Jurnal Tera **E-ISSN : 2776-9666**
Volume 2, Issue 2, September 2022 **P-ISSN : 2776-1789**
Page 73 - 83

KERANGKA KERJA PENGELOLAAN KEAMANAN INFORMASI UNTUK MENUNJANG IMPLEMENTASI *E-LEARNING* PADA PERGURUAN TINGGI

Fakhria Nur Sabrina[1], Nur Farida Irmawati[2], Henri Septanto[3]
Universitas Dian Nusantara, Jakarta, Indonesia

Corresponding author: fakhria.nur.sabrina@undira.ac.id

Diterima : 11/02/2022
Direvisi : 18/08/2022
Dipublikasi : 30/09/2022

Abstrak: Kerangka Kerja Pengelolaan Keamanan Informasi harus melalui alur tahapan proses yang dimulai dari membuat tahapan persiapan, identifikasi aset, kebijakan dan dokumen pengelolaan keamanan informasi, operasional Teknologi Informasi (TI), jaringan komunikasi, pengamanan informasi serta keberlanjutan *Business Planning*. *E-learning* atau pembelajaran daring di era Pandemi Covid 19 sudah menjadi sebuah metode pembelajaran yang wajib dijalankan. *E-learning* sebagai sebuah sarana dan metode pembelajaran dipercaya dapat mengakomodasi pertemuan sebagai pengganti pertemuan tatap muka dalam pembelajaran. *E-learning* kampus yang dikembangkan sesuai dengan kebutuhan di sebuah perguruan tinggi harus dikelola dan terukur agar mutu dari pembelajaran tetap sesuai standar tata Kelola yang yang berlaku. Untuk menjamin dan mengurangi resiko keamanan informasi maka kerangka kerja pengelolaan keamanan informasi harus ditetapkan terlebih dahulu sebagai sebuah mekanisme kontrol untuk pengendalian terhadap tatakelola pada teknologi informasi. Pengukuran tatakelola teknologi informasi khususnya pada implementasi *E-learning* harus dilakukan. Penelitian ini bertujuan mengurangi resiko terhadap keamanan informasi saat penerapan *E-learning* dengan memastikan apakah kerangka kerja keamanan informasi telah dibuat dan dijalankan oleh perguruan tinggi. Sehingga dapat dilihat apakah *E-learning* yang dijalankan memiliki resiko tinggi terhadap masalah keamanan informasi atau sudah cukup aman untuk dijalankan, sehingga dapat dipastikan keberlanjutan *E-learning* dapat berjalan dengan baik,

Kata kunci: kerangka kerja, *E-learning*, keamanan informasi

Abstract: *The Information Security Management Framework must go through a flow of process stages starting from the preparation stages, asset identification, information security management policies and documents, Information Technology (IT) operations, communication networks, information security and Business Planning sustainability. E-learning or online learning in the Covid-19 pandemic era has become a learning method that must be carried out. E-learning as a learning tool and method is believed to be able to accommodate meetings as a substitute for face-to-face meetings in learning. Campus E-learning developed according to the needs of a higher education institution must be managed and measured so that the quality of learning remains in accordance with applicable governance standards. In order to guarantee and reduce information security risks, the information security management framework must first be established as a control mechanism for controlling the governance of information technology. Measurement of information technology governance, especially in the implementation of E-learning, must be carried out. This study aims to reduce the risk to information security when implementing E-learning by ascertaining whether an information security framework has been created and implemented by universities. So that it can be seen whether the E-learning that is run has a high risk of information security problems or is safe enough to run, so that it can be ascertained that the sustainability of E-learning can run well.*

Keywords: *framework, E-learning, information security*

PENDAHULUAN

Masalah keamanan informasi selalu cukup menarik untuk dibahas karena perkembangan teknologi informasi yang semakin cepat dan meluas. Semakin cepatnya perkembangan teknologi informasi ternyata terkadang tidak diikuti dengan penerapan keamanan informasi yang memadai, sehingga ancaman keamanan informasi selalu menjadi momok bagi penerapan sistem keamanan informasi dalam sebuah organisasi atau perusahaan (Februariyanti, 2006).

Salah satu kunci keberhasilan pengamanan sistem informasi adalah adanya visi dan komitmen dari level pimpinan tertinggi di manajemen organisasi. Upaya atau inisiatif pengamanan informasi akan percuma tanpa hal ini. Dengan tidak adanya komitmen dari level top manajemen, berdampak kepada investasi pengamanan informasi yang akan terbuang sia-sia. Pengamanan informasi tidak dapat tumbuh demikian saja tanpa adanya usaha dan biaya. Pengamanan informasi membutuhkan investasi yang cukup besar, namun sayang hal ini sering diabaikan karena tidak adanya komitmen dari pihak manajemen atau seluruh stake holder dalam solusi keamanan informasi.

E-learning atau pembelajaran daring di era Pandemi Covid 19 sudah menjadi sebuah metode pembelajaran yang wajib dijalankan. *E-learning* sebagai sebuah sarana dan metode pembelajaran dipercaya dapat mengakomodasi pertemuan sebagai pengganti pertemuan tatap muka dalam pembelajaran (Septanto, 2015).

Proses pengelolaan teknologi informasi harus terlebih dahulu didefinisikan oleh organisasi sebelum organisasi tersebut merancang struktur divisi atau unit teknologi informasi yang sesuai, karena secara prinsip, terlepas dari jenis atau bentuk struktur organisasi unit teknologi informasi, sejumlah proses tata Kelola harus dimiliki oleh organisasi. Konsep yang sangat baik dalam bentuk standar Tata Kelola Teknologi Informasi diperkenalkan oleh ISACF (*System Audit and Control Foundation*) yang diberi nama COBIT (*Common Objectives for Information and Related Technology*), COBIT diperuntukkan untuk menunjang konsep *IT Governance* (Indrajit, 2014).

E-learning kampus yang dikembangkan sesuai dengan kebutuhan di sebuah perguruan tinggi harus dikelola dan terukur agar mutu dari pembelajaran tetap sesuai standar tata Kelola yang yang berlaku. Untuk menjamin dan mengurangi resiko keamanan informasi maka kerangka kerja pengelolaan keamanan informasi harus ditetapkan terlebih dahulu sebagai sebuah mekanisme kontrol untuk pengendalian terhadap tatakelola pada teknologi informasi.

Pengukuran tatakelola teknologi informasi khususnya pada implementasi *E-learning* harus dilakukan. Penelitian ini bertujuan mengurangi resiko terhadap keamanan informasi saat penerapan *E-learning* dengan memastikan apakah kerangka kerja keamanan informasi telah dibuat dan dijalankan oleh perguruan tinggi. Sehingga dapat dilihat apakah *E-learning* yang dijalankan memiliki resiko tinggi terhadap masalah keamanan informasi atau sudah cukup aman untuk dijalankan, sehingga dapat dipastikan keberlanjutan *E-learning* dapat berjalan dengan baik.

Selain peran utama dari top manajemen,masih terdapat lagi masalah pengamanan system informasi, yaitu :

a. **Kesalahan desain** terjadi pada tahap desain dimana keamanan seringkali diabaikan atau dipikirkan belakangan (*after thought*).Sebagai contoh ada sebuah sistem informasi yang menganggap bahwa sistem informasi akan aman dan juga jaringan akan aman sehingga tidak ada desain untuk pengamanan data, misalnya dengan menggunakan enkripsi.

b. **Kesalahan implementasi** terjadi pada saat desain diimplementasikan menjadi sebuah aplikasi atau sistem. Sistem informasi diimplementasikan dengan menggunakan *software*. Sayangnya para pengembang *software* seringkali tidak memiliki pengetahuan mengenai keamanan sehingga aplikasi yang dikembangkan memiliki banyak lubang keamanan yang dapat dieksploitasi.
c. **Kesalahan konfigurasi** terjadi pada tahap operasional. Sistem yang digunakan biasanya harus dikonfigurasi sesuai dengan kebijakan perusahaan. Selain salah konfigurasi, ada juga permasalahan yang disebabkan karena tidak adanya kebijakan prosedural dari pemilik sistem sehingga menyulitkan bagi pengelola untuk melakukan pembatasan.
d. **Kesalahan penggunaan** terjadi pada tahap operasional juga. Kadang-kadang karena sistem terlalu kompleks sementara sumber daya yang disediakan sangat terbatas maka dimungkinkan adanya kesalahan dalam penggunaan. Kesalahan-kesalahan di atas dapat menimbulkan celah lubang keamanan. Celah ini belum tentu menimbulkan masalah, sebab bisa saja memang celah ada akan tetapi tidak terjadi eksploitasi. Namun celah ini merupakan sebuah resiko yang harus dikendalikandalam sebuah manajemen keamanan.

KAJIAN PUSTAKA

E-learning

E-learning adalah sebuah metode pembelajaran jarak jauh yang pada awalnya merupakan pilihan yang mungkin hanya dijalankan oleh kampus-kampus tertentu namun setelah era pandemi Covid 19 berlangsung akhirnya menjadi sebuah sistem pembelajaran yang harus dijalankan agar kegiatan belajar mengajar di kampus dapat terus berlangsung. Metode pembelajaran jarak jauh atau yang lebih dikenal dengan istilah *E-learning* ini memang pada awalnya diterapkan secara mendadak karena situasi dan kondisi sistem pembelajaran di era pandemic covid 19 tidak memungkinkan untuk melakukan tatap muka langsung, sehingga dalam awal pelaksanaannya terjadi banyak kekurangan baik dari sisi dosen, mahasiswa, administrasi akademik, perangkat *hardware* dan *software* dan infrastruktur penunjang yang mendukung kegiatan pembelajaran jarak jauh (Lionie *et al*, 2021).

Pengelolaan Keamanan Informasi sesuai ISO 27000

International Organization for Standardization (ISO) adalah sebuah organisasi internasional non-pemerintahan untuk standarisasi. Internasional Electrotechnical Commission (IEC) adalah suatu oraganisasi standarisasi internasional yang menyiapkan dan mempublikasikan standar internasional untuk semua teknologi elektrik, elektronika dan teknologi lain yang terkait, yang dikenal dengan elektroteknologi. Standarisasi di gunakan untuk mendukung inovasi dan memberikan solusi untuk tantangan global. Seri ISO/IEC 27000 merupakan pembaharuan dari ISO 17799. ISO/IEC 27001:2005 telah diadopsi Badan Standarisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) untuk SMKI.

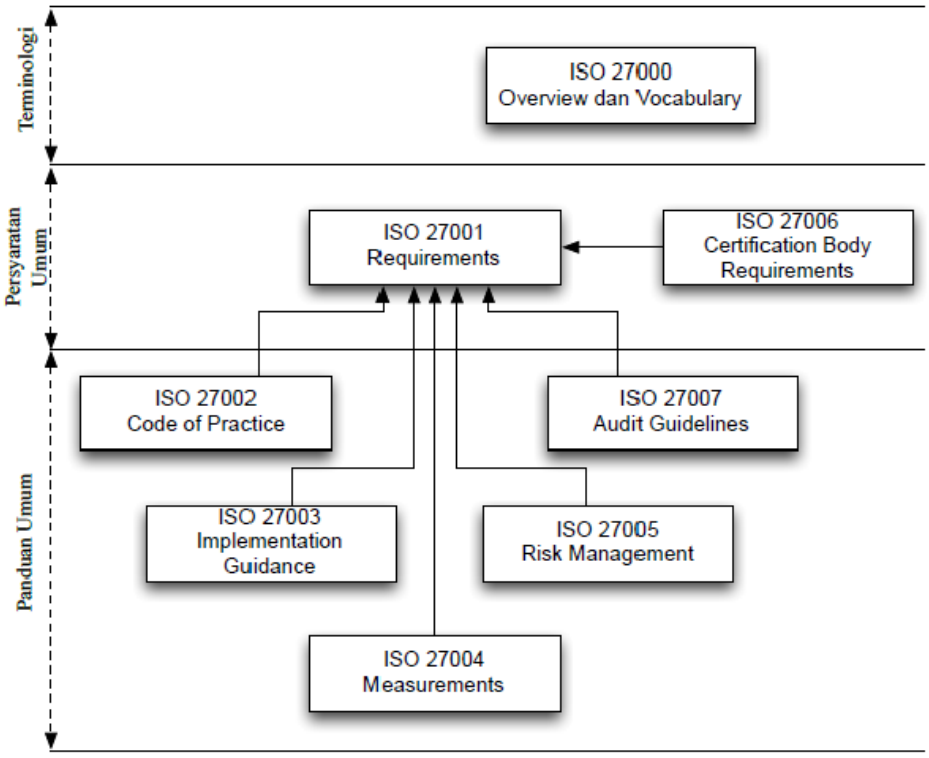
Ancaman-ancaman yang terjadi terhadap keamanan sistem informasi harus diantisipasi dengan pengelolaan Sistem Informasi yang baik. ISO/IEC 27000, merupakan standar tentang *Information Security Management System (ISMS)* atau dikenal juga dengan istilah Sistem Manajemen Keamanan Informasi (SMKI). Menurut ISO/IEC 27000:2014, ISMS adalah

pendekatan sistematis untuk menetapkan, mengimplementasi, operasional, pemantauan, peninjauan, pemelihharaan dan meningkatkan keamanan informasi pada organisasi untuk mencapai tujuan bisnis. (Chazar, 2015)

ISO/IEC 27000 berisi prinsip-prinsip dasar ISMS, definisi sejumlah istilah penting dan hubungan antar standar dalam keluarga ISMS. Standar ini dapat digunakan untuk semua jenis organisasi baik organisasi pemerintahan, komersial maupun non-komersial.

Pendekatan proses ini menekankan pada beberapa hal sebagai berikut:

1. Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi,
2. Penerapan dan pengoperasian kontrol untuk mengelola resiko keamanan informasi dalam bentuk konteks resiko bisnis organisasi secara keseluruhan,
3. Pemantauan dan tinjau ulang kinerja dan efektivitas ISMS
4. Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran.



Gambar 1. ISO 2700

Keamanan Informasi

Keamanan teknologi informasi‖ atau IT Security mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari tentunya, gangguan - gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan. Berbeda dengan ―keamanan informasi yang fokusnya justru pada data dan informasi, yang dalam hal ini tentunya data serta informasi milik perusahaan Pada konsep ini, usaha-usaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak

disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan. (Dewi, 2017)

Sistem Manajemen Keamanan Informasi

Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa Teknologi Informasi maupun industri lainnya, seperti: perusahaan export-import, tranportasi, lembaga pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal. Informasi atau data adalah aset bagi perusahaan. Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan return on investment dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan disharing maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan. (Syafrizal, 2007)

Sistem Manajemen Keamanan Informasi (*Information Security Management System* – ISMS) merupakan sebuah kesatuan system yang disusun berdasarkan pendekatan resiko bisnis, untuk pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaanserta peningkatan keamanan informasi perusahaan. Dan sebagai sebuah sistem, keamanan informasi harus didukung oleh keberadaan dari hal-hal berikut:

1. Struktur Organisasi
2. Kebijakan Keamanan
3. Prosedur dan Proses
4. Tanggung jawab

METODOLOGI PENELITIAN

Metode Pengumpulan Data

1. Jurnal
   Artikel dari berbagai jurnal perguruan tinggi yang membahas penelitian tentang berbagai Tata Kelola Teknologi Informasi dijadikan sebagai sumber referensi dalam penelitian ini.
2. Observasi
   Observasi dilakukan pada kegiatan operasional *E-learning* di Universitas XYZ
3. Interview
   Interview dilakukan pada orang-orang yang terlibat secara langsung pada operasional kegiatan *E-learning* yang terdiri dari Dosen, Kaprodi, Sekprodi dan Staf Akademik dan Staf IT di Universitas XYZ.

Analisa Keamanan Informasi *E-learning*

1. Identifikasi Asset Teknologi

Tahapan pertama melakukan identifikasi aseet perusahaan, asset dapat dilihat pada tabel 1.

Tabel 1. Identifikasi Asset

No.	Asset Perusahaan
1.	Database
2.	Server
3.	Data Centre
4.	Aplikasi
5.	Komputer/PC
6.	Anti Virus
7.	Firewall
8.	Hub
9.	Switch
10.	Bridge
11.	Router

2. Analisis *Capability Level*

Level kapabilitas proses yang digunakan di dalam penilaian proses terdiri dari enam level yaitu:

Level 0

Incomplete process, yaitu proses tidak diimplementasi atau gagal mencapai tujuan proses. Terdapat sedikit atau tidak ada bukti pencapaian tujuan proses secara sistematis.

Level 1

Performed process, yaitu implementasi proses mencapai tujuannya. *Process performance* mengukur sampai sejauh mana tujuan proses dicapai. Hasil pencapaian atribut ini tercermin dari setiap proses menghasilkan keluaran yang diharapkan.

Level 2

Managed process, yaitu proses pada level 1 diimplementasi ke dalam sebuah pengaturan proses (direncanakan, dimonitor, dan dievaluasi) dan produk kerja proses tersebut ditetapkan, dikontrol, dan dipertahankan secara tepat.

Level 3

Established process, yaitu proses pada level 2 diimplementasi menggunakan proses yang terdefinisi dan terdefinisi untuk mencapai hasil proses.mampu mencapai hasil proses.

Level 4

Predictable process, yaitu proses pada level 3 dijalankan dengan batasan yang telah terdefinisi untuk mencapai hasil proses.

Level 5

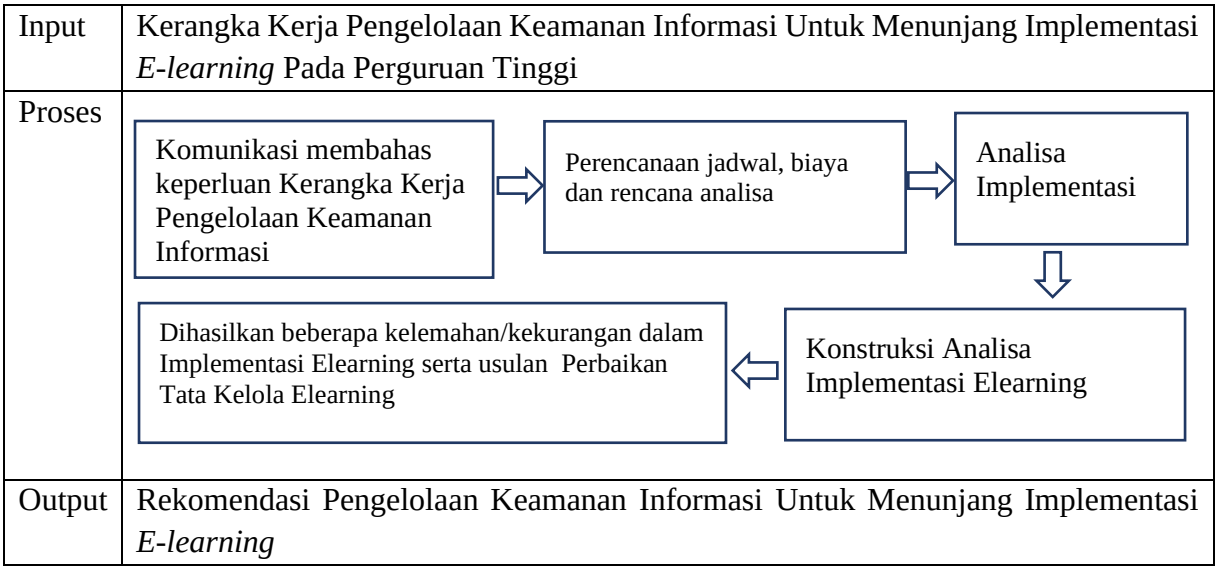
Optimizing process, yaitu proses pada level 4 ditingkatkan secara berkelanjutan untuk memenuhi tujuan organisasi saat ini dan saat mendatang (Putri, 2016).

3. Analisis Resiko

Analisis risiko digunakan untuk mengetahui risiko serta penyebab risiko, dalam analisis risiko melakukan penilaian risiko untuk menangani risiko tersebut. Berikut merupakan hal yang menjelaskan analisis risiko.

1. Rekomendasi Kontrol
2. Rekomendasi Kebijakan

Kerangka Pemikiran



Gambar 2. Kerangka Pemikiran

HASIL DAN PEMBAHASAN

Hasil

Aset yang dilihat dalam Implementasi *E-learning* yang dijadikan pendukung kerangka kerja pengelolaan keamanan informasi untuk menunjang implementasi *E-learning*. Untuk itu peneliti memberikan kuesioner dan wawancara kepada Direktur IT untuk mengetahui sejauhmana bagian utama dari kerangka kerja keamanan informasi telah dijalankan. Kuesioner yang diberikan adalah sebagai berikut:

1. **Aset Kebijakan**

   Apakah Perguruan Tinggi mempunyai sebuah kebijakan yang mengatur tentang tata kelola keamanan informasi pada implementasi *E-learning*?

   a) Belum ada
   b) Sudah ada kebijakan cuma belum dijalankan
   c) Sudah ada kebijakan namun baru dijalankn Sebagian
   d) Sudah ada kebijakan dan hampir seluruhnya dijalankan
   e) Sudah ada kebijakan dan 100% dijalankan

   Saran dari Direktur IT

   Harus segera dibuat SOP tentang / aturan keamanan informasi terkait dengan implementasi *E-learning*.

2. **Aset Kelembagaan**

   Apakah Perguruan Tinggi sudah mempunyai unit kerja yang mempunyai tugas dan fungsi pokok dalam pengelolaan *E-learning* khususnya untuk melaksanakan penyusunan dan pelaksanaan kebijakan teknis pelaksanaan,pemberian bimbingan, dan pengendalian di bidang data dan informasi.

   a) Belum ada
   b) Sudah ada unit kerja namun belum berjalan
   c) Sudah ada unit kerja namun baru menjalankan Sebagian tugas

d) Sudah ada unit kerja dan hampir seluruh tugas dan fungsi dijalankan
e) Sudah ada unit kerja dan menjalankan 100% tugas dan fungsinya

3. Aset Aplikasi

Apakah Perguruan Tinggi sudah mengembangkan berbagai sistem informasi dan aplikasi yang digunakan untuk melaksanakan tugas fungsi pokoknya dalam mendukung terciptanya Good Governance terkait implementasi *E-learning*?

a) Belum memiliki sistem informasi dan aplikasi
b) Sudah ada SI dan Aplikasi namun belum dikembangkan
c) Sudah mengembangkan sebagian kecil sistem informasi dan aplikasi
d) Sudah mengembangkan sebagian besar sistem informasi dan aplikasi
e) Sudah mengembangkan 100% sistem informasi dan aplikasi

4. Aset Infrastruktur

Apakah Perguruan Tinggi sudah memiliki data center yang pengelolaannya dilakukan oleh unit Pusat Data dan Informasi dan mempunyai tempat backup data dan aplikasi di lokasi yang berbeda.sebagai cadangan jika terjadi kejadian yang tidak diinginkan semisal bencana alam dan lain sebagainya.

a) Belum memiliki data center
b) Sudah memiliki data center namun belum dikelola oleh pusat data dan informasi
c) Sudah memiliki data center dan sudah dikelola sebagian
d) Sudah memiliki data center dan sudah dikelola sebagian besar
e) Sudah memiliki data center dan sudah dikelola 100%

Pembahasan

Berdasarkan kuesioner terkait masalah aset yang merupakan bagian utama dari kerangka kerja keamanan informasi maka pembahasannya adalah sebagai berikut:

1. Aset Kebijakan

Pertanyaan:

Apakah Perguruan Tinggi mempunyai sebuah kebijakan yang mengatur tentang tata kelola keamanan informasi pada implementasi *E-learning*?

Jawaban:

Belum ada

Catatan

Memang jawaban ini sepintas agak mengejutkan karena kebijakan yang mengatur tentang tata Kelola keamanan informasi pada implementasi belum ada, namun hal ini cukup beralasan karena Universitas XYZ dimana penelitian ini dilakukan baru berumur 2,5 tahun dan selama ini baru memusatkan perhatian utamanya pada pengurusan akreditasi setiap prodinya, sehingga aspek *E-learning* dari sisi aset kebijakannya belum dibuat namun karena situasi dan kondisi memaksa pelaksanaan atau implementasi harus dilakukan tanpa menunggu kebijakan selesai dibuat. Sehingga Direktur IT sudah mempunyai rencana untuk menyusun SOP terkait kebijakan mengenai keamanan informasi pada implementasi *E-learning*.

2. Aset Kelembagaan

Apakah Perguruan Tinggi sudah mempunyai unit kerja yang mempunyai tugas dan fungsi pokok dalam pengelolaan *E-learning* khususnya untuk melaksanakan penyusunan dan pelaksanaan kebijakan teknis pelaksanaan,pemberian bimbingan, dan pengendalian di bidang data dan informasi?

Jawaban:

Sudah ada unit kerja namun baru menjalankan Sebagian tugas

Catatan:

Unit kerja yang sudah dibentuk memang belum dapat menjalankan tugas dan fungsinya secara optimal karena keterbatasan jumlah SDM, terlebih lagi koordinator pengelola *E-learning* saat ini masih rangkap jabatan sebagai Sekprodi ditambah lagi yang bersangkutan melanjutkan kuliah S3 sehingga beban kerjanya cukup berat ditambah SDM yang ada hanya 1 orang Staf pengelola *E-learning*.

3. Aset Aplikasi

Apakah Perguruan Tinggi sudah mengembangkan berbagai sistem informasi dan aplikasi yang digunakan untuk melaksanakan tugas fungsi pokoknya dalam mendukung terciptanya Good Governance terkait implementasi *E-learning*?

Catatan:

Sudah mengembangkan sebagian kecil sistem informasi dan aplikasi

Pembahasan:

Berdasarkan penjelasan dari Direktur IT dikatakan bahwa divisi IT di perguruan tinggi ini telah mengembangkan sebagian kecil sistem informasi dan aplikasi yang sudah digunakan yaitu Sistem Informasi Akademik yang dikembangkan sehingga beberapa fitur tambahan yang dulunya belum ada sudah ditambahkan, dari sisi *E-learning* fitur video conference yang belum ada dibuat terintegrasi dengan google meet sehingga masalah waktu tatap muka yang sangat terbatas dengan menggunakan Zoom telah teratasi.

4. Aset Infrastruktur

Apakah Perguruan Tinggi sudah memiliki data center yang pengelolaannya dilakukan oleh unit Pusat Data dan Informasi dan mempunyai tempat backup data dan aplikasi di lokasi yang berbeda.sebagai cadangan jika terjadi kejadian yang tidak diinginkan semisal bencana alam dan lain sebagainya.

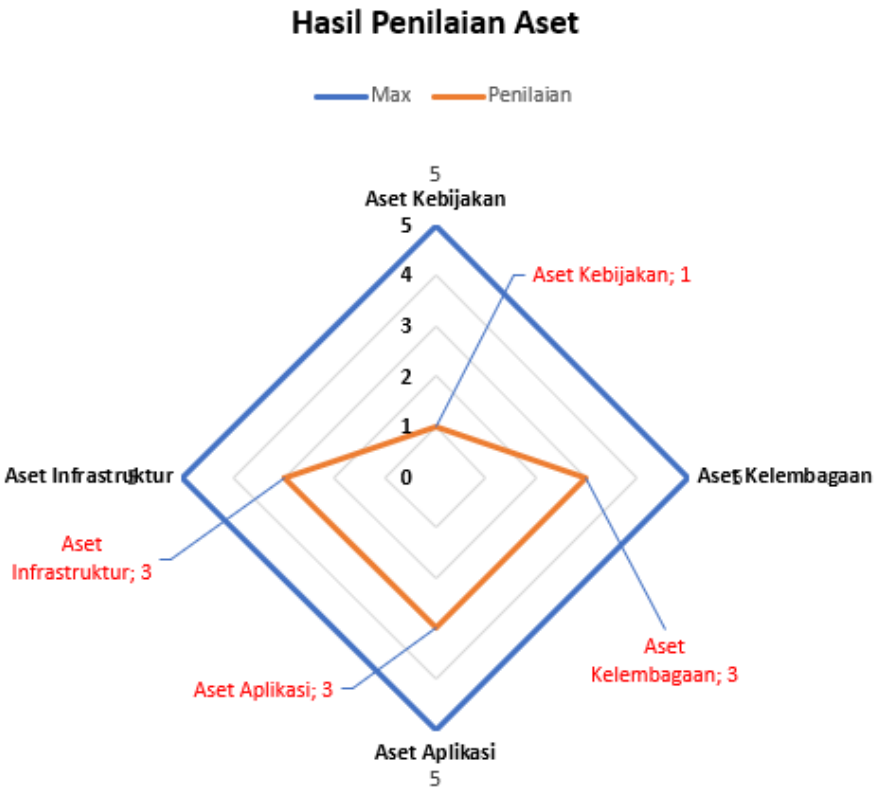
Jawaban:

Sudah memiliki data center dan sudah dikelola Sebagian

Catatan

Pengelolaan data center memang baru dilakukan sebagian karena memang jalannya operasional perguruan tinggi baru 2,5 tahun sehingga belum ada lulusan, karena jumlah mahasiswa akan mempengaruhi jumlah database yang harus dikelola apalagi jika nantinya sudah menghasilkan lulusan database berupa transkrip nilai dan ijazah tentu saja akan semakin menambah jumlah database yang harus disimpan,dikelola dan dijaga dengan baik sehingga keamanan informasi dapat lebih terjamin.

Penilaian Aset dalam diagram berdasarkan kuesioner yang telah diberikan kepada Direktur IT adalah sebagai berikut:



Gambar 3. Grafik Penilaian Aset

Berdasarkan grafik tersebut dapat dilihat bahwa aset kebijakan adalah yang paling rendah maka sesuai dengan saran dari Direktur IT maka harus segera dibuat SOP tentang / aturan keamanan informasi terkait dengan implementasi *E-learning*.

KESIMPULAN DAN SARAN

Kesimpulan

Setelah melihat hasil penilaian aset berdasarkan Kerangka Kerja Pengelolaan Keamanan Informasi maka dapat diketahui sisi kelemahan Pengelolaan Keamanan Informasi pada implementasi *E-learning* di Universitas XYZ ini sehingga perlu segera dilakukan perbaikan dari sisi aset kebijakan karena jika tidak maka akan ada resiko keamanan informasi yang nantinya berpotensi menganggu jalannya proses kegiatan pembelajaran melalui *E-learning*.

Saran

Berdasarkan penilaian terhadap 5 aset yang ada maka ditinjau dari sisi kerangka kerja keamanan inoformasi maka implementasi *E-learning* dari sisi keamanan informasi mempunyai titik lemah dari sudut aset kebijakan, karena dari data dan grafik jelas aset kebijakkan perlu diperbaiki agar implementasi *E-learning* dapat berjalan dengan lebih baik dan aman.

DAFTAR PUSTAKA

Analisis dan Perancangan Manajemen Keamanan Informasi Menggunakan Kerangka Kerja COBIT 5 di PT Pos Indonesia. (2021). Bandung, Jawa Barat, Indonesia: Universitas Telkom.

Basyarahil et al. (2017). *Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi ITS Surabaya.* Surabaya: Jurusan Sistem Informasi Fakultas Teknologi Informasi ITS.

Chazar, C. (2015). Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005. *Jurnal Informasi*, 48-57.

Dewi, A. C. (2017). Penyusunan Tata Kelola Keamanan Informasi Pada Produksi Film Animasi. *Prosiding SNATIF* (pp. 297-302). Fakultas Teknik-Universitas Muria Kudus.

Februariyanti, H. (2006). Standar dan Manajemen Keamanan Komputer. *Jurnal Teknologi Informasi DINAMIK*, 134-142.

Ibrahim et al. (2010). Kerangka Kerja Manajemen Keamanan Berdasar ISO 2700 Beserta Turunannya Untuk Sistem Pada E-Goverment. *Jurnal Computech & Bisnis*, 7-16.

Indrajit, R. E. (2014). *Manajemen Organisasi dan Tata Kelola Teknologi Informasi.* APTIKOM.

Lionie et al. (2021). Peluang dan Tantangan *E-learning* Bagi Mahasiswa dan Dosen di Era Pandemi Covid 19. *Jurnal Tera*, 109-122.

Septanto, H. (2015). *E-learning* Menggunakan Edmodo Sebuah Aplikasi Pembelajaran Berbasis Web Pada Kelas Shift di STMIK Bina Insani. *Bina Insani ICT Journal*, 127-141.

Syafrizal, M. (2007). ISO 17799:Standar Sistem Manajemen Keamanan Informasi. *Seminar Nasional Teknologi 2007* (pp. 1-10). Yogyakarta: STMIK AMIKOM.

Yustanti et al. (2019). Strategi Identifikasi Resiko Keamanan Informasi Dengan Kerangka Kerja ISO 27005:2018. *Journal Information Engineering and Educational Technology*, 51-55.

ISACA. (2012). Enabling Processes. In *Cobit 5*.

ISO/IEC. (2015). INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management for inter-sector and. *27003:2017*, *2015*, 1–45.

Informasi, D. K. (2011). *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik.*