem informasi akademik di STIKES Jenderal Achmad Yani, maka didapatkan kesimpulan :

1. Tingkat kepatuhan penerapan kontrol keamanan yang telah dilakukan cukup baik untuk keamanan komunikasi mendapat nilai 66.6 %. Keamanan sumber daya manusia, keamanan kendali akses, keamanan fisik dan lingkungan, keamanan operasional mendapatkan nilai kurang dari 50 %, untuk itu akan dibuatkan rekomendasi sesuai dengan kebutuhan keamanan sistem informasi akademik yang ada di STIKES.
2. Untuk memperbaiki klausul-klausul yang tingkat kepatuhannya belum baik dibawah 50% dibutuhkan beberapa kendali berupa perancangan kebijakan, prosedur dan formulir.

B. Saran

1. Audit yang dilakukan menggunakan ISO 27001:2013 penelitian lain bisa menggunakann COBIT atau NIST.
2. Audit dalam penelitian ini hanya mengaudit kepatuhan penerapan kontrol keamanan sistem informasi akademik, untuk peneliti yang lain bisa mengaudit kinerja dan efisiensi kontrol keamanan yang telah diterapkan.

Dalam audit kepatuhan peneliti lain bisa menggunakan semua klausul untuk mendapatkan nilai yang lebih baik

Daftar Pustaka

[1] Direktorat Keamanan Informasi, “Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik,” 2011.

[2] J. S. Pan, V. Snasel, E. S. Corchado, A. Abraham, and S. L. Wang, “Information Security Management for Higher Education Institutions,” *Inf. Secur. Manag. High. Educ. Institutions*, p. 5, 2014.

[3] S. Wawak, “THE IMPORTANCE OF INFORMATION SECURITY MANAGEMENT IN CRISIS PREVENTION IN THE COMPANY,” *Glob. Econ. Cris. Chang.*, 2010.

[4] V. Arora, “Comparing different information security standards : COBIT v s . ISO 27001,” *BSI Stand.*, pp. 7–9, 2010.

[5] B. Von Solms, "Information Security governance : COBIT or ISO 17799 or both ?," 2005.
[6] M. Motii and E. Semma, "Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO / IEC 27002 for better use of ITG in the Moroccan parliament," no. June, 2017.
[7] S. Khanyile and H. Abdullah, "COBIT 5 : an evolutionary framework and only framework to address the governance and management of enterprise IT," no. September, p. 7, 2013.
[8] T. Orakzai, "COBIT, ITIL and ISO 27002 Alignment for Information Security Governance in Modern Organisations," *Ssrn*, no. 2, pp. 123–129, 2014.
[9] Y. Ozdemir, H. Basligil, P. Alcan, and B. M. Kandemirli, "Evaluation and Comparison of Cobit , ITIL and ISO27K1 / 2 Standards Within the Framework of Information Security," *Int. J. Tech. Res. Appl. e-ISSN 2320-8163*, vol. 11, no. 11, pp. 22–24, 2014.
[10] M. Motii and A. Semma, "Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for better use of ITG in the Moroccan parliament," *Int. J. Comput. Sci. Issues*, vol. 14, no. 3, pp. 49–58, 2017.
[11] M. Jakábová, J. Urdziková, and E. Mironovová, "Standardization of Information Security Management System: ISO/IEC 27001:2005, ITIL®, CoBIT®," *Int. J. Recent Contrib. from Eng. Sci. IT*, vol. 1, no. 2, p. 11, 2013.
[12] M. Syafrizal, "Information Security Management System (ISMS) Menggunakan Standar ISO/IEC 27001:2005," 2005.
[13] C. Chazar, "Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005," *J. Inf.*, vol. VII, no. 2, pp. 48–57, 2015.
[14] T. Pereira and H. Santos, "A Security Audit Framework to Manage," *Proc. 6th Int. Conf. ICGS3 2010*, pp. 9–18, 2010.
[15] P. G. Anarkhi, I. Kurnia, and A. H. N. Ali, "Penyusunan Perangkat Audit Keamanan Informasi Aplikasi Berbasis Web Menggunakan ISO/IEC 27001 Klausul Kendali Akses," *J. Tek. Pomits*, vol. 1, no. 1, pp. 1–5, 2013.
[16] P. Griffiths, "Information Audit: Towards common standards and methodology," *Bus. Inf. Rev.*, vol. 29, no. 1, pp. 39–51, 2012.
[17] C. Davis and M. Schiller, *IT Auditing: Using Controls to Protect Information Assets*, Second edi. Mc graw Hill, 2011.
[18] S. Jones, S. Ross, and R. Ruusalepp, "Data Audit Framework Methodology," *Jones Ross Ruusalepp*, no. May, pp. 1–70, 2009.
[19] ISACA, "Information systems auditing: tools and techniques," 2016.
[20] R. Sarno, "Audit Sistem & Teknologi Informasi." ITS Pess, surabaya, 2009.
[21] ToolkitISO27001, "Information Security Management System Auditing Guideline," no. 2, 2017.
[22] S. Al-dhahri, "Information Security Management System," no. January, 2017.
[23] Ii. Sarno, Ryanto dan Iffano, "Sistem Manajemen Keamanan Informasi." Surabaya, 2009.
[24] M. Irwan, P. Nasution, and M. Indonesia, "Urgensi keamanan pada sistem informasi," no. July, 2016.
[25] ISO 27001, "Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan Information technology – Security techniques – Information security management systems – Requirements." p. 54, 2013.
[26] P. . Slawomir Wawak, "The Importance of Information security Management," no. January 2010, 2015.
[27] G. Pavlov and J. Karakaneva, "Information Security management System in Organization," vol. 9, no. 4, pp. 20–25, 2011.
[28] P. Yugopuspito, "Prototip Self Assessment Audit Iso 17799," vol. 2007, no. Snati, 2007.
[29] D. Drljača and B. Latinović, "Frameworks for Audit of an Information System in Practice," *JITA - J. Inf. Technol. Appl. (Banja Luka) - APEIRON*, vol. 12, no. 2, 2017.
[30] T. Kristanto *et al.*, "Perancangan Audit Keamanan Informasi Berdasarkan Standar ISO 27001:2005 (Studi Kasus : PT Adira Dinamika Multi finance)," vol. 2005, no. September, pp. 1–6, 2014.
[31] A. Destiara, H. Tanuwijaya, and E. Sutomo, "Audit Keamanan Sistem Informasi pada instalasi Sistem Informasi Manajemen (SIM-RS) Berdasarkan Standar ISO 27002," vol. 27002, pp. 1–8.
[32] D. Rasmona, H. Tanuwijaya, and E. Sutomo, "Audit Keamanan Sistem Informasi pada Instalasi Sistem Informasi Manajemen RSUD Bangil Berdasarkan ISO 27002," *JSIKA*, vol. 3, no. 2, p. 6, 2013.
[33] B. E. Putro, "Analisa Control Self Assessment Audit Pada Klausul A . 5 Security Policy Hingga Klausul A . 9 Physical And Environmental Security Telkom Flexi Kebon Sirih Jakarta Pusat Menggunakan ISO ... Analisa Control Self Assessment Audit Pada Klausul A . 5 Security ," no. April, 2018.
[34] O. Prima, H. Tanuwijaya, and E. Sutomo, "Audit keamanan Informasi pada PT. Bank Rakyat Indonesia (PERSERO) Tbk. Unit Sukomro," *JSIKA*, vol. 5, no. 4, p. 6, 2016.
[35] E. W. T. Dheni Indra, Apol Pribadi, "Pembuatan Dokumen SOP Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja ISO 27002:2013 (Studi Kasus : CV. Cempaka Tulungagung)," *J. Tek. ITS*, 2017.
[36] P. A. Negara, D. A. N. R. Birokrasi, and R. Indonesia, "PEDOMAN PENYUSUNAN STANDAR OPERASIONAL PROSEDUR ADMINISTRASI PEMERINTAHAN," 2012.

Biodata Penulis

SAEPUDIN, memperoleh gelar DIPLOMA III (Amd) dari Politeknik-ITB Ciwaruga Bandung lulus tahun 1994, Program Studi Teknik Elektro, memperoleh gelar sarjana Teknik (S.T), Fakultas Teknik Elektro Program Studi Teknik Telekomunikasi Universitas Jenderal achmad yani (UNJANI) lulus tahun 1999. Tahun 2019 memperoleh gelar Magister Komputer (M.Kom) dari Program Teknik Informatika Universitas Langlangbuana UNLA.