MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

Audit Manajemen Keamanan Teknologi Informasi Menggunakan Standar ISO 27001 : 2005 Di PerguruanTinggi XYZ

[1)] Muhammad Sidik
UKSW Salatiga Jl. Diponegoro 52-60, Salatiga 50711, Jawa Tengah, Indonesia
E-Mail:mgcn.sidik@gmail.com
[2)] Ade Iriani
UKSW Salatiga Jl. Diponegoro 52-60, Salatiga 50711, Jawa Tengah, Indonesia
E-Mail:ade.iriani@staff.uksw.edu
[3)] Sri Yulianto
UKSW SalatigaJl. Diponegoro 52-60, Salatiga 50711, Jawa Tengah, Indonesia
E-Mail:sri.yulianto@staff.uksw.edu

ABSTRAK
Management audit is very important for any colleges towards the examination and assesment of their information technology management to gain efficient and effective business running process. Information technology security as an effort of internal controlling for risk and threat security minimization, is mainly considered due to all learning and lecturing administration activities use information technology. To find out how secure technology information is, it is then recquiring an audit to make sure everything run based on procedure. Standard used is framework international standardization organization (ISO) 27001:2005. It ischosen because framework can be adjusted with instrument of the research used in the organization. It is then developed and focused on information security management system (SMKI). As a results, all have outcome JPA = PA1:PA10, NA=JPA/10 produces value average 65%. Last but not at least, it showspositive level, but still under expectation by college requirement that requires continuous evaluation and enhancement of recommended security control.
Keyword : Audit Manajement, Security technology information, ISO 27001: 2005.

PENDAHULUAN

Kemajuan teknologi informasi yang semakin cepat, berbanding terbalik dengan resiko keamanan informasi yang semakin besar. Usaha dalam mencapai tujuan bisnis perguruan tinggi menggunakan teknologi informasi dalam mengelola data informasi untuk menciptakan layanan yang berkualitas pada tujuan dan proses bisnis.

Perguruan tinggi perlu untuk menjamin keamanan serta privasi dan integrasi data yang diolah, selain itu kinerja sistem informasi juga menjadi bagian penting yang harus di kelola dengan baik sehingga penggunaan teknologi informasi bisa lebih maksimal.[1]

Pengolahan teknologi informasi yang cukup komplek pada perguruan tinggi dilakukan dengan cara komputerisasi. Implementasi manajeman keamanan teknologi informasi yang dijalankan cukup baik. Tetapi, masih ada beberapa persoalan data yang belum terintegrasi dari sistem satu ke sistem lain, misalkan data atau informasi yang mudah di akses oleh pengguna diluar hak aksesnya dan kekurangan sumber daya manusia yang mengelola manajemen keamanan teknologi informasi.

Agar manajemen keamanan teknologi informasi dapat berjalan dengan baik, maka diperlukan audit[2]. Secara khusus tidak ada *framework* standar yang harus digunakan dalam proses audit manajeman keamanan teknologi informasi, maka dalam pelaksanan audit menggunakan *framework* atau standar sesuai dengan kebutuhan.[3]

Audit pada keamanan teknologi informasi menggunakan *International Standarization Organization* (ISO) 27001 : 2005 dipilih dengan pertimbangan bahwa standar ini sangat fleksibel untuk di gunakan dan di kembangkan sesuai kebutuhan perguruan tinggi, persyaratan keamanan serta tujuan dan proses bisnis.[4]

Permasalahan yang dihadapi adalah bagaimana rancangan manajemen keamanan infrastruktur agar lebih efektif dan efisien pada proses bisnis yang berjalan dan bagaimana

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

menyajikan instrumen audit yang sesuai dengan topologi jaringan yang digunakan.

Tujuan penelitian ini adalah membuat rancangan audit manajemen keamanan teknologi informasi yang sesuai dengan infrastruktur perguruan tinggi serta mengetahui tingkat keamanan infrastruktur teknologi informasi dengan menggunakan standar ISO 27001 : 2005 dan menyajikan instrumen audit manajemen keamananan teknologi informasi sesuai topologi yang relevan dengan tujuan dan proses bisnis.

BAHAN PENELITIAN

Pengertian audit adalah pemeriksaan temuan atau buktidengan kritis dan sistematis oleh pihak internal dan atau eksternal yang independen serta di bidangnya, terhadap laporan dan bukti pendukung dengan tujuan mendapatkan temuan kewajaran laporan serta bukti dan memberi rekomendasi yang lebih baik.

Audit teknologi informasi merupakan pengawasan dan pengendalian dari infrastruktur teknologi informasi secara keseluruhan[5]. Istilah lain dari audit teknologi informasi adalah audit teknologi seperti *software* dan *hardware* serta infrastruktur yang dipakai perguruan tinggi untuk menentukan apakah telah efektif dalam mencapai tujuan bisnis.[6]

ISO 27001 : 2005 adalah standar informasi *security* yang memuat prinsip-prinsip dasar SMKI, standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjauan ulang, pemeliharaan dan peningkatan SMKI berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran.[7]

Pemilihan klausul dan instrument berdasarkan analisa dan perancangan hasil observasi tempat penelitian kesesuaian objek audit IT dengan instrument ISO 27001:2005.[8]

Dalam penelitian ini menerapkan 10 klausul SMKI kontrol keamanan yaitu ; Sistem manajemen keamanan teknologi informasi, Tanggung jawab manajemen, Manajemen aset, *Human resource security*, Keamanan fisik dan lingkungan, Manajemen operasi dan komunikasi, Akses kontrol, Sistem informasi, pengembangan dan pemeliharaan, Manajemen pengolahan sistem keamanan dan Manajeman kelanjutan proses dalam proses audit yang dilakukan.[9]

Utomo, dkk. Keamanan informasi yang berhubungan dengan akses kontrol dan implementasi Tata Kelola Keamanan Informasi menurut standar ISO sehingga akan meningkatkan kinerja dan dokumen tata kelola nantinya akan dijadikan pedoman dalam pengolahan keamanan informasidengan judul Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya 1. ISSN: 2301-9271.[10]

Simic, dkk. Menunjukan bagaimana standar untuk evaluasi keamanan IT yang di intergasikan dengan KORA, seperti pemrosesan informasi atau voting online yang legal secara hukum IT,dengan judul Holistic and Law Compatible IT Security Evaluation: Integration of Common Criteria, ISO 27001/IT-Grundschutz and KORA. International Journal of Information Security and Privacy, 2013, IGI Global. [11]

Perbedaan dengan penelitian sebelumnya, metode yang digunakan dalam pelaksanaan audit, selain itu instrumen yang digunakan meliputi 10 klausul ISO 27001:2005 serta hasil audit disajikan dengan radar diagram agar mudah di pahami perguruan tinggi.

Prosentasi Audit (PA) merupakan hasil prosentasi klausul audit, didalam penelitian ini menggunakan 10 klausul audit.

Jumlah Prosentasi Audit (JPA) yaitu hasil keseluruhan pertanyaan, cakupan dan instrument yang terdiri dari 88 instrumen termasuk 10 klausul.

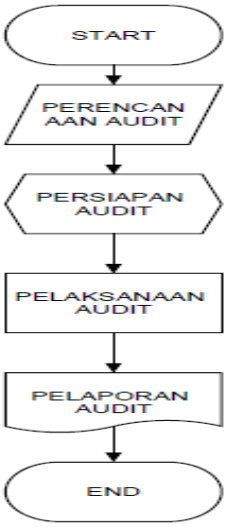
Nilai Akhir (NA) adalah hasil akhir audit dari prosentasi keseluruhan JPA dibagi 10 klausul. NA=JPA/10.

METODE PELAKSANAAN

Penelitian ini adalah penelitian kualitatif, Analisa yang dipakai dengan mendiskripsikan tingkat pengukuran atau penilaian SMKI pada perguruan tinggi XYZ Kota Semarang[12]

Adapun tahapan dalam penelitian ini dapat dilihat pada Gambar 2.

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089



Gambar 2. Metode Penelitian[13]

Metode penelitian terdiri dari empat bagian yaitu, tahap perencanaan audit, tahap persiapan audit, tahap pelaksanaan audit dan tahap pelaporan audit.

1. Perencanaan audit dilakukan penentuan proses dan tujuan bisnis, ditentukan melalui kajian pustaka, observasi dan *study* literatur agar penentuan proses bisnis sesuai dengan keadaan dan tujuan dari manajemen keamanan teknologi informasi perguruan tinggi.
2. Persiapan audit pembuatan instrument audit 10 klausul SMKI dengan 88 pertanyaan audit dimana setiap pertanyaan disesuaikan dengan tujuan bisnis dan proses bisnis yang telah dibuat secara objektif yang dilakukan pada tahap perencanaan audit. Penilaian setiap pernyataan disesuaikan dengan instrumen penilaian yang ditentukan sesuai dengan panduan implementasi yang ada pada standar ISO 27001 : 2005 yang disesuaikan dengan keadaan perguruan tinggi.
3. Pelaksanaan audit digunakan langkah pengumpulan dan pemeriksaaan data dilakukan dengan cara wawancara serta kuesioner ke Dosen, Ka. IT, Ka. Jaringan dan Penjamin Mutu selain itu observasi di tempat penelitian sesuai ruang lingkup yang telah disepakati.
4. Pelaporan audit menjadi tahap akhir pembuatan dan penyusunanlaporan berdasarkan temuan bukti di lapangan dan berisi saran atau rekomendasi perbaikan pada perguruan tinggi.

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.

Penilaian seluruh instrumen rerata dengan rumus JPA = PA1:PA10, NA=JPA/10 NA : nilai akhir, PA : prosentasi audit, JPA : jumlah prosentasi audit. Hasil audit keseluruhan bernilai *negatif* jika nilai 0 – 50 %, hasil audit keseluruhan bernilai *positif* jika nilai rerata 51 – 100 %.

HASIL DAN PEMBAHASAN

Dalam perencanaan audit, harus memahami proses bisnis dan teknologi informasi yang akan di audit. Pemahaman yang harus dilakukan yaitu mempelajari laporan, dokumen serta mengetahui apakah sebelumnya perguruan tinggi telah melakukan proses audit internal.

Topologi jaringan dan infrastruktur pada perguruan tinggi dimana terdapat tiga *server* utama dengan pembagian *server* yayasan, dosen dan mahasiswa. Jaringan yang keluar dari ruangan *server* utama di bagi kebeberapa *switch* luar ruangan, untuk pembagian di masing-masing ruangan dan laboratorium terdapat *switch* yang menghubungkan dari *switch* luar ruangan

Kontribusi Penelitian adalah :

1. Membuat instrumen baru yang spesifik untuk arsitektur atau topologi jaringan dalam skala tertentu, dalam mengaudit

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

managemen keamanan TI menggunakan 10 klausul audit yang didalamnya ada 88 pertanyaan audit.

2. Menghasilkan indikator baru yang di jadikan untuk mengukur data jaringan, persyaratan keamanan teknologi informasi pada system yang dibangun dan Rumusan instrument yang spesifik.

Berdasarkan analisa object audit dengan Framework ISO 27001 : 2005.

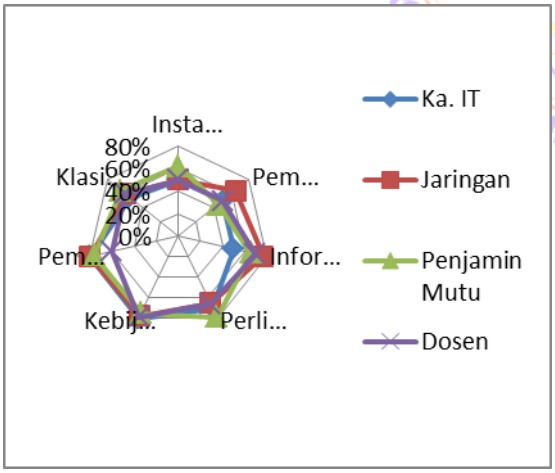
↓

Membuat instrument baru yang spesifik untuk jaringan skala tertentu dan Hasil disajikan dalam bentuk radar.

↓

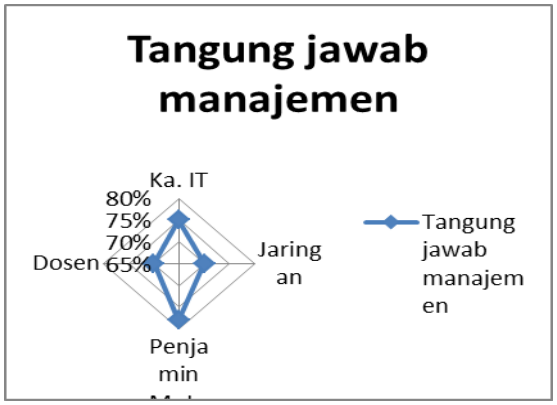
Indikator pengukuran yang digunakan adalah persyaratan keamanan teknologi informasi pada sistem yang dibangun dan Rumusan instrument.

Hasil Audit Dengan Menggunakan Diagram Radar



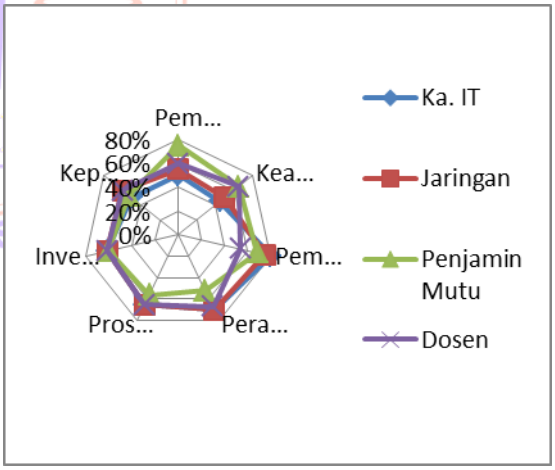
Gambar3. Representasi Sistem Manajemen Keamanan Teknologi Informasi.

Diagram Gambar 3 memiliki nilai, instalasi perangkat lunak dalam sistem operasi 53%, pembatasan instalasi perangkat lunak 53%, informasi tentang analisis dan spesifikasi persyaratan keamanan 66%, perlindungan aplikasi layanan transaksi 70%, kebijakan pengembangan yang aman 78%, pembatasan pada perubahan terhadap paket perangkat lunak 74% dan klasifikasi informasi 60%. Kinerja teknisi dan kepala laboratorium perguruan tinggi dalam melakukan instalasi perangkat lunak serta pembatasan aplikasi rata-rata 53% dapat di simpulkan dari kuesioner uji lapangan kinerja Baik.



Gambar 4.Representasi Tanggung Jawab Manajemen.

Diagram Gambar 4 dapat dianalisis tangung jawab manajemen dari hasil responden memiliki nilai rata-rata 73 % yang menunjukan bahwa tangung jawab manajemen secara keseluruhan baik.

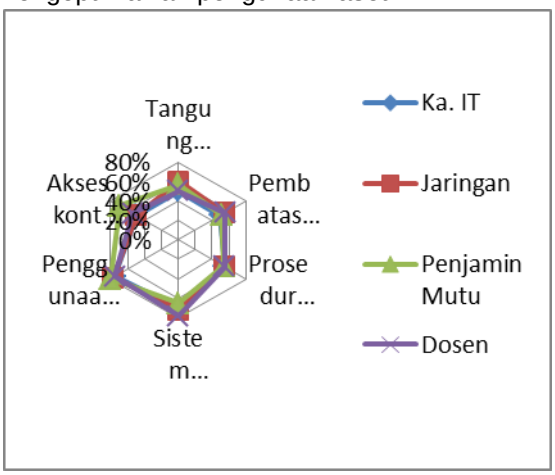


Gambar 5.Representasi Manajemen Aset.

Diagram Gambar 5 dapat dilihat pemindahan aset 60%, keamanan peralatan dan aset yang keluar 56%, pembuangan atau pemakaian kembali peratalan atau perangkat secara aman 69%, peralatan penggunaan tanpa pengawasan 65%, prosedur operasi yang terdokumentasi 63%, inventaris aset 61%, kepemilikan aset 56%. Pengolahan manajemen aset prakondisi untuk meyakinkan bahwa

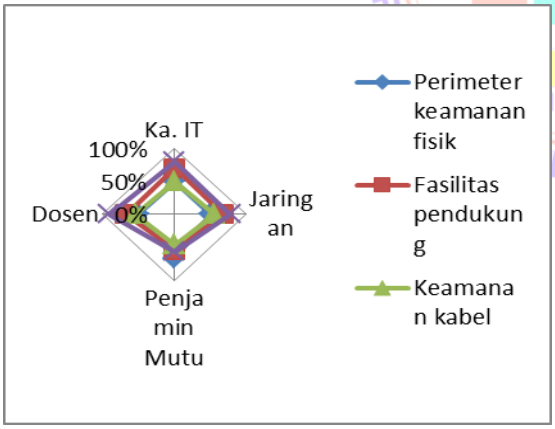
MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

perguruan tinggi mampu memanfaatkan tangung jawabnya dalam memelihara dan mengoptimalkan pengunaan aset.



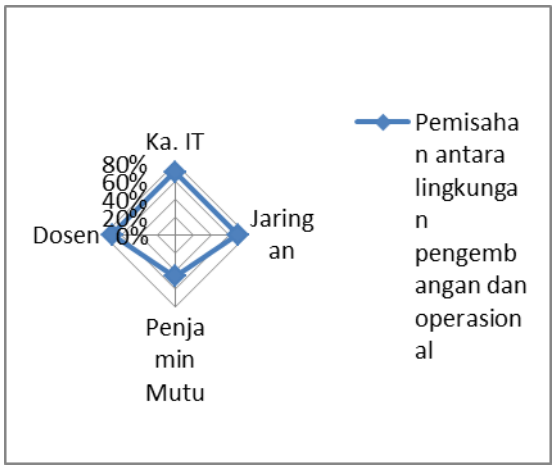
Gambar 6.Representasi *Human Resource Security.*

Dapat dicermati dari diagram Gambar 6 Tangung jawab pengakhiran pekerjaan 54%, Pembatasan akses informasi 53%, Prosedur keamanan *log in* 55%, Sistem manajeman password 71%, Penggunaan utility sistem 77%, Akses kontrol ke program kode sumber 56%. Pembatasan hak akses dan lemahnya tangung jawab pengakhiran pekerjaan, memiliki nilai rata-rata 53 % menunjukan bahwa kelalaian saat pengakhiran pekerjaan.



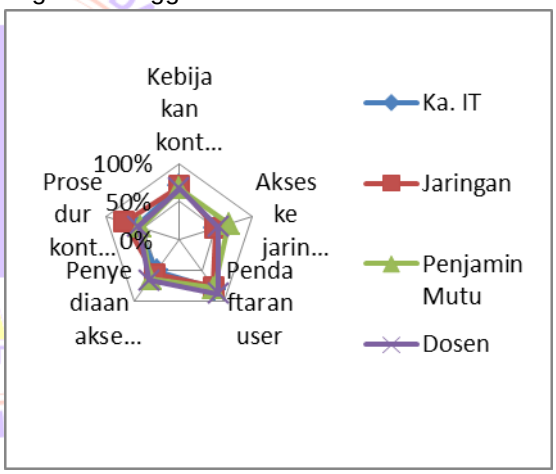
Gambar 7. Representasi Keamanan Fisik dan Lingkungan.

Diagram Gambar 7 Perimeter keamanan fisik 54%, Fasilitas pendukung 65%, Keamanan kabel 54% dan Pemeliharaan peralatan 74%. Dapat dilihat keamanan fisik yang belum rapi di setiap ruangan.



Gambar 8. Representasi Manajemen Operasi dan Komunikasi.

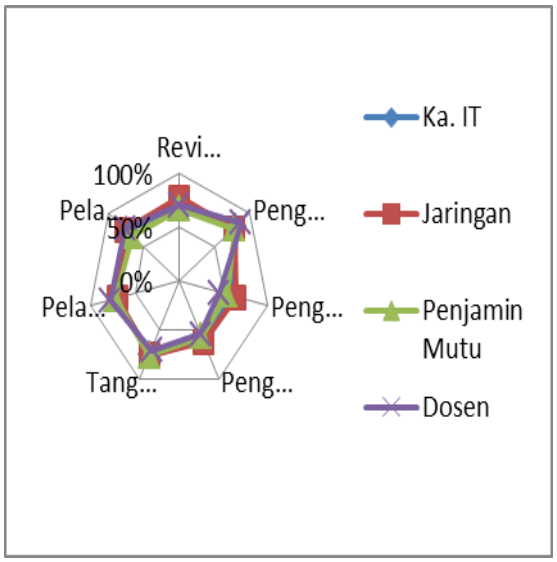
Dari diagram Gambar 8 pemisahan lingkungan pengembangan dan operasional menunjukan nilai rendah dengan rerata dari responden 64 %, yang artinya perlu perbaikan pemisahan lingkungan pengembangan di perguruan tinggi.



Gambar 9. Representasi Akses Kontrol.

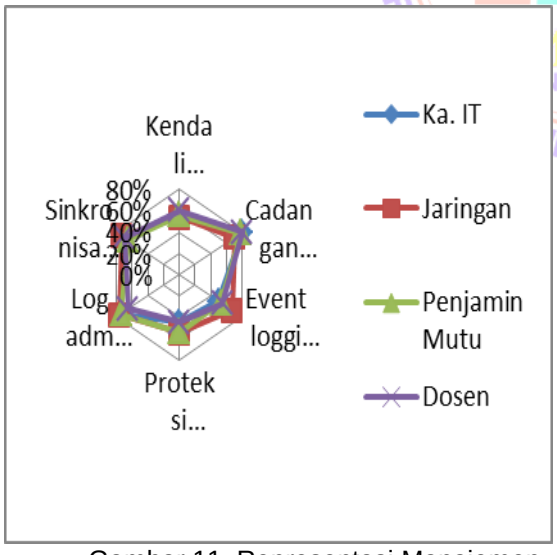
Dari diagram Gambar 9 Kebijakan kontrol akses 69%, Akses ke jaringan dan layanan jaringan 59%, Pendaftaran user 80%, Penyediaan akses pengguna 59%, Prosedur kontrol perubahan sistem yang sedang berjalan 61%. Dapat dicermati penyediaan akses pengguna dan akses ke layanan jaringan memiliki rata-rata 59 %.

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089



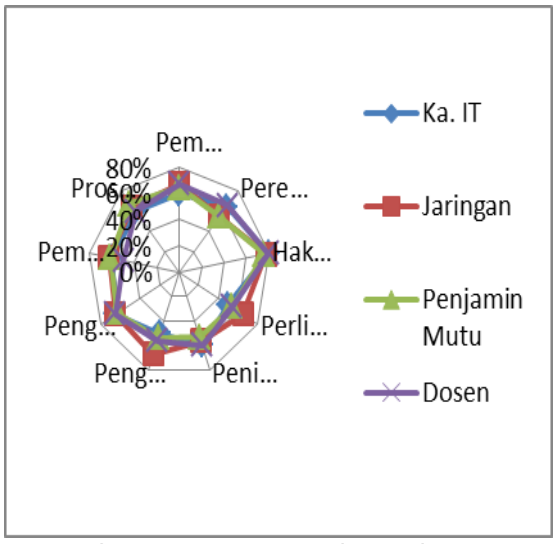
Gambar 10. Representasi Sistem Informasi, Pengembangan dan Pemeliharaan.

Dari diagram Gambar 10 Review secara teknis terhadap aplikasi setelah perubahan platform yang beroperasi 71%, Pengembangan perangkat lunak yang outsource 81%, Pengujian sistem keamanan 58%, Pengawasan dan peninjauan layanan pengembang 58%, Tangung jawab dan prosedur 74%, Pelaporan kejadian keamanan informasi 73%, Pelaporan kelemahan keamanan informasi 74%, Penilaian dan keputusan kejadian keamanan informasi 69%.



Gambar 11. Representasi Manajemen Pengolahan Sistem Keamanan.

Diagram Gambar 11 Kendali terhadap *malware* 56%, Cadangan informasi 77%, *Event logging* 56%, Proteksi terhadap informasi log 50%, *Log* administrasi dan operator 73%, Sinkronisasi petunjuk waktu manajeman keamanan sistem 70%.



Gambar 12. Representasi Manajeman Kelanjutan Proses.

Diagram Gambar 12 Pembelajaran dari insiden keamanan informasi 65%, Perencanaan keamanan informasi yang berkesinambungan 60%, Hak kekayaan intelektual (HAKI) 79%, Perlindungan data dan rahasia informasi pribadi 56%, Peninjauan pemenuhan teknis 57%, Pengendalian audit sistem informasi 57%, Pengendalian jaringan 65%, Pemisahan jaringan 59%, Prosedur dan kebijakan penyaluran informasi 63%.

Berikut ini adalah hasil dari pelaksanaan audit keseluruhan proses.

Tabel 2. Penilaian Klausul Audit.

No	Klausul Audit	% 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%

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

9	Manajemen pengolahan sistem keamanan	64%
10	Manajeman kelanjutan proses	62%

Setelah melakukan audit manajemen keamanan teknologi informasi, maka diketahui beberapa kondisi yang sesuai dengan standar ISO 27001 : 2005 yaitu;

1. Terdapat aturan mengenai tanggung jawab keamanan teknologi informasi pada perguruan tinggi.
2. Memiliki dokumentasi penetapan persyaratan keamanan informasi untuk kontrol akses pengguna.
3. Terdapat kebutuhan persyaratan keamanan teknologi informasi pada sistem yang dibangun.

KESIMPULAN

Audit manajemen keamanan teknologi informasi memiliki rancangan infrastruktur menjadi lebih efektif, efisien dan relevan pada tujuan serta proses bisnis yang sedang berjalan.

Memiliki instrumen audit manajemen keamanan teknologi informasi yang sesuai dengan topologi jaringan yang digunakan pada perguruan tinggi XYZ Kota Semarang dengan *Framework* ISO 27001:2005.

Hasil keseluruhan 10 klausul yang digunakan dalam penelitian ini adalah JPA = PA1:PA10, NA=JPA/10 NA : nilai akhir, PA : prosentasi audit, JPA : jumlah prosentasi audit, memiliki nilai akhir rerata 65%. Perlu pembenahan pada setiap temuan yang bernilai rendah, begitu juga dengan nilai baik harus ada pembenahan dengan melakukan evaluasi yang berkesinambungan.

Saran tindak lanjut agar penilaian audit keamanan teknologi informasi menjadi lebih baik secara teknis, perguruan tinggi dapat menerapkan audit manajemen keamanan teknologi informasi dalam runtun rentang waktu 12 bulan agar keamanan infrastruktur tetap terkontrol, penerapan standar operasional pekerjaan serta menginventaris seluruh asset yang dimiliki dan instrumen audit manajemen keamanan teknologi informasi menggunakan ISO 27001 : 2005.Dengan penilaian akhir model prosentasi diharapkan pengembangan penelitian selanjutnya sebagai bahan perbandingan.

DAFTAR PUSTAKA

[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] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] M. Utomo, A. Holil, N. Ali, and I. Affandi, “Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I," *Inst. Teknol. Sepuluh Nop.*, vol. 1, no. 1, pp. 2–7, 2012.

[11] 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.

[12] S. P.D, *Metode penelitian pendidikan pendekatan kuantitatif.pdf*. 2014.

[13] 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.