TUGAS AKHIR - KS141501

EVALUASI KEAMANAN INFORMASI MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI) (STUDI KASUS: STIE PERBANAS SURABAYA)

RADHIFAN HIDAYAT
NRP 5211 100 177

Dosen Pembimbing
Dr. Apol Pribadi S., S.T., M.T.
Hanim Maria Astuti, S.Kom., M.Sc.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

FINAL PROJECT - KS141501

THE EVALUATION OF INFORMATION SECURITY USING INDEKS KEAMANAN INFORMASI (KAMI) (CASE STUDY: STIE PERBANAS SURABAYA)

RADHIFAN HIDAYAT
NRP 5211 100 177

Academic Promotors
Dr. Apol Pribadi S., S.T., M.T.
Hanim Maria Astuti, S.Kom., M.Sc.

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Institut Teknologi Sepuluh Nopember
Surabaya 2016

LEMBAR PENGESAHAN

EVALUASI KEAMANAN INFORMASI MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI) (STUDI KASUS: STIE PERBANAS SURABAYA)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:
RADHIFAN HIDAYAT
5211 100 177

Surabaya, Juli 2016

KETUA
JURUSAN SISTEM INFORMASI

Dr. Ir. Aris Tjahyanto, M.Kom
NIP 196503101991021001

LEMBAR PERSETUJUAN

EVALUASI KEAMANAN INFORMASI MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI) (STUDI KASUS: STIE PERBANAS SURABAYA)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :

RADHIFAN HIDAYAT
5211 100 177

Disetujui Tim Penguji : Tanggal Ujian : Juli 2016
Periode Wisuda : September 2016

Dr. Apol Pribadi S., S.T., M.T. **(Pembimbing 1)**

Hanim Maria Astuti, S.Kom., M.Sc. **(Pembimbing 2)**

Feby Artwodini, S.Kom., M.T. **(Penguji 1)**

Bekti Cahyo Hidayanto, S.Si., M.Kom. **(Penguji 2)**

EVALUASI KEAMANAN INFORMASI MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI) (STUDI KASUS: STIE PERBANAS SURABAYA)

Nama Mahasiswa : Radhifan Hidayat
NRP : 5211 100 177
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing 1 : Dr. Apol Pribadi S., S.T., M.T.
Dosen Pembimbing 2 : Hanim Maria A., S.Kom., M.Sc.

ABSTRAK

Sekolah Tinggi Ilmu Ekonomi Perbanas Surabaya atau STIE Perbanas Surabaya merupakan lembaga pendidikan dalam bidang bisnis dan perbankan di bawah naungan Perhimpunan Bank-Bank Umum Nasional (Perbanas) Jawa Timur, Didirikan pada tahun 1970. Perguruan tinggi merupakan satuan pendidikan formal yang mengemban misi mencari, menemukan dan menyebarluaskan kebenaran ilmiah melalui pendidikan dan pembelajaran, penelitian, serta pengabdian kepada masyarakat. Menurut UU. No. 12 Tahun 12 Ttg. Perguruan Tinggi, misi mencari, menemukan, dan menyebarluaskan kebenaran ilmiah tersebut dapat diwujudkan apabila perguruan tinggi di kelola berdasarkan suatu Tata kelola perguruan tinggi yang baik (Good University Governance). Pengelolaan Informasi merupakan salah satu aspek dalam Good University Governance, termasuk kualitas dan keamanan pengelolaan informasi.

Untuk meningkatkan kesadaran akan pentingnya keamanan informasi, sejak tahun 2008 Kementerian Kominfo telah menyelenggarakan sosialisasi kepada instansi penyelenggara pelayanan publik tentang metode atau cara melakukan penilaian terhadap status keamanan informasi

suatu instansi penyelenggara pelayanan publik dengan menggunakan alat bantu Indeks Keamanan Informasi (KAMI).

Indeks Keamanan Informasi (KAMI) adalah alat evaluasi yang dibuat oleh Kementerian Komunikasi dan Informatika untuk menganalisis tingkat kesiapan dan kematangan pengamanan informasi di instansi baik pemerintah ataupun non pemerintah yang telah disesuaikan dengan standar internasional, yaitu ISO 27001:2005. Alat evaluasi ini selanjutnya akan digunakan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi pada STIE Perbanas Surabaya.

Hasil penilaian tingkat ketergantungan TIK adalah sebesar 30 dari total keseluruhan 48, dan termasuk dalam kategori tinggi. Hasil penilaian kelima area yang telah dilakukan adalah sebesar 252 dari total keseluruhan 588. Dengan ketergantungan TIK yang tinggi tersebut penilaian kelima area masih termasuk ke dalam kategori tidak layak. Dan untuk mencapai status kesiapan baik minimal membutuhkan skor sebesar 393. Untuk itu akan dibuatkan suatu rekomendasi perbaikan pada bagian-bagian yang masih kurang dari hasil penilaian indeks KAMI yang telah dilakukan.

Kemudian rekomendasi dari penelitian ini dapat dijadikan sebagai bahan pertimbangan dan evaluasi bagi pihak STIE Perbanas Surabaya dalam melakukan perbaikan yang berkaitan dengan mitigasi atau pencegahan kerentanan keamanan informasi, serta memastikan regulasi dapat dicapai dengan baik dan kebijakan keamanan institusi di masa yang akan datang.

Kata Kunci: Evaluasi, Keamanan Informasi, Indeks KAMI, ISO 27001, Manage Security.

THE EVALUATION OF INFORMATION SECURITY USING INDEKS KEAMANAN INFORMASI (KAMI) (CASE STUDY: STIE PERBANAS SURABAYA)

Name	**: Radhifan Hidayat**
NRP	**: 5211 100 177**
Department	**: Sistem Informasi FTIF-ITS**
Supervisor 1	**: Dr. Apol Pribadi S., S.T., M.T.**
Supervisor 2	**: Hanim Maria A., S.Kom., M.Sc.**

ABSTRACT

STIE Perbanas Surabaya is an educational institution in the field of business and banking under the auspices of the Association of Commercial Banks (Perbanas) East Java, was established in 1970. The college is a unit of formal education with the mission of searching, finding and disseminate scientific truth through education and learning, research and community service. According to Act. No. 12 of 12 About Universities, the mission of searching, finding and disseminating scientific truth can be realized if the college is managed by a governance good college (Good University Governance). Information management is one aspect of the Good University Governance, including the quality and security information management.

To raise awareness of the importance of information security, since 2008 the Indonesian Ministry of Communications and Information Technology has provided outreach to providers of public services agencies on methods or how to evaluate the information security status of an institution of public service providers using the tools of the Information Security Index (KAMI).

Information Security Index (KAMI) is an evaluation tool created by the Ministry of Communications and Information

Technology to analyze the degree of readiness and maturity in information security agencies both government and non government that has been adapted to international standards, such as ISO 27001: 2005. This evaluation tool will then be used as a device to provide an overview of readiness condition (completeness and maturity) information security framework in STIE Perbanas Surabaya.

Results of assessment of the level of ICT dependence is 30 out of the total 48, and included in the high category. The results of the five areas that assessment has been carried out amounted to 252 out of the total 588. With such high dependence on ICT fifth assessment area still fall into the category is not feasible. And to achieve good status of preparedness requires a minimum score of 393. For that would be made a recommendation repairs on parts that are still less than the index of assessment results Information Security Index (KAMI) have done.

Then the recommendation from this study can be used as a material consideration and evaluation for the STIE Perbanas Surabaya in the improvement associated with mitigation or prevention of a security vulnerability information, and ensure the regulation can be achieved by both institutions and security policies in the future.

Keywords: Evaluation, Information Security, Information Security Index (KAMI), ISO 27001, Manage Security

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

Pada bab ini akan diuraikan proses indentifikasi masalah penelitian yang meliputi *Latar Belakang Masalah, Rumusan Masalah, Batasan Masalah, Tujuan Tugas Akhir, Manfaat Tugas Akhir, serta Relevansi dari Penelitian*. Berdasarkan uraian pada bab ini, harapannya gambaran umum permasalahan dan pemecahan masalah pada tugas akhir ini dapat dipahami.

1.1. Latar Belakang

Teknologi Informasi dan Komunikasi telah mengalami perkembangan yang sangat hebat. Hadirnya internet berhasil menembus hambatan geografis, batasan negara, ras, adat, dll. Pada era pendidikan tinggi sekarang ini khususnya universitas perkiraan jumlah pengguna internet di Indonesia per 8 Mei 2014 mendekati 82 juta pengguna [1].

Implementasi TI di lembaga pendidikan sudah menjadi hal yang umum. Implementasi tersebut ditujukan untuk membantu berbagai fungsi dalam menjalankan aktivitas belajar mengajar secara optimal, namun dari sekian banyak organisasi yang menerapkan TI penerapan tata kelola TI secara efektif masih sangat sedikit terutama di institusi pendidikan tinggi.

Informasi merupakan salah satu aset yang sangat berharga bagi suatu intitusi perguruan tinggi. Pengelolaan informasi yang baik, akan menjadikan perguruan tinggi memiliki kemampuan manajerial yang baik serta meningkatkan daya saing perguruan tinggi tersebut. Pengamanan Informasi secara teori pada dasarnya ditujukan untuk menjamin integritas informasi, pengamanan kerahasiaan data, ketersediaan informasi, dan pemastian memenuhi peraturan, ataupun hukum yang berlaku.

Di Indonesia sendiri *Dasar Hukum Penerapan Tata Kelola Keamanan Informasi, Undang-undang No. 11 Tahun 2008 Pasal 15 ayat 1* menyatakan bahwa: “Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. [2]”

Kemudian tercantum juga *Peraturan Pemerintah No. 82 Tahun 2012 pasal 14 ayat 1*, bahwa: “Penyelenggara Sistem Elektronik wajib memiliki kebijakan tata kelola, prosedur kerja pengoperasian, dan mekanisme audit yang dilakukan berkala terhadap Sistem Elektronik. [3]”

Untuk meningkatkan kesadaran akan pentingnya keamanan informasi, sejak tahun 2008 Kementerian Kominfo telah menyelenggarakan sosialisasi dalam bentuk seminar dan bimbingan teknis (bimtek) kepada instansi penyelenggara pelayanan publik, baik di lingkungan pemerintah pusat maupun daerah. Direktorat Keamanan Informasi Kementerian Kominfo telah menyusun metode atau cara melakukan penilaian mandiri (self assessment) terhadap status keamanan informasi suatu instansi penyelenggara pelayanan publik dengan menggunakan alat bantu Indeks Keamanan Informasi [4].

Indeks Keamanan Informasi atau disingkat indeks KAMI merupakan alat evaluasi berbasis SNI-ISO/IEC 27001:2009 untuk menganalisis tingkat kesiapan pengamanan informasi nasional di instansi-instansi baik pemerintah ataupun non pemerintah. Alat evaluasi ini ditujukan sebagai sarana untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi pada suatu instansi. [5].

Berdasarkan hal tersebut, maka dipandang perlu untuk mengamankan informasi yang dimiliki, terutama dalam dunia pendidikan yang menjunjung nilai luhur, dan untuk

mewujudkan hal tersebut maka terlebih dahulu perlu dilakukan evaluasi atas keamanan informasi dengan menggunakan indeks KAMI pada STIE Perbanas Surabaya untuk mengetahui bagaimana gambaran terkini dari keamanan informasi itu sendiri yang setelahnya dilanjutkan dengan pembuatan rekomendasi perbaikan terhadap keamanan informasi dengan harapan rekomendasi yang telah dibuat dapat digunakan sebagai bahan pertimbangan dalam meningkatkan kualitas keamanan informasi di STIE Perbanas Surabaya agar senantiasa dapat memberikan pelayanan yang lebih baik kedepannya dan dalam memastikan pemanfaatan yang efektif dari sumber daya Teknologi Informasi (TI) dan meminimalkan terjadinya kerugian atau insiden karena penyalahgunaan terhadap peralatan atau sistem yang tersedia baik secara sengaja maupun tidak disengaja.

1.2. Perumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan, rumusan masalah yang menjadi fokus dan akan diselesaikan dalam tugas akhir ini, yaitu:

1. Berapa nilai kematangan, kelengkapan dan pengelolaan keamanan informasi pada STIE Perbanas Surabaya?
2. Bagaimana rekomendasi pada STIE Perbanas Surabaya berdasarkan dari hasil evaluasi Indeks KAMI?

1.3. Batasan Masalah

Batasan masalah dalam tugas akhir ini meliputi beberapa hal dan digunakan untuk membantu memperjelas pengerjaan penelitian, diantarannya adalah:

1. Penilaian yang dilakukan menggunakan standar penilaian Indeks Keamanan Informasi (KAMI) Versi 2.2, 19 April 2012 dari Kementerian Kominfo.
2. Penilaian keamanan informasi meliputi tingkat kematangan dalam penerapan pengelolaan keamanan informasi.
3. Lingkup penilaian hanya pada pengelolaan keamanan informasi pada STIE Perbanas Surabaya.

1.4. Tujuan Tugas Akhir

Berdasarkan rumusan masalah yang akan diselesaikan dalam tugas akhir ini, berikut merupakan tujuan penelitian yang diharapkan:

1. Menganalisa pengelolaan teknologi informasi yang sedang berjalan di STIE Perbanas Surabaya.
2. Mendapatkan hasil penilaian mengenai pengelolaan keamanan TI pada STIE Perbanas Surabaya.
3. Mengetahui tingkat kematangan pengelolaan keamanan teknologi informasi pada STIE Perbanas Surabaya.
4. Memberikan rekomendasi dalam rangka meningkatkan kualitas pengelolaan keamanan informasi pada STIE Perbanas Surabaya.

1.5. Manfaat Tugas Akhir

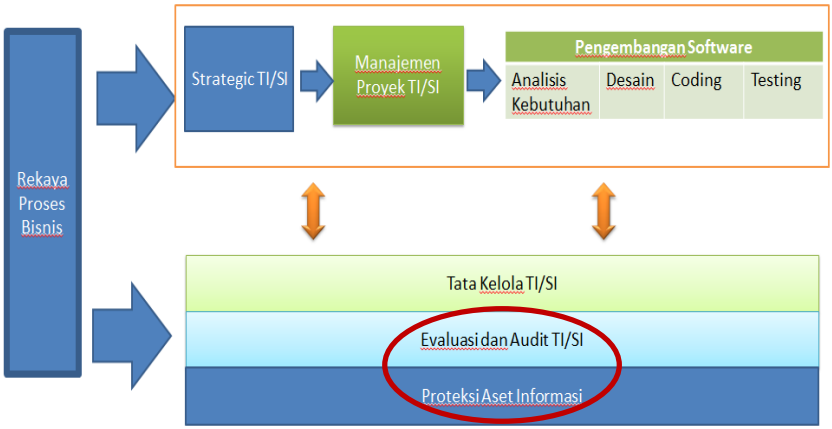
Manfaat yang diharapkan dari pembuatan tugas akhir ini meliputi beberapa hal, diantarannya adalah:

1. Memberikan *output* berupa hasil penilaian mengenai tingkat keamanan pengelolaan TI serta hasil dari penilaian tersebut dapat memberikan gambaran atas kesiapan dan kelengkapan dalam keamanan informasi pada STIE Perbanas Surabaya.
2. Memberikan *output* berupa evaluasi pengukuran tingkat kematangan pengelolaan keamanan yang dapat membantu STIE Perbanas Surabaya untuk mengetahui tingkat kesiapan dan kelengkapan terhadap keamanan informasi yang kemudian dapat membantu melakukan tindak lanjut dalam menentukan kebijakan kedepannya.

1.6. Relevansi Tugas Akhir

Relevansi atau keterkaitan dari hasil penelitian terhadap keilmuan di Jurusan Sistem Informasi ITS adalah:

1. Mata kuliah yang membahas tentang mengevaluasi kinerja adalah PKETI (Pengukuran Kinerja & Evaluasi TI) dan mata kuliah KAI (Keamanan Aset Informasi) membahas tentang keamanan informasi.
2. Laboratorium untuk penelitian ini adalah Manajemen Sistem Informasi (MSI), karena penelitian masuk dalam lingkup MSI. Berikut ini merupakan *road map* penelitian pada Lab MSI, Jurusan Sistem Informasi ITS:



Gambar 1.1 Relevansi Penelitian

BAB II
TINJAUAN PUSTAKA

Bab ini akan menjelaskan mengenai penelitian sebelumnya dan dasar teori yang dijadikan acuan atau landasan dalam pengerjaan tugas akhir ini. Landasan teori akan memberikan gambaran secara umum dari landasan penjabaran tugas akhir ini.

2.1. Penelitian Sebelumnya

Berikut ini merupakan beberapa penelitian yang pernah dilakukan untuk membuat arsitketur sistem informasi:

1. Penelitian oleh Afrianto, Suryana, Sufa'atin (2015)

Tabel 2.1 Penelitian oleh Afrianto, Suryana, Sufa'atin

No	Aspek	Keterangan
1.	Judul	Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009 (Studi Kasus: Perguruan Tinggi X)
2.	Nama Peneliti	Irawan Afrianto, Taryana Suryana, Sufa'atin
3.	Metode	Analisis Indeks KAMI
4.	Tujuan Penelitian	Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI Pada Tata Kelola Keamanan Informasi di PT.X.
6.	Ulasan Penelitian	Analisis Indeks KAMI digunakan untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang ada didalam lingkungan organisasi/institusi.

No	Aspek	Keterangan
7.	Hasil Yang Didapatkan	Hasil pengukuran keamanan informasi menggunakan indeks KAMI untuk PT. X menunjukkan tingkat kematangan keamanan informasi I s/d II. Sementara untuk mendapatkan kesiapan sertifikasi ISO/IEC 27001:2009, tingkat kematangna keamanan informasi minimal berada pada level III (Terdefinisi dan Konsisten).

2. Penelitian oleh Endi Lastyono Putra (2014)

Tabel 2.2 Penelitian oleh Endi Lastyono Putra

No	Aspek	Keterangan
1.	Judul	Evaluasi Keamanan Informasi Pada Divisi Network Of Broadband Pt. Telekomunikasi Indonesia Tbk Dengan Menggunakan Indeks Keamanan Informasi (KAMI)
2.	Nama Peneliti	Endi Lastyono Putra
3.	Metode	Analisis Indeks KAMI
4.	Tujuan Penelitian	Mengukur tingkat kematangan pengelolaan keamanan TI pada Divisi Network Of Broadband Pt. Telekomunikasi Indonesia Tbk.
5.	Ulasan Penelitian	Analisis Indeks KAMI digunakan untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang ada didalam lingkungan organisasi/institusi.

No	Aspek	Keterangan
6.	Hasil Yang Didapatkan	Hasil dari penelitian ini adalah penilaian kelima area menunjukkan nilai sebesar 582, dengan hasil nilai tingkat kepentingan TIK sebesar 44 maka divisi Network pf Broadband PT. Telekomunikasi Indonsia Tbk. Sudah dapat dikatakan matang dan sesuai dengan standart ISO 27001.

3. Penelitian oleh Luthfiya Ulinnuha (2013)

Tabel 2.3 Penelitian oleh Luthfiya Ulinnuha

No	Aspek	Keterangan
1.	Judul	Evaluasi Pengelolaan Keamanan Jaringan Di ITS Dengan Menggunakan Standar Indeks Keamanan Informasi (KAMI) Kemenkominfo RI
2.	Nama Peneliti	Luthfiya Ulinnuha
3.	Metode	Analisis Indeks KAMI
4.	Tujuan Penelitian	Melakukan evaluasi pengelolaan keamanan jaringan di ITS
5.	Ulasan Penelitian	Analisis Indeks KAMI digunakan untuk mendapatkan gambaran mengenai evaluasi keamanan jaringan yang ada didalam lingkungan institusi dan aspek kepatuhan terhadap ISO 27001.

No	Aspek	Keterangan
6.	Hasil Yang Didapatkan	Penilaian menunjukkan nilai sebesar 401 (dari nilai maksimum 588), dengan hasil nilai tingkat kepentingan TIK sebesar 29 (dari 48) lumayan tergolong tinggi namun masih perlu perbaikan untuk kelengkapan perangkat keamanan kelima area.

2.2. Dasar Teori

Pada bagian ini dipaparkan beberapa teori yang digunakan dalam pengerjaan tugas akhir.

2.2.1. Evaluasi

Kata evaluasi merupakan kata serapan dari bahasa Inggris yaitu “evaluation” yang berarti penilaian atau penaksiran.

Evaluasi adalah tahapan proses yang direncanakan untuk memperoleh penyediaan informasi yang sangat diperlukan untuk membuat alternatif-alternatif keputusan [6]. Menurut pendapat lain evaluasi juga dilakukan untuk untuk mengetahui/menguji apakah suatu kegiatan, proses kegiatan, keluaran suatu program telah sesuai dengan tujuan atau kriteria yang telah ditentukan [7].

Kemudian evaluasi juga berkutat tentang sejauh mana suatu kegiatan tertentu telah dicapai, bagaimana perbedaan pencapaian itu dengan suatu standar tertentu untuk mengetahui apakah ada selisih di antara keduanya, serta bagaimana manfaat yang telah dikerjakan itu bila dibandingkan dengan harapan-harapan yang ingin diperoleh [8].

2.2.2. Keamanan Informasi

Keamanan informasi merupakan sebuah bentuk perlindungan informasi dan unsur-unsur penting, termasuk sistem dan perangkat keras, penggunaan, penyimpanan, dan pengiriman informasi. Untuk dapat melakukan perlindungan diperlukan beberapa alat kerja seperti kebijakan, kesadaran, pelatihan, pendidikan, serta teknologi. Sedangkan konsep keamanan informasi menurut ISO adalah suatu upaya untuk melindungi aset informasi yang dimiliki organisasi atau perusahaan. Hal ini bertujuan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dimasa datang dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis [9].

Konsep kunci keamanan informasi merupakan sebuah nilai pedoman atau kunci karakteristik dalam melakukan penilaian terhadap keamanan informasi di sebuah organisasi atau perusahaan. The C.I.A Tringle yang merupakan dasar dari model CNSS (Committe On National Security System) di Amerika, mengumumkan adanya standar karakteristik keamanan informasi menjadi delapan konsep yaitu [10]:

- *Confidentiality*
  Karakteristik ini merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses informasi.
- *Integrity*
  Karakteristik tentang keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.
- *Avaibility*
  Menjamin pengguna yang valid selalu bisa mengakses informasi dan sumber daya miliknya sendiri. Untuk memastikan bahwa orang-orang yang memang berhak

tidak ditolak untuk mengakses informasi yang memang menjadi haknya.

- *Privacy*
  Karakteristik ini merupakan bentuk dari perlindungan penggunaan informasi yang dikumpulkan, diproses dan digunakan dalam sebuah organisasi sesuai dengan pemilik dari informasi tersebut.
- *Identification*
  Karakteristik ini memungkinkan sebuah sistem informasi memiliki karakteristik identifikasi dan mampu mengenali pengguna individu yang menggunakan informasi tersebut.
- *Authentication*
  Merupakan sebuah karakteristik keamanan informasi agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi.
- *Authorization*
  Merupakan karakteristik informasi yang berada pada sistem jaringan agar informasi tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
- *Accountability*
  Merupakan karakteristik dari informasi yang telah ada dimana terdapat kontrol penjaminan informasi yang ada (akuntabel).

2.2.3. Indeks Keamanan Informasi (KAMI)

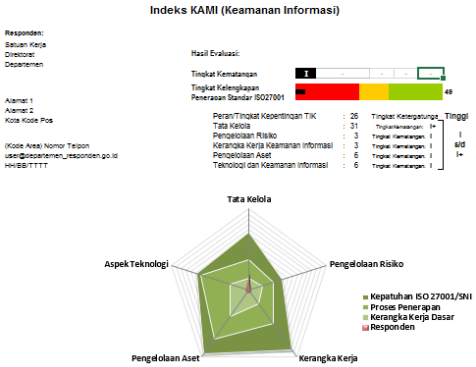
Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan

keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2009 [11].

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh Instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan *gambaran* indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Penilaian dapat dilakukan secara berkala sesuai dengan kebutuhan masing-masing institusi yang menerapkan. Wakil dari perusahaan akan menjawab pertanyaan yang diberikan dalam indeks KAMI dengan memilih status penerapan, yaitu:

a. Tidak Dilakukan
b. Dalam Perencanaan
c. Dalam Penerapan / Diterapkan Sebagian
d. Diterapkan Secara Menyeluruh



Gambar 2.1 Dashboard Indeks KAMI

Dashboard dari Indeks KAMI itu sendiri berisi nilai-nilai total dari setiap area yang ada di dalam Indeks KAMI dan memvisualisasikan nilai-nilai total tersebut dalam bentuk diagram radar dan diagram bar yang menunjukkan seberapa besar kematangan keamanan informasi tersebut.

Walau pengukuran tingkat kematangan dan kelengkapan keamanan informasi (melalui indeks KAMI) dalam penerapan SNI ISO/IEC 27001 ditujukan untuk instansi pemerintah, alat bantu tersebut juga dapat diterapkan pada perusahaan yang memberikan layanan kepada konsumen dalam skala besar. Dengan demikian usaha institusi dalam meningkatkan keamanan informasi dapat diukur dan terus diperbaiki sehingga mencapai suatu target yang diinginkan oleh intitusi sesuai dengan kebutuhannya masing-masing.

Dengan menggunakan indeks KAMI yang dilakukan secara berulang, maka suatu institusi dapat melakukan hal sebagai berikut:

- Memantau langkah pembenahan atau peningkatan tingkat kelengkapan tata kelola keamanan informasi.
- Mengevaluasi kesesuaian tata kelola keamanan setelah terjadinya perubahan yang signifikan dalam infrastruktur ataupun organisasi kerja yang ada dalam cakupan evaluasi.
- Memastikan diterapkannya tata kelola keamanan informasi yang sesuai.
- Sebagai bentuk pelaporan pelaksanaan tata kelola keamanan informasi kepada pimpinan.

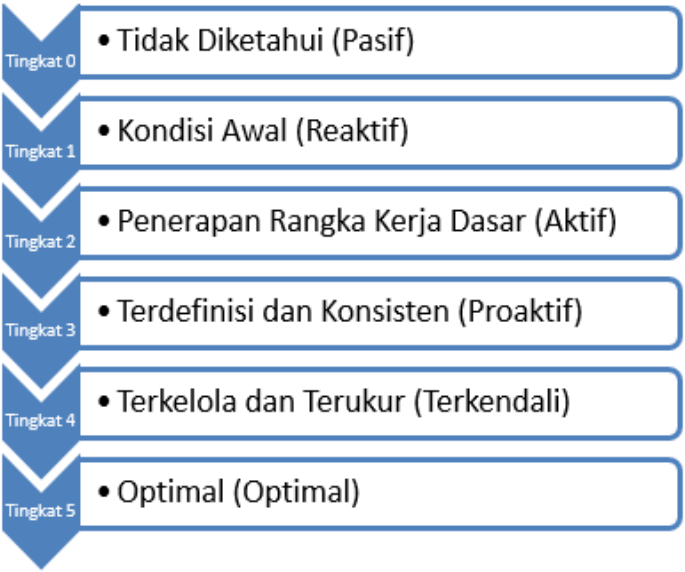
2.2.3.1. 5 Area Evaluasi Indeks KAMI

Indeks KAMI membantu institusi dalam melihat dan menilai tingkat kematangan penerapan SNI ISO/IEC 27001:2009. Indeks KAMI mengevaluasi 5 area penting yang meliputi:

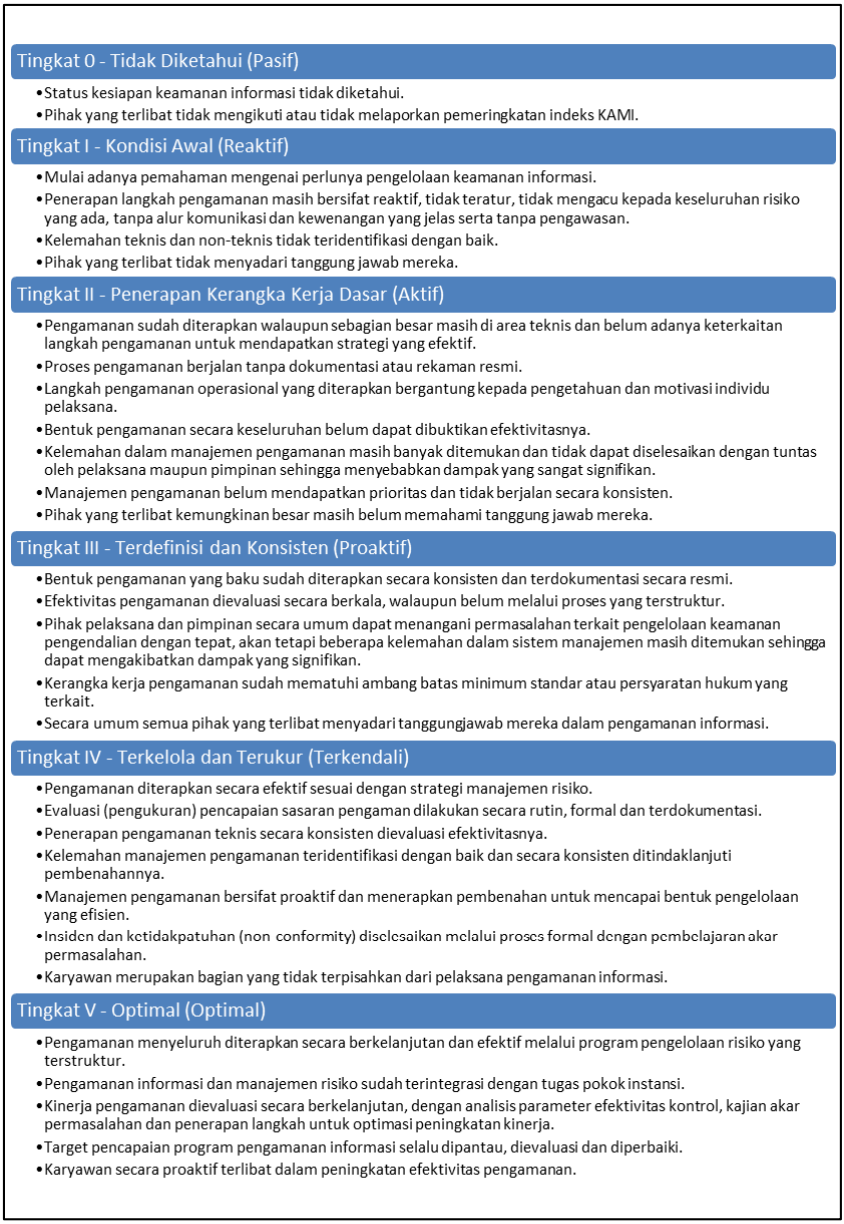
- *Tata Kelola Keamanan Informasi*
  Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
- *Manajemen Keamanan Informasi*
  Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi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

2.2.3.2. Tingkat Kematangan Indeks KAMI

Tingkat kematangan yang digunakan dalam Indeks KAMI dibagi dalam 6 tingkat, yaitu:



Gambar 2.2 Tingkat Kematangan Indeks KAMI



Gambar 2.3 Deskripsi Tingkat Keamanan Indeks KAMI

2.2.4. Pengelolaan TI *(IT Governance)*

Secara umum kinerja merupakan hasil kerja suatu organisasi dalam rangka mewujudkan tujuan strategis yang ditetapkan organisasi, kepuasan pelanggan, serta kontribusinya terhadap perkembangan ekonomi masyarakat. Teknologi Informasi (TI) memiliki peranan penting bagi perusahaan sebagai salah satu faktor dalam mencapai tujuan perusahaan. Peran TI akan optimal jika penerapan TI dikelola dengan baik. Pengelolaan yang baik dapat dipastikan dengan menilai kesesuaian antara penerapan TI dengan kebutuhan bisnis perusahaan. Selain itu, pengelolaan TI yang baik harus disertai dengan pengidentifikasian resiko-resiko dari penerapan IT dan penanganan dari resiko-resiko tersebut. Untuk mewujudkan kedua hal tersebut, kita dapat menerapkan pengelolan teknologi informasi (IT Governance) [12].

IT governance merupakan suatu struktur dan proses yang saling berhubungan serta mengarahkan dan mengendalikan perusahaan dalam pencapaian tujuan melalui nilai tambah dan penyeimbangan antara resiko dan manfaat dari TI serta prosesnya. IT Governance adalah sebuah kerangka kebijakan, prosedur dan kumpulan proses-proses yang bertujuan untuk mengarahkan dan mengendalikan perusahaan dalam rangka pencapaian tujuan perusahaan dengan memberikan tambahan nilai bisnis, melalui penyeimbangan keuntungan dan resiko IT beserta proses-proses yang ada di dalamnya [13].

Suatu organisasi dapat dianggap sukses membangun TI dalam suatu kerangka sistem informasi yang lengkap bila telah memenuhi kriteria ukuran informasi (efektifitas, efisiensi, kerahasiaan, integritas, ketersediaan, pemenuhan, keandalan), mencakup sumber daya TI (orang, aplikasi, teknologi, fasilitas dan data) untuk memberikan dukungan penuh pada sasaran bisnis perusahaan.

2.2.5. *Information Security Management System*

Menurut McLeod Informasi didefinisikan sebagai data yang sudah diproses ataupun data yang memiliki arti. Informasi dibentuk dari gabungan data yang diharapkan memiliki arti untuk penerima. Menurut ISO/IEC 17799:2005 mengenai information security management system menjelaskan keamanan informasi merupakan upaya untuk melindungi dari berbagai ancaman untuk memastikan kelanjutan bisnis, mengurangi resiko bisnis, serta meningkatkan investasi dan peluang bisnis yang ada.

International Organization for Standardization (ISO) atau yang biasa disebut sebagai Organisasi International untuk Standarisasi sudah membuat dan mengembangkan sejumlah standar mengenai Information Security Management Systems (ISMS) atau yang disebut Sistem Manajemen Keamanan Informasi (SMKI) mulai berupa persyaratan hingga panduan sejak tahun 2005. Secara umum, arti dari sebuah Sistem Manajemen Keamanan Informasi adalah sebuah prosedur yang ada dalam memanajemen keamanan informasi dengan tujuan agar terhindar dari berbagai resiko negatif.

ISMS Dikelompokkan sebagai seri / rangkaian dari ISO 27000, berikut ini adalah pembagian kelompok dari standar ISMS [14]:

- ISO/IEC 27000:2009 – ISMS Overview and Vocabulary
- ISO/IEC 27001:2005 – ISMS Requirements
- ISO/IEC 27002:2005– Code of Practice for ISMS
- ISO/IEC 27003:2010 – ISMS Implementation Guidance
- ISO/IEC 27004:2009 – ISMS Measurements
- ISO/IEC 27005:2008 – Information Security Risk Management

- ISO/IEC 27006: 2007 – ISMS Certification Body Requirements
- ISO/IEC 27007 – Guidelines for ISMS Auditing

2.2.6. ISO/IEC 27001: 2005

ISO/IEC 27001: 2005 merupakan suatu standar internasional yang mencakup keamanan informasi yang dikembangkan oleh International Standarization for Organization (ISO) dan International Electrotecnical Comission (IEC). ISO/IEC 27001 menyediakan kerangka kerja dalam penggunaan teknologi dan manajemen sistem pengelolaan yang membantu suatu organisasi memastikan keamanan informasi sudah efektif. Hal ini termasuk kemampuan akses data secara berkelanjutan, kerahasiaan, dan integritas atas informasi yang dimilikinya [9]. ISO/IEC 27001 dapat digunakan pada setiap organisasi untuk mencegah kesalahan dalam penggunaan, kerusakan, atau hilangnya data bisnis yang dapat berdampak merugikan pada aktifitas bisnis utama perusahaan. Pemanfaatan ISO/IEC 27001 digunakan untuk berbagai keperluan, antara lain sebagai berikut:

- Sebagai penduan untuk merumuskan tujuan dan kebutuhan keamanan di sebuah organisasi
- Sebagai alat untuk memastikan bahwa risiko-risiko keamanan yang ada telah tertangani dengan efektif
- Sebagai alat untuk memastikan bahwa standar keamanan yang digunakan oleh perusahaan telah mematuhi hukum dan perundang-undangan
- Sebagai alat untuk menentukan status manajemen keamanan informasi pada sebuah organisasi
- Sebagai panduan bagi auditor, baik internal maupun eksternal untuk menentukan kesesuaian antara SMKI yang ada dengan kebijakan, arahan, dan standar yang diacu oleh organisasi

- Sebagai panduan implementasi keamanan informasi dalam berbisnis

Struktur organisasi ISO/IEC 27001 dibagi ke dalam dua bagian besar yaitu :

1. Klausul : Mandatory Process
   Klausul (pasal) adalah persyaratan yang harus dipenuhi jika organisasi menerapkan SMKI dengan menggunakan ISO/IEC 27001.

2. Annex A: Security Control
   Annex A adalah dokumen referensi yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol keamanan (security control) yang perlu diimplementasikan dalam SMKI, yang terdiri dari 11 klausul kontrol keamanan, 39 kontrol objektif, dan 133 kontrol.

   Kemudian dalam kerangka kerja ISO/IEC 27001 terdapat model PLAN-DO-CHECK-ACT (PDCA) yang diterapkan pada keseluruhan proses Information Security Management Systems atau Sistem Manajemen Keamanan Informasi (SMKI) seperti berikut ini:

   - PLAN (Menetapkan SMKI)
     Menetapkan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi agar memberikan hasil sesuai dengan keseluruhan kebijakan dan sasaran.

   - DO (Menerapkan dan mengoperasikan SMKI)
     Menerapkan dan mengoperasikan kebijakan SMKI, kontrol, proses dan prosedur-prosedur.

- CHECK (Memantau dan meninjau ulang SMKI)
  Mengkaji dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau efektivitasnya.

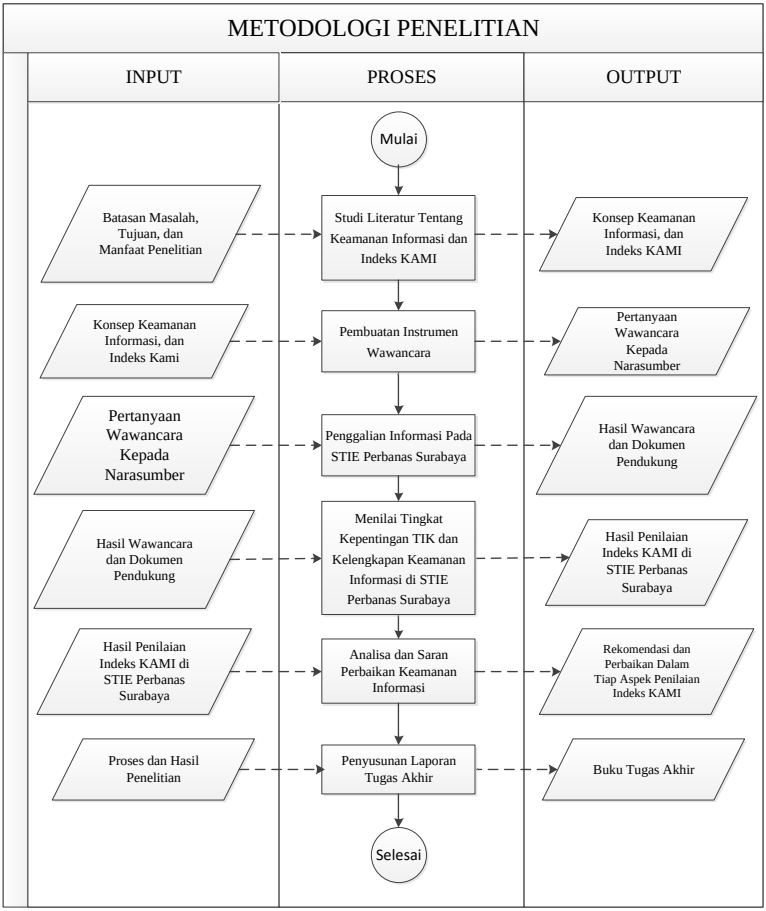
- ACT (Memelihara dan meningkatkan SMKI)
  Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasil evaluasi, audit internal dan tinjauan manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatan yang berkelanjutan.

Aktivitas utama diatas memiliki detail aktivitas secara teknis dalam mengelola sasaran kontrol pada standar ini dimana ukuran kontrol keamanan informasi meliputi berbagai area keamanan informasi sebagai berikut :

1. Kebijakan Keamanan Informasi (*Security Policy*)
2. Organisasi Keamanan Informasi (*Organizational of Information Security*)
3. Manajemen Aset (*Asset Management*)
4. Keamanan Sumber Daya Manusia (*Human Resources Security*)
5. Keamanan Fisik dan Lingkungan (*Physical and Environtment Security*)
6. Komunikasi dan Manajemen Operasi (*Communication and Operation Management*)
7. Akses Kontrol (*Access Kontrol*)
8. Pengadaan/akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi (*Information Systems Acquisitions, Development and Maintenance*)
9. Pengelolaan Insiden Keamanan Informasi (*Information Security Incident Management*)
10. Manajemen Kelangsungan Usaha (*Business Continuity Management*)
11. Kesesuaian (*Compliance*)

BAB III
METODOLOGI PENELITIAN

Bab ini menggambarkan metodologi yang akan digunakan sekaligus berisi gambaran rencana pengerjaan dan uraian. Berikut ini merupakan metodologi pengerjaan yang akan digunakan selama penelitian berlangsung:



Gambar 3.1 Alur Metodologi Penelitian

3.1. Studi Literatur

Merupakan tahap awal, yaitu dilakukan pengumpulan untuk mencari tahu literatur atau sumber yang berkaitan dengan permasalahan yang dihadapi, baik itu diambil dari sejumlah paper, jurnal, serta sumber lain yang ada di Internet. Beberapa hal yang dipelajari adalah teori dari beberapa pakar mengenai keamanan informasi itu sendiri, seputar metode Indeks KAMI, serta penelitian terdahulu yang pernah dilakukan. Dengan adanya studi literatur pula penulis dapat memahami dengan lebih jelas topik yang menjadi fokus penelitian.

3.2. Pembuatan Instrumen Wawancara

Merupakan tahap inisiasi sebelum melakukan pengambilan data dan terjun langsung ke lapangan, terlebih dahulu dibuat pedoman (*guideline)* untuk membantu dan mempermudah peneliti dalam melakukan pengambilan data sesuai dengan karakteristik yang dimiliki oleh Indeks KAMI itu sendiri. Pedoman yang dimaksud nantinya mengandung bahan-bahan wawancara, maupun keterangan *checklist* yang dilaksanakan dengan tanya jawab baik secara lisan, sepihak, dengan arah serta tujuan yang telah ditentukan.

3.3. Penggalian Informasi Pada STIE Perbanas Surabaya

Pada tahap ini dilakukan pengamatan dan pengumpulan data secara langsung berdasarkan teori pada objek studi kasus yang merupakan Departemen TIK STIE Perbanas Surabaya. Nantinya data akan berupa hasil wawancara dan dokumen pendukung lainnya yang terkait dalam 5 Area Indeks KAMI.

Pengambilan data bertujuan untuk mengetahui keadaan di STIE Perbanas Surabaya. Hasil pengambilan data akan menjadi bahan pertimbangan dalam perhitungan menggunakan

metode Indeks KAMI. Beberapa teknik pengambilan data akan dilakukan diantaranya sebagai berikut:

1. **Wawancara**
   Wawancara merupakan teknik pengambilan data atau informasi dengan cara memberikan pertanyaan secara langsung kepada pihak atau narasumber yang telah ditentukan. Pada studi kasus ini narasumber adalah *Kepala Seksi* di *Departemen TIK STIE Perbanas Surabaya.* Wawancara yang dilakukan bertujuan untuk menggali informasi terkait tentang tingkat kesiapan dan efektifitas pengamanan informasi sesuai dengan kriteria penilaian dalam metode Indeks KAMI.

2. **Observasi**
   Teknik Observasi merupakan salah satu upaya yang dilakukan dalam mengidentifikasi dan mengamati secara langsung keadaan yang sebenarnya terjadi (situasi, kondisi) di *STIE Perbanas Surabaya*. Tipe objek yang akan diamati dalam observasi dapat berupa ruang dalam aspek fisiknya, seperangkat kegiatan (aktivitas), benda (objek), tindakan, rangkaian aktivitas (event), tujuan yang ingin dicapai (struktur organisasi, rencana strategis, dll.). Observasi itu sendiri nantinya akan dilakukan secara terstruktur dan sesuai dengan kebutuhan dari pembuktian (validitas) wawancara yang telah dilakukan.

3. **Review Dokumen**
   Review dokumen akan dilakukan terhadap dokumen-dokumen pendukung yang dibutuhkan terkait dengan elemen wawancara. Nantinya akan dilakukan peninjauan atau menganalisis kembali dokumen guna melihat apakah dokumen yang dibutuhkan memenuhi syarat atau telah benar sebagaimana mestinya. Dokumen yang dimaksud dapat berupa dokumen Kebijakan, Pedoman, Prosedur, Standar, Instruksi Kerja dsb.

3.4. Menilai Tingkat Kepentingan & Kesiapan TIK

3.4.1. Menilai Tingkat Kepentingan TIK

Tahap ini merupakan langkah awal yang dilakukan untuk melakukan penilaian menggunakan indeks KAMI yaitu dengan melakukan klasifikasi terlebih dahulu terhadap peran TIK di STIE Perbanas. Pengelompokan digunakan untuk menilai peran TIK dalam instansi tersebut kedalam ukuran tertentu yaitu minim, rendah, sedang, tinggi, dan kritis. Dari hasil pengelompokan tersebut akan di dapat gambaran umum peran TIK di STIE Perbanas. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik kepentingan TIK yang sama. Kategori Peran TIK yang dimaksud adalah sebagai berikut:

- Minim
  Penggunaan TIK dalam lingkup yang didefinisikan tidak signifikan, dan keberadaannya tidak berpengaruh proses kerja yang berjalan.
- Rendah
  Penggunaan TIK mendukung proses kerja yang berjalan, walaupun tidak pada tingkatan yang signifikan.
- Sedang
  Penggunaan TIK merupakan bagian dari proses kerja yang berjalan, akan tetapi ketergantungannya masih terbatas.
- Tinggi
  TIK merupakan bagian yang tidak terpisahkan dari proses kerja yang berjalan.
- Kritis
  Penggunaan TIK merupakan satu-satunya cara untuk menjalankan proses kerja yang bersifat strategis atau berskala nasional.

Tabel 3.1 Interval Skor Peran TIK

Peran TIK	
Rendah	
0	12
Sedang	
13	24
Tinggi	
25	36
Kritis	
37	48

Tabel diatas merupakan skor yang telah ditentukan dalam kriteria penilaian Peran TIK Indeks KAMI.

Tabel 3.2 Daftar Pertanyaan Seputar Peran TIK

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi		
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam instansi anda.		
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis	**Status**	Skor
#	**Karakteristik Instansi**	
1.1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah	Minim	0
1.2	Jumlah staff/pengguna dalam instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah	Kritis	4
1.3	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok		
1.4	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh instansi anda		
1.5	Dampak dari kegagalan sistem TIK utama yang digunakan instansi anda		
1.6	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja instansi anda		

Minim: hanya digunakan untuk mempermudah sejumlah kecil pekerjaan rutin, pencatatan, penyimpanan salinan dokumen, dll
Rendah: digunakan untuk menunjang kegiatan rutin
Sedang: digunakan untuk membantu penyelenggaraan layanan publik atau tugas utama instansi
Tinggi: digunakan sebagai sarana utama penyelenggaraan

3.4.2. Menilai Tingkat Kelengkapan Keamanan Informasi

Selanjutnya setelah melakukan pemetaan terhadap peran TIK, pada tahap ini akan dilakukan penilaian terhadap kesiapan dan kelengkapan keamanan informasi di STIE Perbanas berdasarkan data-data yang telah dikumpulkan sebelumnya. Indikator Kelengkapan Keamanan Informasi yang dimaksud adalah :

- Tata Kelola Keamanan Informasi

  Kontrol yang diperlukan adalah kebijakan formal yang mendefinisikan peran, tanggung-jawab, kewenangan pengelolaan keamanan informasi, dari pimpinan unit kerja sampai ke pelaksana operasional. Termasuk dalam area ini juga adalah adanya program kerja yang berkesinambungan, alokasi anggaran, evaluasi program dan strategi peningkatan kinerja tata kelola keamanan informasi.

- Pengelolaan Risiko Keamanan Informasi

  Bentuk tata kelola yang diperlukan adalah adanya kerangka kerja pengelolaan risiko dengan definisi yang eksplisit terkait ambang batas diterimanya risiko, program pengelolaan risiko dan langkah mitigasi yang secara reguler dikaji efektifitasnya.

- Kerangka Kerja Keamanan Informasi

  Kelengkapan kontrol di area ini memerlukan sejumlah kebijakan dan prosedur kerja operasional, termasuk strategi penerapan, pengukuran efektifitas kontrol dan langkah perbaikan.

- Pengelolaan Aset Informasi

  Kontrol yang diperlukan dalam area ini adalah bentuk pengamanan terkait keberadaan aset informasi,

termasuk keseluruhan proses yang bersifat teknis maupun administratif dalam siklus penggunaan aset tersebut.

- Teknologi dan Keamanan Informasi

  Untuk kepentingan Indeks KAMI, aspek pengamanan di area teknologi mensyaratkan adanya strategi yang terkait dengan tingkatan risiko, dan tidak secara eksplisit menyebutkan teknologi atau merk pabrikan tertentu.

Narasumber akan menjawab pertanyaan yang diberikan dalam indeks KAMI dengan memilih status penerapan, yaitu:

a. Tidak Dilakukan
b. Dalam Perencanaan
c. Dalam Perencanaan/Diterapkan Sebagian
d. Diterapkan Secara Menyeluruh

Setiap jawaban akan diberi skor yang nilainya disesuaikan dengan tahapan penerapan (kategori) bentuk pengamanan. Tabel pemetaan skor dapat dilihat seperti di bawah ini :

Tabel 3.3 *Range* Skor Kelengkapan Keamanan Informasi

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Tabel 3.4 Pertanyaan Kelengkapan Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi				
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Fungsi/Instansi Keamanan Informasi**	
2.1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi, termasuk penetapan kebijakan terkait?	Tidak Dilakukan
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	✓ Tidak Dilakukan Dalam Perencanaan Dalam Penerapan / Diterapkan Sebagian Diterapkan Secara Menyeluruh
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan
2.7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan
2.8	II	1	Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Tidak Dilakukan
2.9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan
2.10	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?	Tidak Dilakukan

3.5. Analisis dan Saran Perbaikan Keamanan Informasi

Pada tahapan ini akan dibuat saran dan perbaikan, Setelah sebelumnya dilakukan penilaian dengan indeks KAMI dan mengetahui hasil dari setiap area yang terdapat dalam indeks KAMI, maka tahap selanjutnya adalah membuat saran atau rekomendasi perbaikan pada setiap bagian yang masih kurang baik bagi STIE Perbanas Surabaya.

3.6. Penyusunan Laporan Tugas Akhir

Tahap ini adalah tahap terakhir dimana proses penyusunan hasil dan proses selama pengerjaan tugas akhir, dan disusun menjadi buku sebagai dokumentasi dari pengerjaan tugas akhir.

3.7. Jadwal Kegiatan

Berikut ini adalah jadwal dari pengerjaan tugas akhir yang dilakukan selama dua belas minggu :

Tabel 3.5 Alur Kegiatan Pengerjaan Tugas Akhir

No	Kegiatan	Maret				April				Mei				Juni			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Studi Literatur Tentang Keamanan Informasi dan Indeks KAMI																
2.	Pembuatan Instrumen Wawancara																
3.	Penggalian Informasi Pada STIE Perbanas Surabaya																
4.	Menilai Tingkat Kepentingan TIK dan Kelengkapan Keamanan Informasi di STIE Perbanas Surabaya																
5.	Analisis dan Saran Perbaikan																
6.	Penyusunan Buku Tugas Akhir																

(Halaman ini sengaja dikosongkan)

BAB IV
PERANCANGAN

Bagian ini menjelaskan perancangan penelitian tugas akhir. Perancangan ini diperlukan sebagai panduan dalam melakukan penelitian tugas akhir.

4.1. Perancangan Studi Kasus

Bagian ini menjelaskan rancangan studi kasus yang akan dilakukan pada penelitian ini seperti tujuan studi kasus dan *unit of analysis* yang digunakan.

4.1.1. Tujuan Studi Kasus

Menurut Creswell studi kasus merupakan suatu proses eksplorasi, deskriptif, atau penjelasan dari suatu kasus maupun beragam kasus dari waktu ke waktu melalui pengumpulan data yang mendalam serta melibatkan berbagai sumber informasi yang "kaya" dalam suatu konteks [15]. Menurut Yin studi kasus adalah cara unik untuk mengamati fenomena alam yang ada di satu set data [16]. Yin mengemukakan ada tiga kategori studi kasus yaitu eksplorasi (menggali), deskriptif, dan *explanatory* (memperjelas) [17]. Studi kasus eksplorasi yaitu melakukan eksplorasi terhadap fenomena apapun dalam data yang berfungsi sebagai tempat tujuan untuk peneliti. Studi kasus deskriptif digunakan untuk menggambarkan fenomena alamiah yang terjadi dalam data. Tujuan dari studi kasus deskriptif digunakan untuk menggambarkan data yang terjadi dalam bentuk narasi. Studi Kasus *explanatory* yaitu menjelaskan fenomena dalam data secara jelas mulai dari hal yang dasar sampai dalam.

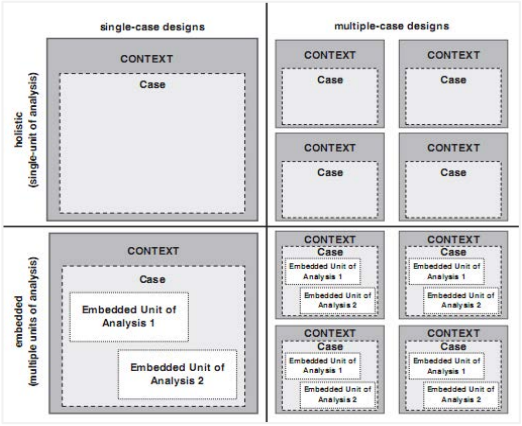
Untuk mencari jawaban dari rumusan masalah penelitian tugas akhir yang telah dijelaskan sebelumnya, dalam penelitian tugas akhir ini kategori studi kasus yang digunakan adalah deskriptif dan eksplorasi. Studi kasus yang digunakan dalam

penelitian ini karena diperlukan sebuah objek untuk dilakukan eksplorasi atau penggalian mengenai kondisi di organisasi.

Metode yang digunakan selama penggalian data kondisi kekinian adalah wawancara secara mendalam (*In-depth interview*) dan *review* dokumen. Responden yang dituju berdasarkan studi kasus di STIE Perbanas Surabaya adalah Bagian Program. Pemilihan responden tersebut dilakukan, karena pihak tersebut yang memiliki sumber informasi utama terkait kondisi kekinian fungsi, program, aktivitas, dan kondisi kekinian aplikasi yang diterapkan.

4.1.2. Unit of Analysis

Perancangan studi kasus dibagi menjadi dua yaitu *single-case* design dan *multiple-case design*. *Single-case design* menggunakan satu kasus untuk diuji sedangkan multiple case design menggunakan dua atau lebih kasus yang diuji. Dari kedua perancagan tersebut dibagi menjadi empat tipe yang diseuaikan dengan banyaknya *unit of analysis* yang digambarkan pada gambar 4.1



Gambar 4.1 Hubungan *Unit of Analysis*

Single-case dapat digunakan pada penelitian dengan kasus kritis atau unik, menguji teori yang telah dirumuskan dan melakukan eksplorasi. Sedangkan *multicase* digunakan pada penelitian eksplorasi perbedaan di dalam dan diantara kasus serta bertujuan untuk melakukan replikasi temuan di seluruh kasus.

Penelitian tugas akhir ini menggunakan perancangan *single case* (satu studi kasus) dengan beberapa unit of analysis. *Single case* dipilih karena pada penelitian ini bertujuan untuk melakukan eksplorasi atau menggali studi kasus. *Unit of analysis* (unit analisis) yang telah ditentukan oleh peneliti dalam penelitian ini adalah melakukan analisis Indeks KAMI di STIE Perbanas Surabaya.

4.2. Data yang Diperlukan

Pada bagian ini akan dijelaskan mengenai data yang diperlukan dalam penelitian tugas akhir. Dalam melakukan penelitian dibutuhkan data yang dapat mendukung tahapan pengalian data dan informasi sesuai dengan studi kasus penelitian. Poin-poin mengenai data yang diperlukan antara lain sebagai berikut:

1. Tugas Pokok dan fungsi dari Departemen Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas Surabaya.
2. Gambaran kondisi Tata Kelola Keamanan Informasi saat ini seperti apakah terdapat kontrol yang diperlukan (kebijakan formal yang mendefinisikan peran, tanggung-jawab, kewenangan pengelolaan keamanan informasi, dari pimpinan unit kerja sampai ke pelaksana operasional). Termasuk dalam area ini juga adalah apakah ada program kerja yang berkesinambungan, alokasi anggaran, evaluasi program dan strategi peningkatan kinerja tata kelola keamanan informasi.

3. Gambaran kondisi Pengelolaan Risiko Keamanan Informasi seperti bagaimana bentuk tata kelola yang diperlukan adalah adanya kerangka kerja pengelolaan risiko dengan definisi yang eksplisit terkait ambang batas diterimanya risiko, program pengelolaan risiko dan langkah mitigasi yang secara reguler dikaji efektifitasnya.
4. Gambaran kondisi Kerangka Kerja Keamanan Informasi yang digunakan seperti apakah ada sejumlah kebijakan dan prosedur kerja operasional, termasuk strategi penerapan, pengukuran efektifitas kontrol dan langkah perbaikannya.
5. Gambaran kondisi Pengelolaan Aset Informasi seperti kontrol dalam bentuk pengamanan terkait keberadaan aset informasi, termasuk keseluruhan proses yang bersifat teknis maupun administratif dalam siklus penggunaan aset tersebut.
6. Gambaran kondisi Teknologi dan Keamanan Informasi seperti aspek pengamanan di area teknologi mensyaratkan adanya strategi yang terkait dengan tingkatan risiko.

4.3. Persiapan Pengumpulan Data

Pada bagian ini akan menjelaskan mengenai persiapan pengumpulan data pada penelitian tugas akhir ini. Terdapat beberapa metode yang digunakan untuk pengumpulan data, diantaranya: pengamatan langsung, wawancara, catatan arsip, dokumen, survei dan pastisipan observasi. Dalam penelitian tugas akhir ini, metode pengumpulan data yang digunakan adalah wawancara, observasi, dan *review* dokumen.

Instrumen Wawancara

Instrumen Wawancara adalah pertanyaan yang akan diajukan pada saat wawancara dengan narasumber. Dalam penelitian ini, instrumen wawancara yang digunakan dibuat berdasarkan dan sesuai dengan kriteria dalam Indeks KAMI yang

mencakup peran TIK, dan kelengkapan pengamanan 5 area keamanan informasi.

Wawancara Mendalam (*In-depth Interview*)

Wawancara dilakukan kepada narasumber yang paham mengenai kondisi kekinian STIE Perbanas Surabaya dimana narasumber tersebut merupakan narasumber utama. Narasumber dipilih dengan memperhatikan kapasitas serta kewenangannya untuk memberikan informasi yang valid sesuai pertanyaan yang diajukan untuk menghindari terjadinya misinformasi. Berikut ini merupakan profil narasumber dalam penelitian :

Tabel 4.1 Narasumber Beserta Jabatan

Nama	Jabatan
Hariadi Yutanto, S.Kom., M.Kom.	Kasie TIK (Manajemen Jaringan dan Technical Support)

Narasumber tersebut dipilih karena saat penulis turun langsung ke lapangan untuk bertanya mengenai poin penilaian yang nantinya akan ditanyakan, pihak Pimpinan Departemen TIK menunjuk serta mengarahkan langsung kepada narasumber tersebut yaitu Bapak Hariadi Yutanto, S.Kom., M.Kom. yang telah 10 tahun menjabat sebagai kasie TIK sehinga relevan dengan keahlian maupun memiliki informasi yang luas terkait wawancara indikator-indikator yang nantinya ditanyakan. Sedangkan untuk pimpinan Departemen TIK baru 2 tahun menjabat sebagai pimpinan departemen.

Kondisi kekinian yang dimaksud, akan dilihat dari kondisi kekinian fungsi, program, dan aktivitas, serta kondisi kekinian aplikasi yang sudah diterapkan. Instrumen wawancara yang digunakan untuk pengumpulan data disertakan dalam LAMPIRAN A s/d LAMPIRAN F.

Angket
Angket digunakan untuk mengumpulkan informasi yang nantinya memberikan gambaran (deskripsi) yang dibutuhkan dalam instansi yang mengacu pada perspektif dari narasumber. Angket yang diberikan berupa angket tertutup yang terdiri dari pertanyaan di sertai dengan alternatif jawaban.

Observasi
Observasi dilakukan untuk mengamati secara langsung keadaan yang sebenarnya terjadi di *STIE Perbanas Surabaya* dan juga untuk memperkuat dan mendukung hasil dari wawancara itu sendiri.

Review Dokumen
Review dokumen merupakan metode yang digunakan untuk mendukung berbagai informasi yang belum didapatkan dan memiliki kaitan dengan hasil wawancara. Dalam penelitian ini, berbagai informasi yang didapatkan dari *review* dokumen terkait kondisi kekinian STIE Perbanas Surabaya adalah informasi struktur organisasi, fungsi, strategi, tupoksi, program, dan aktivitas yang terlampir dalam dokumen fisik maupun digital yang berhubungan dengan hasil wawancara.

4.4. Metode Pengolahan Data

Setelah wawancara (*In-depth Interview*) dilakukan maka selanjutnya hasil tersebut akan diolah dengan menulis ulang rekaman wawancara yang tersimpan pada media *recorder*, dan penulisannya dilakukan menggunakan aplikasi pengolah kata (Word Processing). Untuk pengolahan data selanjutnya, berdasarkan hasil *In-depth Interview*, *Observasi* dan *review* dokumen, kemudian berdasarkan hasil tersebut akan dilakukan pembobotan terhadap karakteristik Indeks KAMI dan selanjutnya, seluruh skor hasil pembobotan dari tiap komponen dijumlahkan yang pada akhirnya menghasilkan skor total pada Dashboard Indeks KAMI, skor total tersebut akan menggambarkan kondisi keamanan informasi di STIE

Perbanas Surabaya. Berdasarkan hasil tersebut maka selanjutnya akan dibuat rekomendasi berdasarkan komponen pertanyaan pada Indeks KAMI. Keseluruhan data yang tekait dengan operasi matematis diolah menggunakan perantara *Dashboard* Indeks KAMI yang dikembangkan dari *software* Microsoft Office Excel.

4.5. Pendekatan Analisis

Analisis terhadap data perlu dilakukan setelah melakukan pengumpulan data. Hal ini dilakukan untuk mengetahui hubungan antara data dengan objek yang diinginkan. Beberapa pendekatan yang akan dilakukan adalah:

1. **Pendekatan Tingkat Kepentingan TIK Indeks KAMI**
   Pendekatan ini adalah bagian dan merupakan tahap awal dari Indeks KAMI yang digunakan untuk mengetahui tingkat klasifikasi terhadap peran dan kepentingan TIK di STIE Perbanas.

2. **Pendekatan 5 Area Keamanan Informasi Indeks KAMI**
   Pendekatan ini digunakan untuk membantu proses identifikasi kesiapan dan kelengkapan keamanan informasi di STIE Perbanas yang nantinya akan dilakukan penilaian.

3. **Pemberian Rekomendasi Berdasarkan**
   Rekomendasi yang diberikan mengacu pada standar kontrol keamanan informasi ISO/IEC 27002:2005 dimana standar ini memberikan panduan serta rekomendasi dalam perencanaan dan implementasi suatu program untuk melindungi aset informasi ukuran pemetaan sasaran kontrol keamanan informasi yang meliputi berbagai aspek berikut ini:

- Kebijakan Keamanan Informasi (*Security Policy*)
- Organisasi Keamanan Informasi (*Organizational of Information Security*)
- Manajemen Aset (*Asset Management*)
- Keamanan Sumber Daya Manusia (*Human Resources Security*)
- Keamanan Fisik dan Lingkungan (*Physical and Environtment Security*)
- Komunikasi dan Manajemen Operasi (*Communication and Operation Management*)
- Akses Kontrol (*Access Control*)
- Pengadaan/akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (*Information Systems Acquisitions, Development, and Maintenance*)
- Pengelolaan Insiden Keamanan Informasi (*Information Security Incident Management*)
- Manajemen Kelangsungan Usaha (*Business Continuity Management*)
- Kesesuaian (*Compliance*)

BAB V
IMPLEMENTASI

Bab ini menjelaskan hasil dari proses perancangan studi kasus yang didapatkan melalui wawancara dan review dokumen.

5.1. Profil Organisasi

Pada bagian ini dibahas mengenai profil organisasi STIE Perbanas Surabaya.

5.1.1. Sejarah STIE Perbanas Surabaya

Sekolah Tinggi Ilmu Ekonomi Perbanas Surabaya atau STIE Perbanas Surabaya adalah sebuah perguruan tinggi swasta yang terdapat di Surabaya, Jawa Timur, Indonesia. STIE Perbanas Surabaya merupakan lembaga pendidikan dalam bidang bisnis dan perbankan di bawah naungan Perhimpunan Bank-bank Umum Nasional (Perbanas) Jawa Timur.

Didirikan pada tahun 1970, STIE Perbanas Surabaya saat ini telah mengombinasikan berbagai fasilitas modern dan pendekatan dinamis untuk pengajaran dan penelitian yang telah menghasilkan berbagai prestasi yang membanggakan. Perolehan berbagai sertifikasi, penghargaan, dan dana hibah merupakan bentuk pengakuan atas komitmen dan kerja keras dalam peningkatan mutu layanan pendidikan. Sejak Januari 2006, STIE Perbanas Surabaya telah memperoleh sertifikasi ISO 9001:2000.

Pada tahun 2009 STIE Perbanas Surabaya mendapat pengakuan dari Kopertis Wilayah VII sebagai 5 besar perguruan tinggi unggulan di Jawa Timur untuk kelompok institut, sekolah tinggi, akademi, dan politeknik. Selain itu STIE Perbanas Surabaya juga menjadi perguruan tinggi

berprestasi di Jawa Timur dalam bidang penelitian dan pengabdian masyarakat serta dalam bidang tata kelola. Bentuk lain dari pengakuan atas kualitas pengelolaan perguruan tinggi adalah diperolehnya bantuan dana dari Direktorat Jenderal Pendidikan Tinggi, Departemen Pendidikan Nasional Republik Indonesia, untuk pengembangan pendidikan STIE Perbanas Surabaya tahun 2007–2011.

5.1.2. Visi STIE Perbanas Surabaya

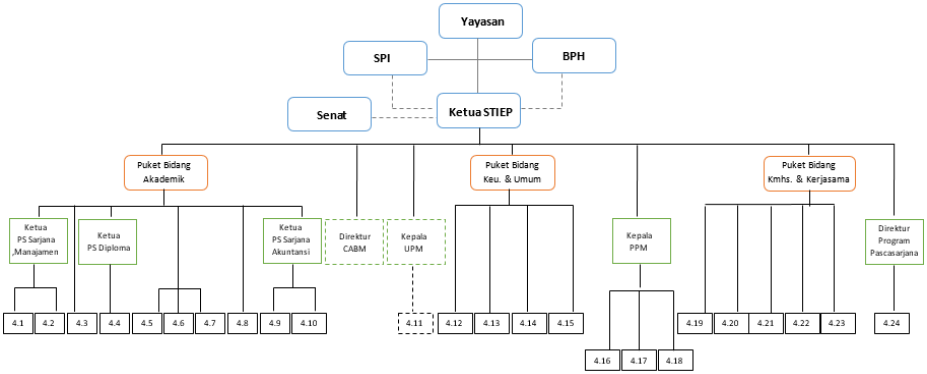
Menjadi Perguruan Tinggi terkemuka yang memiliki keunggulan kompetitif di bidang bisnis dan perbankan yang berwawasan global.

5.1.3. Misi STIE Perbanas Surabaya

1. Menyelenggarakan pendidikan dan pengajaran yang memiliki keunggulan kompetitif di bidang bisnis dan perbankan yang berwawasan global.
2. Menyelenggarakan penelitian dan pengabdian kepada masyarakat yang berkualitas, yang dapat memberikan kontribusi bagi pengembangan ilmu dan praktek di bidang bisnis dan perbankan serta peningkatan kesejahteraan masyarakat.
3. Menjalin kerjasama yang berkesinambungan dengan berbagai instansi yang terkait, baik di dalam maupun luar negeri dalam rangka pelaksanaan Tri Dharma Perguruan Tinggi.
4. Melakukan penataan manajemen yang menciptakan suasana akademik yang berorientasi pada tata kelola Perguruan Tinggi yang sehat, dinamis, ramah dan bersahabat.

5.1.4. Struktur Organisasi STIE Perbanas Surabaya

Berikut ini adalah diagram struktur organisasi dalam STIE Perbanas Surabaya :



Gambar 5.1 Struktur Organisasi STIE Perbanas Surabaya

Berikut ini adalah keterangan dari struktur organisasi dalam STIE Perbanas Surabaya :

1.1 Sekretaris Program Studi (PS) Sarjana Manajemen
1.2 Kepala Laboratorium Manajemen
1.3 Kepala Bagian Akademik
1.4 Sekretaris PS Diploma
1.5 Kepala Laboratorium Komputer & PTP
1.6 Kepala Laboratorium Bahasa
1.7 Kepala Laboratorium Bank STIE
1.8 Kepala Bagian Perpustakaan
1.9 Sekretaris PS Sarjana Akuntansi
1.10 Kepala Laboratorium Akuntansi
1.11 Wakil Ketua Unit Penjaminan Mutu (UPM)
1.12 Kepala Bagian SDM
1.13 Kepala Bagian Keuangan
1.14 Kepala Bagian Umum
1.15 Kepala Bagian Teknologi Informasi dan Komunikasi
1.16 Kepala Bidang Abdimas
1.17 Kepala Bidang Penelitian
1.18 Kepala Pengelolaan Jurnal dan Penerbitan Buku

1.19 Kepala Bagian Humas
1.20 Kepala Bagian Kerjasama
1.21 Kepala Perbanas Career Center
1.22 Kepala Bagian Kemahasiswaan
1.23 Kepala Student Advisory Center
1.24 Sekretaris Program Pascasarjana

5.1.5. Peran Departemen Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas Surabaya

STIE Perbanas Surabaya membangun kebutuhan akan informasi dan komunikasi pada awalnya dengan membuat unit kerja setingkat seksi, yaitu Electronic Data Processing (EDP) dengan dikepalai seorang Kepala Seksi pada akhir tahun 2002. Melihat perkembangan dan kebutuhan akan teknologi informasi dan komunikasi yang mendukung penyelenggaraan pendidikan di STIE Perbanas Surabaya, maka pada pertengahan tahun 2006 unit kerja ini ditingkatkan menjadi Bagian Pusat Data Informasi (PDI). Penigkatan status unit kerja ini sebagai cerminan dari meningkatnya kebutuhan dan tuntutan aktivitas dalam bidang informasi dan komunikasi.

Departemen TIK STIE Perbanas Surabaya memiliki visi dan misi sebagai berikut [18]:

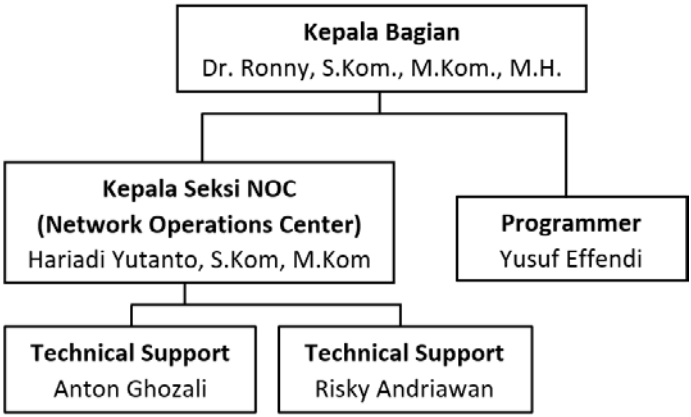
- Visi
  Mewujudkan *ICT-Based* sebagai sarana utama dalam peningkatan kualitas penyelenggaraan pendidikan dan berkontribusi pada pengembangan sistem informasi perbankan indonesia.

- Misi
  1. Meningkatkan kualitas akses informasi penyelengaraan pendidikan bagi seluruh civitas akademika baik di lingkungan internal maupun eksternal.

2. Meningkatkan suasana akademik berbasis teknologi informasi dan komunikasi dalam proses pengajaran.
3. Meningkatkan efisiensi proses penyelengaraan pendidikan.

5.1.6. Struktur Organisasi Departemen Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas Surabaya

Berikut ini adalah diagram struktur organisasi Departemen Teknologi Informasi dan Komunikasi (TIK) di STIE Perbanas Surabaya :



Gambar 5.1 Struktur Organisasi Departemen TIK

5.1.7. Hasil Wawancara Mengenai Indeks Keamanan Informasi Di STIE Perbanas Surabaya

Berdasarkan perancangan studi kasus yang dilakukan mengenai Indeks Keamanan Informasi, dengan bapak Hariadi Yutanto, S.Kom, M.Kom selaku Kepala Seksi Bidang TIK (Manajemen Jaringan dan Technical Support) sebagai narasumber. Wawancara telah dilakukan pada tanggal 14-15

April 2016 di Kampus 2 STIE Perbanas. Hasil wawancara tersebut secara singkat diuraikan dalam poin berikut:

5.1.7.1. Peran & Tingkat Kepentingan TIK di STIE Perbanas Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi STIE Perbanas Surabaya dengan kriteria Peran & Tingkat Kepentingan TIK pada Indeks KAMI. Kriteria Hasil wawancara secara lengkap dapat dilihat pada Lampiran A.

5.1.7.2. Tata Kelola Keamanan Informasi di STIE Perbanas Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi STIE Perbanas Surabaya dengan kriteria Tata Kelola Keamanan Informasi pada Indeks KAMI. Kriteria Hasil wawancara secara lengkap dapat dilihat pada Lampiran B.

5.1.7.3. Pengelolaan Risiko Keamanan Informasi di STIE Perbanas Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi STIE Perbanas Surabaya dengan kriteria Pengelolaan Risiko Keamanan Informasi pada Indeks KAMI. Kriteria Hasil wawancara secara lengkap dapat dilihat pada Lampiran C.

5.1.7.4. Kerangka Kerja Pengelolaan Keamanan Informasi di STIE Perbanas Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi STIE Perbanas Surabaya dengan kriteria Kerangka

Kerja Pengelolaan Keamanan Informasi pada Indeks KAMI. Kriteria Hasil wawancara secara lengkap dapat dilihat pada Lampiran D.

5.1.7.5. Pengelolaan Aset Informasi di STIE Perbanas Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi STIE Perbanas Surabaya dengan kriteria Pengelolaan Aset Informasi pada Indeks KAMI. Kriteria Hasil wawancara secara lengkap dapat dilihat pada Lampiran E.

5.1.7.6. Teknologi dan Keamanan Informasi di STIE Perbanas Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi STIE Perbanas Surabaya dengan kriteria Teknologi dan Keamanan Informasi pada Indeks KAMI. Kriteria Hasil wawancara secara lengkap dapat dilihat pada Lampiran F.

(Halaman ini sengaja dikosongkan)

BAB VI
HASIL DAN PEMBAHASAN

Bab ini menjelaskan pembahasan terhadap objek penelitian dan hasil yang diperoleh. Pada penelitian ini akan dilakukan pembahasan, dari penilaian yang dilakukan untuk mendapatkan Indeks Keamanan Informasi pada STIE Perbanas Surabaya.

6.1. Hasil Penilaian Skor Per Bagian

6.1.1. Peran & Tingkat Kepentingan TIK

Tahap ini merupakan tahap pertama yang dilakukan sebelum tahap penilaian terhadap 5 (lima) area selanjutnya. Tahap ini bertujuan untuk mengetahui klasifikasi Peran & Tingkat Kepentingan TIK di instansi ke dalam klasifikasi spesifik yang telah ditentukan yaitu: Rendah, Sedang, Tinggi, dan Kritis.

Berikut ini merupakan hasil dari penilaian Peran & Tingkat TIK di STIE Perbanas Surabaya :

Tabel 6.1 Penilaian Peran dan Tingkat Kepentingan

No	Pertanyaan	Status	Skor
1.1	Total anggaran untuk TIK/Tahun - < Rp. 1 Milyard = Minim - Rp. 1 Milyard - Rp. 3 Milyard = Rendah - Rp. 3 Milyard - Rp 8 Milyard = Sedang - Rp. 8 Milyard - Rp. 20 Milyard = Tinggi - Rp. 20 Milyard > = Kritis	Rendah	1
	Temuan		
	Anggaran yang dialokasikan untuk TIK masih rendah		

	Sumber Penggalian Data		
	Wawancara & Review Dokumen		
	Bukti Dokumen		
	Lampiran Foto G-18		
1.2	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60 = Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Sedang	2
	Temuan		
	Jumlah staff/pengguna TIK dalam range sedang (120 - 240)		
	Sumber Penggalian Data		
	Wawancara		
	Bukti Dokumen		
	-		
1.3	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok dan Fungsi Instansi anda	Kritis	4
	Temuan		
	Terdapat berbagai macam sistem informasi yang digunakan seperti sistem informasi mahasiswa baru, kemahasiswaan, akademik, kepegawaian, keuangan, kesekretariatan, humas, kesekretariatan, humas, pusat penelitian dan pengabdian masyarakat, perpustakaan, umum, dan pimpinan		
	Sumber Penggalian Data		
	Observasi		
	Bukti Dokumen		
	Lampiran Foto G-12		
1.4	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Sedang	2
	Temuan		
	Lembaga pendidikan dimana terdapat sistem/aplikasi yang merupakan aset nasional dan data/ informasi penting berskala nasional		

	Sumber Penggalian Data		
	Observasi		
	Bukti Dokumen		
	Lampiran Foto G-10 dan Foto G-12		
1.5	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Tinggi	3
	Temuan		
	Kegagalan aplikasi/sistem informasi akademik dapat mengganggu tersedianya layanan karena digunakan sebagai komponen utama dan tugas utama instansi, sulit untuk digantikan proses manual		
	Sumber Penggalian Data		
	Observasi		
	Bukti Dokumen		
	Lampiran Foto G-10 dan Foto G-12		
1.6	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Tinggi	3
	Temuan		
	Sistem beroperasi secara terintegrasi dengan sistem lainnya, tetapi ketersediaannya tidak mengganggu fungsi sistem lain tersebut		
	Sumber Penggalian Data		
	Observasi		
	Bukti Dokumen		
	Lampiran Foto G-12 dan Foto G-16		
1.7	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi pemerintah lainnya atau terhadap ketersediaan sistem pemerintah berskala nasional	Tinggi	3
	Temuan		
	Gangguan terhadap layanan publik yang bersifat nasional, hilangnya data publik dalam jumlah sangat besar seperti data mahasiswa, data akademik, dll.		
	Sumber Penggalian Data		
	Observasi		

	Bukti Dokumen		
	Lampiran Foto G-12		
1.8	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Kritis	4
	Temuan		
	Sangat membutuhkan layanan TIK untuk menjalankan tugas instansi seperti proses belajar mengajar, pengelolaan data akademik, dll.		
	Sumber Penggalian Data		
	Observasi		
	Bukti Dokumen		
	Lampiran Foto G-12		
1.9	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Rendah	1
	Temuan		
	Ada sejumlah Kebijakan yang harus diikuti dalam penyelenggaraan layanan menggunakan sistem namun tidak didefinisikan		
	Sumber Penggalian Data		
	Wawancara		
	Bukti Dokumen		
	-		
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Tinggi	3
	Temuan		
	Terungkapnya informasi sensitif atau terbatas seperti data mahasiswa yang dapat berakibat pada gagalnya program kerja atau mengganggu kinerja/kredibilitas dari institusi sendiri		
	Sumber Penggalian Data		
	Observasi		
	Bukti Dokumen		
	Lampiran Foto G-12		
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Sedang	2
	Temuan		
	Sistem harus dioperasikan dengan dukungan teknis dari pihak eksternal, teknologi dengan spesifikasi yang cukup spesifik		

	Sumber Penggalian Data		
	Wawancara dan Observasi		
	Bukti Dokumen		
	Lampiran Foto G-9		
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Sedang	2
	Temuan		
	Sistem informasi akademik dan infrastruktur TI digunakan untuk membantu penyelenggaraan tugas utama instansi, dan sistem digunakan secara internal dan terbatas		
	Sumber Penggalian Data		
	Observasi		
	Bukti Dokumen		
	Lampiran Foto G-12, Foto G-13 dan Foto G-16		
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	Tinggi	30

Berdasarkan penilaian pada Tabel 6.1 dapat dilihat Skor Peran dan Tingkat Kepentingan TIK menunjukkan nilai 30, kemudian selanjutnya dilakukan pemetaan skor seperti yang ditunjukkan pada Tabel 6.2 maka Skor Peran dan Tingkat Kepentingan TIK di STIE Perbanas Surabaya termasuk ke dalam kategori Tinggi sehingga jika terdapat gangguan pada pada layanan teknologi informasi khususnya keamanan informasi maka akan terjadi dampak kerugian yang akan menghambat proses yang terjadi di lingkup internal maupun eksternal STIE Perbanas Surabaya sendiri yang artinya kebutuhan TIK bagi layanan akademis dan administratif di STIE Perbanas Surabaya cukup vital serta diperhitungkan.

Tabel 6.2 Mapping Skor Peran dan Tingkat Kepentingan TIK

Bagian I: Indeks Ketergantungan TIK		
Terendah	**Tertinggi**	**Status**
0	12	Rendah
13	24	Sedang
25	36	Tinggi
37	48	Kritis

Beberapa poin yang menjadi perhatian adalah poin 1.3 dan 1.8 pada Tabel 6.1 yang mendapat status kritis yaitu tingkat ketergantungan dan tingkat sensifitas pengguna terhadap layanan TIK di STIE Perbanas Surabaya dapat dilihat dari jumlah sistem informasi yang digunakan seperti sistem informasi mahasiswa baru, kemahasiswaan, akademik, kepegawaian, keuangan, kesekretariatan, humas, kesekretariatan, humas, pusat penelitian dan pengabdian masyarakat, perpustakaan, umum, dan pimpinan seperti ditunjukkan Foto G-12 pada lampiran.

Hal tersebut menandakan bahwa sistem informasi yang ada selain menjadi alat bantu untuk meningkatkan efisiensi, juga menjadi sesuatu yang berfungsi sangat strategis, dalam artian sistem tersebut dapat secara signifikan memberikan dukungan terhadap berbagai aplikasi operasional dan manajerial atas berbagai fungsi maupun proses bisnis di STIE Perbanas Surabaya yang secara umum berhubungan dengan proses penciptaan dan pengaliran informasi.

6.1.2. Tata Kelola Keamanan Informasi

Berikut ini merupakan hasil dari penilaian Tata Kelola Keamanan Informasi di STIE Perbanas Surabaya :

Tabel 6.3 Penilaian Tata Kelola Keamanan Informasi

No			Pertanyaan	Status	Skor
2.1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Pemimpin bertanggungjawab namun masalah spesifik keamanan informasi belum didefinisikan dan masih dalam perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-1 dan Foto G-19				
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Dalam Perencanaan	1
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-2 dan Foto G-19				

2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Kebijakan yang mengatur secara detail masih dalam tahap penyusunan (blueprint)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-3, dan Foto G-19				
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Ada alokasi sumber daya namun masih minim				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-4				

2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Dalam Perencanaan	1
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara & Review				
	Bukti Dokumen				
	Lampiran Interview Protocol B-5 dan Gambar G-19				
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan	0
	Temuan				
	Belum ada standar kompetensi yang didefinisikan				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-6 dan Foto G-19				
2.7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan	0

	Temuan				
	Tidak ada standar kompetensi yang menjadi acuan				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-7				
2.8	II	1	Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Ada sosialisasi secara individual namun untuk sosialisasi secara resmi masih belum dilaksanakan				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-8				
2.9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	4
	Temuan				
	Ada walau belum dijadwalkan secara rutin				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Foto G-25, Foto G-26, dan Foto G-27				

2.10	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?	Dalam Penerapan / Diterapkan Sebagian	4
	Temuan				
	Ada namun belum cukup sistematis dan cenderung kondisional saat terjadi *accident*				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-10				
2.11	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	4
	Temuan				
	Ada namun belum dilakukan secara proaktif				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-11				

2.12	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Dalam Perencanaan	2
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara dan Review Dokumen				
	Bukti Dokumen				
	Lampiran Interview Protocol B-12 dan Foto G-19				
2.13	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Dalam Penerapan / Diterapkan Sebagian	4
	Temuan				
	Hanya ada pelaporan secara insidentil				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-13				
2.14	III	2	Apakah kondisi dan permasalahan keamanan informasi menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Dalam Penerapan / Diterapkan Sebagian	4

	Temuan				
	Menjadi pertimbangan, walaupun dalam gambaran keseluruhannya masih belum jelas				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-14				
2.15	IV	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Dalam Perencanaan	0
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-15 dan Foto G-19				
2.16	IV	3	Apakah Instansi anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi?	Dalam Perencanaan	0
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-16, dan Foto G-19				

2.17	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Dalam Perencanaan	1
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-17, dan Gambar G-19				
2.18	IV	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi?	Dalam Perencanaan	1
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-18, Foto G-19				
2.19	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Dalam Perencanaan	0
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				

	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-19, dan Foto G-19				
2.20	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Dalam Perencanaan	0
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol B-20, Gambar G-19				
				Total Nilai Evaluasi Tata Kelola	**32**

Tabel 6.4 Mapping Skor Tata Kelola Keamanan Informasi

Validitas Tata Kelola							
Tingkat Kematangan I		**Tingkat Kematangan II**		**Tingkat Kematangan III**		**Tingkat Kematangan IV**	
Validitas	Yes	**Validitas**	No	**Validitas**	No	**Validitas**	No
Status	I+	**Status**	No	**Status**	No	**Status**	No

Status Akhir	**I+**

Keterangan :

- Berdasarkan penilaian pada Tabel 6.3 dapat dilihat Skor Tata Kelola Keamanan Informasi di STIE Perbanas Surabaya menunjukkan nilai 32 (dari skor maksimum 114) yang berarti masuk ke dalam kategori Rendah.

- Untuk penilaian aspek Tata Kelola Keamanan Informasi dapat dilihat pada Tabel 6.3 tidak ada aspek yang memenuhi kriteria “Diterapkan Secara Menyeluruh” karena belum memenuhi persyaratan minimal.
- Dari keseluruhan poin pertanyaan, status yang menjadi mayoritas adalah "Dalam Perencanaan" hal tersebut menunjukkan bahwa pihak Departemen TIK cukup menyadari pentingnya Tata Kelola Keamanan Informasi namun untuk implementasinya masih belum ada khususnya untuk Dokumen Kebijakan Keamanan Informasi (*Security Policies*).

  Dokumen Kebijakan Keamanan Informasi (*Security Policies*) dibutuhkan untuk menjadi acuan untuk melindungi aset informasi penting. Dokumen tersebut berisi berbagai cara yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata cara dalam mengamankan informasi.
- Perlu dilaksanakan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi secara rutin.

6.1.3. Pengelolaan Risiko Keamanan Informasi

Berikut ini merupakan hasil dari penilaian Risiko Keamanan Informasi di STIE Perbanas Surabaya :

Tabel 6.5 Penilaian Pengelolaan Risiko Keamanan Informasi

No			Pertanyaan	Status	Skor
3.1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Perencanaan	1
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				

	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-1, dan Gambar G-19				
3.2	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Perencanaan	1
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-2, dan Foto G-19				
3.3	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	Dalam Perencanaan	1
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-3, dan Foto G-19				

3.4	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Dalam Perencanaan	1
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-4, dan Foto G-19				
3.5	II	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Dalam Perencanaan	1
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-5 dan Foto G-19				
3.6	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Perencanaan	1
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				

	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-6 dan Foto G-19				
3.7	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Dalam Perencanaan	1
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-7, dan Foto G-19				
3.8	II	1	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Dalam Perencanaan	1
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-8, dan Foto G-19				

3.9	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Perencanaan	1
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-9, dan Foto G-19				
3.10	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Dalam Perencanaan	2
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-10, dan Foto G-19				
3.11	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Dalam Perencanaan	2

	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-11, dan Foto G-19				
3.12	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya?	Dalam Perencanaan	2
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-12, dan Foto G-19				
3.13	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Dalam Perencanaan	2
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-13, dan Foto G-19				

3.14	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Dalam Perencanaan	0
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-14, dan Foto G-19				
3.15	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Dalam Perencanaan	0
	Temuan				
	Belum ada standar mengenai pengelolaan risiko, masih dalam tahap penyusunan (*blueprint*)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol C-15, dan Foto G-19				
Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi					**17**

Tabel 6.6 Mapping Skor Pengelolaan Risiko

Validitas Pengelolaan Risiko Keamanan Informasi							
Tingkat Kematangan I		**Tingkat Kematangan II**		**Tingkat Kematangan III**		**Tingkat Kematangan IV**	
Validitas	No	**Validitas**	No	**Validitas**	No	**Validitas**	No
Status	No	**Status**	No	**Status**	No	**Status**	No
Status Akhir	**I**						

Keterangan :

- Berdasarkan penilaian pada Tabel 6.5 dapat dilihat Skor Pengelolaan Risiko Keamanan Informasi di STIE Perbanas Surabaya menunjukkan nilai 17 (dari skor maksimum 69) dan juga belum melewati tingkat kematangan I yang berarti masuk ke dalam ambang batas minimum dengan keseluruhan status pertanyaan menunjukkan status "Dalam Perencanaan".
- Pihak STIE Perbanas melakukan penyusunan dokumen cetak biru (*blueprint*) setiap 5 tahun sekali dan memiliki rencana pembuatan dokumen manajemen resiko pada dokumen *blueprint* periode berikutnya yang masih dalam tahap penyusunan seperti pada dokumen *blueprint* periode 2011-2015 dalam Foto G-19 pada lampiran.
- Belum ada standar atau program kerja mengenai pengelolaan risiko yang didefinisikan secara umum maupun yang spesifik mengenai keamanan informasi pada STIE Perbanas Surabaya.
- Pihak STIE Perbanas Surabaya masih belum menyadari potensi ancaman atau risiko yang akan terjadi dan dapat menyebabkan kerugian pada aset informasinya.
- Perlu mendefinisikan dokumen serta strategi penerapan Manajemen Risiko Keamanan Informasi yang bertujuan untuk meminimalkan kemungkinan dan pengaruh atas terjadinya peristiwa yang merugikan terhadap keamanan informasi dengan perencanaan penanganan risiko yang terdokumentasi, serta mengkaji secara rutin risiko secara lebih lanjut serta rencana penanganan risiko yang diperlukan.

6.1.4. Kerangka Kerja Pengelolaan Keamanan Informasi

Berikut ini merupakan hasil dari penilaian Kerangka Kerja Keamanan Informasi di STIE Perbanas Surabaya :

Tabel 6.7 Penilaian Kerangka Kerja Keamanan Informasi

No			Pertanyaan	Status	Skor
4.1	II	1	Apakah kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Dalam Perencanaan	1
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara & Review Dokumen				
	Bukti Dokumen				
	Lampiran Interview Protocol D-1, dan Foto G-19				
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Dalam Perencanaan	0
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara & Review Dokumen				
	Bukti Dokumen				
	Lampiran Interview Protocol D-2, dan Foto G-19				

4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Tidak Dilakukan	0
	Temuan				
	Belum ada prosedur khusus Keamanan Informasi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-3, dan Foto G-19				
4.4	II	1	Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Dalam Perencanaan	0
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara & Interview				
	Bukti Dokumen				
	Lampiran Interview Protocol D-4, dan Foto G-19				
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	Tidak Dilakukan	1

	Temuan				
	Belum ada prosedur keamanan informasi yang terdefinisi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-5				
4.6	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?	Tidak Dilakukan	2
	Temuan				
	Belum ada prosedur keamanan informasi yang terdefinisi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-6				
4.7	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Tidak Dilakukan	4
	Temuan				
	Belum ada kebijakan keamanan informasi yang terdefinisi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-7				
4.8	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?	Dalam Perencanaan	0

	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara & Reviw Dokumen				
	Bukti Dokumen				
	Lampiran Interview Protocol D-8, dan Foto G-19				
4.9	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Dalam Penerapan / Diterapkan Sebagian	0
	Temuan				
	Masih belum terstruktur dan belum ada prosedur operasional (Lampiran D-9)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-9				
4.10	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dalam Penerapan / Diterapkan Sebagian	4
	Temuan				
	Ada program pengembangan namun untuk spesifik manajemen resiko untuk menanggulangi permasalahan yang muncul masih belum ada				

	Sumber Penggalian Data				
	Wawancara & Review Dokumen				
	Bukti Dokumen				
	Lampiran Interview Protocol D-10, Foto G-17, dan Foto G-18				
4.11	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	Tidak Dilakukan	4
	Temuan				
	Belum ada proses penanggulangan				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-11				
4.12	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Dalam Perencanaan	2
	Temuan				
	Belum ada kerangka kerja apapun				
	Sumber Penggalian Data				
	Wawancara & Review Dokumen				
	Bukti Dokumen				
	Lampiran Interview Protocol D-12, dan Gambar G-19				

4.13	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Dalam Perencanaan	0
	Temuan DRP Masih dalam tahap perencanaan Sumber Penggalian Data Wawancara & Review Dokumen Bukti Dokumen Lampiran Interview Protocol D-13, dan Gambar G-19				
4.14	III	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Dalam Perencanaan	0
	Temuan Rencana pemulihan masih dalam perencanaan Sumber Penggalian Data Wawancara & Review Dokumen Bukti Dokumen Lampiran D-14, dan Gambar G-19				

4.15	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Dalam Perencanaan	0
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara & Review Dokumen				
	Bukti Dokumen				
	Lampiran D-15, dan Foto G-19				
4.16	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Diterapkan Secara Menyeluruh	0
	Temuan				
	QoP (Quality of Procedure) di evaluasi				
	Sumber Penggalian Data				
	Wawancara & Review Dokumen				
	Bukti Dokumen				
	Lampiran D-16, Foto G-17, dan Foto G-19				
Pengelolaan Strategi dan Program Keamanan Informasi					
4.17	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Dalam Penerapan / Diterapkan Sebagian	2

	Temuan				
	Strategi penerapan keamanan masih belum didefinisikan dengan baik				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-17				
4.18	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Terdapat divisi *research and development* namun belum spesifik ke manajemen risiko				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-18				
4.19	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Strategi penerapan keamanan informasi masih minim				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-19				

4.20	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Tidak Dilakukan	0
	Temuan				
	Audit masih belum berfokus pada keamanan informasi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-20				
4.21	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Tidak Dilakukan	0
	Temuan				
	Belum ada audit spesifik keamanan informasi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-21				
4.22	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0

	Temuan				
	Belum ada audit spesifik keamanan informasi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-22				
4.23	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0
	Temuan				
	Belum ada audit spesifik keamanan informasi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-23				
4.24	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Diterapkan Secara Menyeluruh	0
	Temuan				
	Ada analisa berdasarkan laporan				
	Sumber Penggalian Data				
	Wawancara				

	Bukti Dokumen				
	Lampiran Interview Protocol D-24				
4.25	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah diterapkan secara efektif?	Tidak Dilakukan	0
	Temuan				
	Belum ada analisa tingkat kepatuhan keamanan informasi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-25				
4.26	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Diterapkan Secara Menyeluruh	0
	Temuan				
	Terdapat program evaluasi 5 tahun sekali				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol D-26, dan Foto G-19				
Total Nilai Evaluasi Kerangka Kerja					**24**

Tabel 6.8 Mapping Kerangka Kerja Pengelolaan Informasi

Validitas Kerangka Kerja Pengelolaan Informasi							
Tingkat Kematangan I		**Tingkat Kematangan II**		**Tingkat Kematangan III**		**Tingkat Kematangan IV**	
Validitas	Yes	**Validitas**	No	**Validitas**	No	**Validitas**	No
Status	I+	**Status**	No	**Status**	No	**Status**	No
Status Akhir	**I+**						

Keterangan :

- Berdasarkan penilaian tersebut dapat dilihat pada Tabel 6.7 Skor Kerangka Kerja Pengelolaan Keamanan Informasi di STIE Perbanas Surabaya menunjukkan nilai 24 (dari skor maksimum 144) yang berarti masuk ke dalam kategori rendah.
- Untuk poin 4.24 pada Tabel 6.7 STIE Perbanas Surabaya telah melakukan analisa finansial secara berkala mengenai perubahan terhadap infrastruktur dan pengelolaan seperti ditunjukkan Foto G-18 dan G-24 pada lampiran.
- Untuk poin 4.26 Pihak STIE Perbanas mempunyai rencana strategis pengembangan teknologi informasi termasuk program peningkatan keamanan informasi dalam jangka menengah (5 tahun) yang direalisasikan secara konsisten seperti pada dokumen blueprint periode 2011-2015 seperti yang ditunjukkan Foto G-19 pada lampiran.
- Berdasarkan Tabel 6.7 sejumlah kebijakan dan prosedur kerja operasional, termasuk strategi penerapan, pengukuran efektifitas kontrol mayoritas masih belum diterapkan dan tidak diterapkan secara maksimal (status “Tidak Diterapkan” dan “Diterapkan Sebagian”).

- Perlu disusun kebijakan keamanan informasi yang meliputi aspek infrastruktur dan regulasi keamanan informasi yang mendetail, contohnya yang mencakup masalah-masalah non teknis seperti penggunaan password yang tidak sesuai yang menunjukan tidak adanya kepatuhan dalam menjalankan sistem keamanan informasi.

6.1.5. Pengelolaan Aset Informasi

Berikut ini merupakan hasil dari penilaian Pengelolaan Aset Informasi di STIE Perbanas Surabaya :

Tabel 6.9 Penilaian Pengelolaan Aset Informasi

No			Pertanyaan	Status	Skor
5.1	II	1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Terdapat daftar inventaris, namun masih kurang lengkap				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-1				
5.2	II	1	Apakah tersedia proses yang mengevaluasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Terdapat evaluasi namun untuk keperluan pengamanan masih kurang spesifik				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-2				

5.3	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Ada tingkatan akses namun belum ada suatu matrix tertentu				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-3				
5.4	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Perubahan konfigurasi dilakukan saat mendesak, namun untuk proses secara konsisten masih belum ada				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-4				
5.5	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Terdapat konfigurasi yang konsisten				
	Sumber Penggalian Data				
	Wawancara & Review Dokumen				
	Bukti Dokumen				
	Lampiran Interview Protocol E-5, Foto G-13, dan Foto G-14				

5.6	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Terdapat proses untuk merilis suatu aset baru				
	Sumber Penggalian Data				
	Wawancara & Review Dokumen				
	Bukti Dokumen				
	Lampiran Interview Protocol E-6, Foto G-18, dan Foto G-24				
Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?					
5.7	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Secara in-person sudah, namun tidak terdefinisi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-7				
5.8	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Secara in-person sudah, namun tidak terdefinisi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-8				
5.9	II	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Tidak Dilakukan	0

	Temuan				
	Belum ada tata tertib terkait HAKI				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-9				
5.10	II	1	Peraturan pengamanan data pribadi	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Secara in-person sudah, namun tidak terdefinisi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-10				
5.11	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Ada pengelolaan namun untuk kebijakan belum ada				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-11				
5.12	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Tidak Dilakukan	0
	Temuan				

	Kebijakan *username* masih belum ada				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-12				
5.13	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Tidak ada retensi data, namun jika ada karyawan yang berhenti maka akunnya akan dihapus				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-13				
5.14	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Belum ada pertukaran data yang melibatkan pihak eksternal hanya kepada pihak DIKTI				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-14				
5.15	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Proses penyelidikan hanya bersifat insidensial				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-15				

5.16	II	1	Prosedur *back-up* ujicoba pengembalian data (*restore*)	Diterapkan Secara Menyeluruh	3
	Temuan				
	Proses *back-up* dilakukan setiap hari				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran E-16, Foto G-8, dan Foto G-10				
5.17	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Diterapkan Secara Menyeluruh	6
	Temuan				
	Pengamanan aset telah dilakukan				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol E-17, dan Foto G-9				
5.18	III	2	Proses pengecekan latar belakang SDM	Dalam Penerapan / Diterapkan Sebagian	4
	Temuan				
	Proses pengecekan masih belum spesifik				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-18				
5.19	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Tidak Dilakukan	0

	Temuan				
	Tidak ada pelaporan insiden terhadap pihak eksternal ataupun pihak yang berwajib				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-19				
5.20	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Tidak Dilakukan	0
	Temuan				
	Tidak ada retensi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-20				
5.21	III	2	Prosedur kajian penggunaan akses (*user access review*) dan langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku.	Dalam Penerapan / Diterapkan Sebagian	4
	Temuan				
	Akses sudah diatur, namun tidak ada dokumen tertulis				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-21				
5.22	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Dalam Penerapan / Diterapkan Sebagian	6

	Temuan				
	Tidak ada daftar spesifik namun dilakukan backup untuk seluruh data				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-22				
5.23	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Dalam Penerapan / Diterapkan Sebagian	6
	Temuan				
	Terdapat log namun kurang mendetail, namun untuk klasifikasi hak akses telah dilakukan. ()				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-23, dan Foto G-15				
5.24	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Dalam Penerapan / Diterapkan Sebagian	6
	Temuan				
	Belum ada prosedur khusus terhadap hubungan dengan pihak ketiga				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-24				

Pengamanan Fisik					
5.25	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Terdapat pengamanan yang cukup memadai				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran E-25, Foto G-7, dan Foto G-8				
5.26	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Ada alokasi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-26, dan Foto G-7				
5.27	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Terdapat perlindungan yang memadai				
	Sumber Penggalian Data				
	Wawancara				

	Bukti Dokumen				
	Lampiran Interview Protocol E-27, Foto G-1, Foto G-2, Foto G-3, Foto G-4, Foto G-5, dan Foto G-6				
5.28	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Terdapat genset dan penangkal petir				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-28				
5.29	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Tidak Dilakukan	0
	Temuan				
	Belum ada peraturan resmi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-29				

5.30	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Diterapkan Secara Menyeluruh	6
	Temuan				
	Terdapat fasilitas pendukung yang ditempatkan di beberapa titik				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-30, Foto G-1, Foto G-2, Foto G-3, Foto G-4, Foto G-5, dan Foto G-6				
5.31	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Diterapkan Secara Menyeluruh	6
	Temuan				
	Maintenance dilakukan secara rutin				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-31, Foto G-20, dan Foto G-21				

5.32	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	4
	Temuan				
	Untuk aturan ada namun untuk kebijakan tertulis belum ada				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-32				
5.33	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Diterapkan Secara Menyeluruh	6
	Temuan				
	Terdapat beberapa prosedur permintaan				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-33, dan Foto G-22				

5.34	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Diterapkan Secara Menyeluruh	9
	Temuan				
	Terdapat satuan pengamanan (Satpam)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol E-34, dan Foto G-7				
Total Nilai Evaluasi Pengelolaan Aset					**106**

Tabel 6.10 Mapping Pengelolaan Aset Informasi

Validitas Pengelolaan Aset Informasi							
Tingkat Kematangan I		**Tingkat Kematangan II**		**Tingkat Kematangan III**		**Tingkat Kematangan IV**	
Validitas	Yes	**Validitas**	Yes	**Validitas**	No	**Validitas**	No
Status	I	**Status**	II	**Status**	No	**Status**	No
		Status Akhir	**II**				

Keterangan :

- Berdasarkan penilaian tersebut dapat dilihat Skor Pengelolaan Aset Informasi di STIE Perbanas Surabaya menunjukkan nilai 106 (dari skor maksimum 153) dan mencapai Tingkat Kematangan II.
- Untuk aspek pengelolaan aset informasi secara umum sudah cukup baik seperti terdapat form pemeriksaan aset secara berkala seperti pada Foto G-20 s/d G-21 dan form permintaan website seperti pada Foto G-22.

- Perlu peningkatan pada beberapa poin seperti untuk poin 3.29 mengenai regulasi perangkat diluar instansi dan poin 5.32 mekanisme pemindahan data kepada pihak ketiga, namun untuk aspek pengamanan seputar infrastruktur di STIE Perbanas seperti lokasi kerja, akses pintu masuk, pengamanan fisik, aktivitas inspeksi, peraturan mayoritas telah "Diterapkan Secara Menyeluruh" seperti ditunjukkan pada Foto G-1 s/d G-9 dan G-20 s/d G-21.
- Perlu disusun kebijakan pengelolaan keamanan aset informasi yang meliputi aspek infrastruktur dan regulasi keamanan informasi yang mendetail, contohnya yang mencakup masalah-masalah non teknis seperti penggunaan password yang tidak sesuai yang menunjukan tidak adanya kepatuhan dalam menjalankan sistem keamanan informasi.

6.1.6. Teknologi dan Keamanan Informasi

Berikut ini merupakan hasil dari penilaian Teknologi dan Keamanan Informasi di STIE Perbanas Surabaya:

Tabel 6.11 Penilaian Teknologi dan Keamanan Informasi

No			Pertanyaan	Status	Skor
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Terdapat *firewall* dan otorisasi akses				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-1				

6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Terdapat segmentasi				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-2				
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Terdapat konfigurasi namun belum mencakup keseluruhan keamanan perangkat				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-3				
6.4	II	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Belum dilakukan secara rutin				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-4				

6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Perencanaan	1
	Temuan				
	Tidak dilakukan, dan masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-5, Foto G-19				
6.6	II	1	Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Terdapat evaluasi penjaminan mutu				
	Sumber Penggalian Data				
	Wawancara & Review Dokumen				
	Bukti Dokumen				
	Lampiran Interview Protocol F-6, dan Foto G-17				
6.7	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Dalam Penerapan / Diterapkan Sebagian	2
	Temuan				
	Informasi yang ada dalam log kurang spesifik				
	Sumber Penggalian Data				
	Wawancara & Review Dokumen				

	Bukti Dokumen				
	Lampiran Interview Protocol F-7, dan dan Foto G-19				
6.8	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Dalam Perencanaan	1
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol F-8, dan Foto G-19				
6.9	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Log dianalisis				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol F-9, Foto G-15, dan Foto G-19				
6.10	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Penggunaan enkripsi md5 pada database				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-10				

6.11	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Tidak Dilakukan	0
	Temuan				
	Tidak ada standar enkripsi yang digunakan				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-11				
6.12	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Diterapkan Secara Menyeluruh	6
	Temuan				
	Enkripsi md5 digunakan pada database yang berisi *password*				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-12				
6.13	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Dalam Penerapan / Diterapkan Sebagian	4
	Temuan				
	Pergantian password masih *by case*				
	Sumber Penggalian Data				
	Wawancara				

	Bukti Dokumen				
	Lampiran Interview Protocol F-13				
6.14	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Diterapkan Secara Menyeluruh	6
	Temuan				
	Terdapat beberapa lapis keamanan sistem				
	Sumber Penggalian Data				
	Wawancara & Obsevasi				
	Bukti Dokumen				
	Lampiran Interview Protocol F-14, Foto G-7, dan Foto G-8				
6.15	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	Diterapkan Secara Menyeluruh	6
	Temuan				
	Terdapat *session* pada sistem				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-15				
6.16	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Diterapkan Secara Menyeluruh	6
	Temuan				
	Terdapat *id* dan *password* akses				

	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-16				
6.17	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Dalam Perencanaan	1
	Temuan				
	Belum ada, masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-17, dan Foto G-19				
6.18	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Menggunakan versi terbaru				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-18				
6.19	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Diterapkan Secara Menyeluruh	3
	Temuan				
	Terdapat antivirus berlisensi				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol F-19, dan Foto G-11				

6.20	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis?	Diterapkan Secara Menyeluruh	6
	Temuan				
	Antivirus diperbaharui secara rutin				
	Sumber Penggalian Data				
	Wawancara & Observasi				
	Bukti Dokumen				
	Lampiran Interview Protocol F-20, dan Foto G-11				
6.21	III	2	Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak Dilakukan	0
	Temuan				
	Belum ada prosedur pelaporan terkait penyerangan virus				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-21				
6.22	III	2	Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Diterapkan Secara Menyeluruh	6
	Temuan				
	Masing-masing sistem informasi menggunakan standar waktu yang sama				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-22				

6.23	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba?	Tidak Dilakukan	0
	Temuan				
	Tidak ada spesifikasi khusus yang digunakan				
	Sumber Penggalian Data				
	Wawancara				
	Bukti Dokumen				
	Lampiran Interview Protocol F-23				
6.24	IV	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Dalam Perencanaan	3
	Temuan				
	Belum ada kerja sama pihak independen, dan masih dalam tahap perencanaan (blueprint)				
	Sumber Penggalian Data				
	Wawancara & Review Dokumen				
	Bukti Dokumen				
	Lampiran Interview Protocol F-24, dan Foto G-19				
Total Nilai Evaluasi Teknologi dan Keamanan Informasi					**73**

Tabel 6.12 Mapping Teknologi dan Keamanan Informasi

Validitas Teknologi dan Keamanan Informasi							
Tingkat Kematangan I		**Tingkat Kematangan II**		**Tingkat Kematangan III**		**Tingkat Kematangan IV**	
Validitas	Yes	**Validitas**	Yes	**Validitas**	No	**Validitas**	No
Status	I	**Status**	II	**Status**	No	**Status**	No
		Status Akhir	**II**				

Keterangan :

- Berdasarkan penilaian tersebut dapat dilihat Skor Teknologi dan Keamanan Informasi di STIE Perbanas Surabaya menunjukkan nilai 73 (dari skor maksimum 108) dan mencapai Tingkat Kematangan II.
- Untuk jaringan komunikasi di STIE Perbanas telah disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll) seperti pada lampiran Foto G-13, G-14, dan G-23.
- Untuk infrastruktur TI di STIE Perbanas dilakukan pemeriksaan aset secara berkala seperti pada Foto G-20 s/d G-21.
- Setiap perubahan dalam sistem informasi terekam dalam log seperti pada Foto G-15.
- Terdapat antivirus yang diperbaharui secara berkala seperti pada Foto G-11.
- STIE Perbanas Surabaya perlu melakukan pemindaian secara rutin seputar jaringan dan celah keamanan informasi, serta melakukan kerja sama dari pihak independen untuk mengkaji kehandalan keamanan informasi yang diterapkan.

6.2. Pembahasan

Berikut ini akan dibahas mengenai hasil analisis secara keseluruhan lima area keamanan informasi pada STIE Perbanas Surabaya.

6.2.1. Analisis Hasil Penilaian Indeks KAMI

Berdasarkan hasil penilaian skor per bagian, berikut ini merupakan analisis hasil tingkat kematangan untuk seluruh area berasarkan tingkat validitas skor dapat dilihat pada Tabel 6.13.

Tabel 6.13 Mapping Validitas Skor 5 Aspek Indeks KAMI

Validitas	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
Tingkat Kematangan I					
Validitas	Yes	No	Yes	Yes	Yes
Status	I+	No	I+	I	I
Tingkat Kematangan II					
Validitas	No	No	No	Yes	Yes
Status	No	No	No	II	II
Tingkat Kematangan III					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Tingkat Kematangan IV					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Status Akhir	**I+**	**I**	**I+**	**II**	**II**

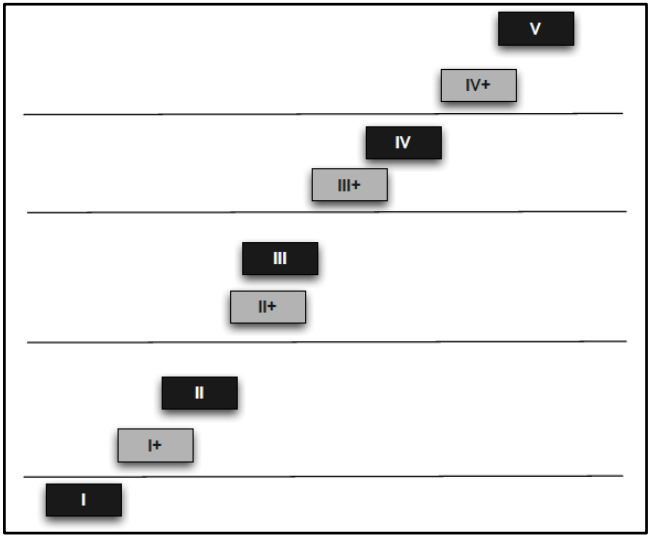
Untuk tingkat validitas disini bukan untuk menunjukkan valid atau tidaknya data, namun untuk menunjukkan valid atau tidaknya skor untuk menuju tingkat kematangan selanjutnya.

Berdasarkan Tabel 6.13 dapat dilihat bahwa Skor Pengelolaan Risiko tidak mencapai Tingkat Validitas Kematangan I, diikuti dengan area Tata Kelola dan area Kerangka Kerja yang mencapai Tingkat Validitas Kematangan I+ yang berarti mencapai Tingkat Kematangan I namun tidak cukup mencapai Tingkat Kematangan II, kemudian area dengan Tingkat Kematangan tertinggi yaitu area Teknologi Keamanan Informasi, dan area Pengelolaan Aset mencapai Tingkat Validitas Kematangan II.

Tabel 6.14 Mapping Total Skor 5 Aspek Indeks KAMI

Indeks KAMI	Skor	Tingkat Kematangan
Bagian II: Tata Kelola Keamanan Informasi	32	I+
Bagian III: Pengelolaan Risiko Keamanan Informasi	17	I
Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi	24	I+
Bagian V: Pengelolaan Aset Informasi	106	II
Bagian VI: Teknologi dan Keamanan Informasi	73	II
Total Skor (II+III+IV+V+VI)	252	I s/d II

Pada Tabel 6.14 menunjukkan hasil pengukuran tingkat kematangan keamanan informasi untuk Bagian II , III, IV dan V dan VI di STIE Perbanas Surabaya. Untuk penjelasan urutan peringkatan pada tabel di atas, urutan terendah adalah I, sedangkan yang paling tinggi adalah V, seperti pada Gambar 6.1.



Gambar 6.1 Urutan Tingkat Keamanan Informasi

Tabel 6.15 Mapping Seluruh Aspek Dengan Status Kesiapan

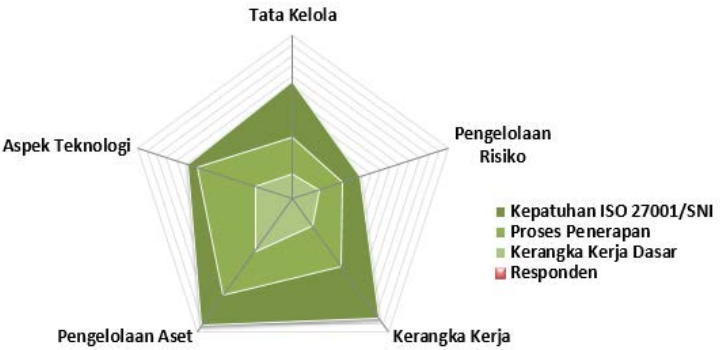
Peran TIK					
Skor Bagian I			Skor Bagian II+III+IV+V+VI		Status Kesiapan
0	12	Rendah	0	124	Tidak Layak
			125	272	Perlu Persiapan
			273	588	Baik/Cukup
13	24	Sedang	0	174	Tidak Layak
			175	312	Perlu Persiapan
			313	588	Baik/Cukup
25	36	Tinggi	0	272	Tidak Layak
			273	392	Perlu Persiapan
			393	588	Baik/Cukup
37	48	Kritis	0	333	Tidak Layak
			334	453	Perlu Persiapan
			454	588	Baik/Cukup

Tabel 6.15 menunjukkan pemetaan antara seluruh bagian Indeks KAMI dimana semakin tinggi ketergantungan terhadap TIK atau semakin penting peran TIK terhadap tugas instansi tersebut, maka semakin banyak pula bentuk pengamanan yang diperlukan.

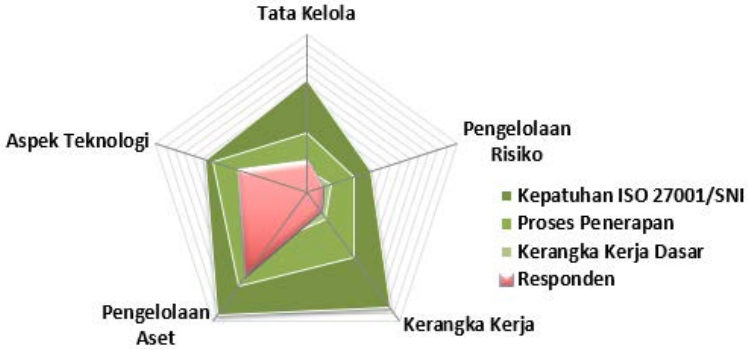
Kemudian selanjutnya akan ditampilkan diagram radar. Diagram radar merupakan metode grafis berbentuk grafik dua dimensi yang menggambarkan data multivarian, dimana tiga atau lebih variabel kuantitatif digambarkan dalam bentuk sumbu yang dimulai dari titik yang sama. Grafik radar terdiri dari jari-jari yang mewakili nilai satu variabel. Panjang dari jari-jari tersebut menggambarkan besarnya nilai variabel. Jari-jari tersebut kemudian dihubungkan dengan garis, sehingga membentuk plot yang berbentuk radar. Diagram radar ini digunakan untuk memudahkan dalam mengamati suatu pemisahan logis antara variabel-variabel yang akan dibandingkan. Dalam diagram ini terlihat karakteristik objek terhadap variabel-variabel yang ada. Kemudian pada grafik

radar ketika salah satu grafik lebih besar dari yang lain pada beberapa variabel maka grafik yang ditampilkan tersebut hanya menggambarkan deskripsi bukan untuk menggambarkan kesimpulan. Diagram radar pada gambar berikut menunjukkan sejauh mana kelengkapan pengamanan sudah mendekati atau mencapai tingkat kelengkapan yang diharapkan.

Berikut ini adalah tampilan dari diagram radar Indeks KAMI:



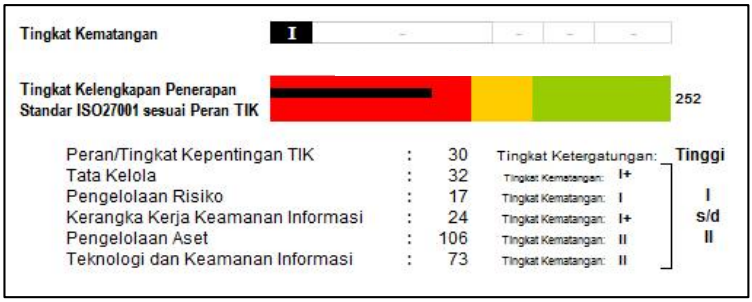
Gambar 6.2 Diagram Radar Sebelum Dilakukan Penilaian



Gambar 6.3 Diagram Radar Setelah Dilakukan Penilaian

Diagram radar pada Gambar 6.2 dan 6.3 merupakan bentuk gambaran visual keseluruhan dari serangkaian penilaian yang telah dilakukan dengan menggunakan Indeks KAMI. Nilai dari masing-masing area ditampilkan dalam area merah. Dalam diagram tersebut bisa dilihat perbandingan antara kondisi kesiapan sebagai hasil dari proses evaluasi dengan acuan tingkat kelengkapan yang ada. Dalam diagram radar, latar belakang area menunjukkan ambang batas tingkat kelengkapan (kategori) I s/d III (hijau muda s/d hijau tua) Indeks KAMI.

Berdasarkan diagram radar pada Gambar 6.3 dapat dilihat bahwa perolehan nilai Tingkat Kematangan terkecil dari seluruh skor pada area Pengelolaan Risiko, diikuti dengan area Kerangka Kerja, area Tata Kelola, area Teknologi Keamanan Informasi, dan area Pengelolaan Aset.



Gambar 6.4 Keamanan Informasi Di STIE Perbanas Surabaya

Untuk nilai masing-masing area dirangkum dalam Gambar 6.4 menunjukkan seberapa besar tingkat kelengkapan masing-masing area yang telah dicapai pada STIE Perbanas Surabaya.

Status Kelengkapan yang ditampilkan oleh instrumen *Bar Chart* pada Gambar 6.4 menunjukkan bahwa pencapaian masih berada di area berwarna merah dan masih dalam status

kesiapan ***"Tidak Layak"*** dengan total jumlah nilai kelengkapan ***252*** sehingga masih belum sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2009. Untuk area berwarna merah masih dalam status kesiapan "Tidak Layak", kemudian pencapaian di area warna kuning masih "Memerlukan Perbaikan", sedangkan pencapaian warna hijau menunjukkan bahwa status kesiapan sudah "Baik/Cukup".

Gambar 6.4 juga menunjukkan bahwa tingkat kematangan keamanan informasi di STIE Perbanas Surabaya masih belum cukup bagus, yang bisa dilihat dari gambar mencapai tingkat kematangan I namun masih belum mencapai tingkat kematangan II.

Gambar 6.5 *Range* Kematangan Indeks KAMI

Selanjutnya Gambar 6.5 merupakan gambar tingkat kematangan berurutan dari tingkatan yang terendah hingga tertinggi. Kemudian diketahui batasan minimal yang harus dicapai untuk dapat melakukan sertifikasi ISO 27001.

Tabel 6.16 Karakteristik Tingkat Keamanan I

Tingkat I – Kondisi Awal (Reaktif)
✓ Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi.
✓ Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan.
✓ Kelemahan teknis dan non-teknis tidak teridentifikasi dengan baik.
✓ Pihak yang terlibat tidak menyadari tanggung jawab mereka.

Berdasarkan hasil yang didapatkan pada analisis yang telah dilakukan sebelumnya maka disimpulkan tingkat keamanan informasi di STIE Perbanas Surabaya digolongkan pada Tingkat I (Pertama) – Kondisi Awal (Reaktif) dengan karakteristik yang telah dijelaskan pada Tabel 6.16. Sedangkan batasan minimal yang harus dicapai untuk dapat melakukan sertifikasi ISO adalah III.

6.2.2. Rekomendasi Perbaikan 5 Area Pengamanan

Berdasarkan analisis yang telah dilakukan, berikut ini merupakan saran secara singkat yang diberikan untuk meningkatkan kelima area pengamanan Indeks Keamanan Informasi (KAMI):

a) Rekomendasi Area Tata Kelola

- Meningkatkan dan memperbaiki beberapa kelemahan dalam sistem manajemen tata kelola keamanan informasi di STIE Perbanas.
- Menyusun suatu Dokumen Kebijakan Keamanan Informasi secara formal yang kemudian dipublikasikan dan dikomunikasikan kepada seluruh staff maupun pihak-pihak yang terkait, yang kemudian melakukan pengawasan, monitoring dan evaluasi rutin secara berkala.
- Meningkatkan kesadaran terhadap keamanan informasi kepada semua pihak yang terlibat baik itu dengan mengadakan sosialisasi, pelatihan, sertifikasi, dll.

b) Rekomendasi Area Pengelolaan Risiko

- Menyusun dan menerapkan Sistem/Program Manajemen Risiko dan Keamanan Informasi.
- Menyusun Disaster Recovery Planning (DRP) dalam rangka meminimumkan risiko dan mempersiapkan pihak internal secara optimal dalam menghadapi ancaman dan bencana.

c) Rekomendasi Area Kerangka Kerja

- Membenahi perangkat pengelolaan keamanan informasi seperti adanya standar manajemen keamanan informasi (SMKI), kebijakan, prosedur hingga pengendalian kontrol seperti formulir dan checklist.
- Untuk pengelolaan keamanan informasi masih perlu adanya perbaikan dalam memenuhi standarisasi ISO/IEC 27001:2005 terlebih pada dokumentasi kerangka kerja keamanan informasi.

d) Rekomendasi Area Pengelolaan Aset

- Menyusun dan menerapkan prosedur pengelolaan aset informasi
- Melakukan kajian mengenai perencanaan finansial (investasi) serta evaluasi kelayakan sistem baru yang nantinya akan diimplementasikan.

e) Rekomendasi Area Teknologi

- Menetapkan konfigurasi standar untuk keamanan sistem bagi keseluruhan sistem bagi keseluruhan aset informasi dan perangkat jaringan.

Lampiran A
Angket Mengenai Peran Dan Tingkat Kepentingan TIK Pada STIE Perbanas Surabaya

Hari/Tanggal : **Kamis, 14 April 2016**
Pukul : **13:00**
Lokasi : **Kampus 2 STIE Perbanas Surabaya**
Pewawancara : **Radhifan Hidayat**
Narasumber : **Hariadi Yutanto, S.Kom, M.Kom (Kasie TIK)**

Lampiran ini berisikan form wawancara yang digunakan untuk pendokumentasian dan penjelasan program, aktivitas bisnis, struktur organisasi, dan tupoksi. Berikut ini merupakan lampiran tersebut:

No	Pertanyaan & Jawaban
1.	Total anggaran tahunan yang dialokasikan untuk TIK? Jawaban: • Minim - Kurang dari Rp. 1 Milyard • ***Rendah - Rp. 1 Milyard sampai dengan Rp. 3 Milyard*** • Sedang - Rp. 3 Milyard sampai dengan Rp 8 Milyard • Tinggi - Rp. 8 Milyard sampai dengan Rp. 20 Milyard • Kritis - Rp. 20 Milyard atau lebih
2.	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK? Jawaban: • Minim - Kurang dari 60 • Rendah - 60 sampai dengan 120 • **Sedang - 120 sampai dengan 240** • Tinggi - 240 sampai dengan 600 • Kritis - 600 atau lebih

3.	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok dan Fungsi Instansi anda? Jawaban: • Minim Hanya digunakan untuk mempermudah sejumlah kecil pekerjaan rutin, pencatatan, penyimpanan salinan dokumen, dll. • Rendah Digunakan untuk menunjang kegiatan rutin • Sedang Digunakan untuk membantu penyelenggaraan layanan publik atau tugas utama instansi • Tinggi Digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi • ***Kritis*** ***Digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi yang bersifat nasional dan strategis***
4.	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda? Jawaban: • Minim Tidak ada atau sedikit sekali - proses kerja sistem/aplikasi yang bersifat umum dan penyimpanan data publik • Rendah Ada sejumlah proses kerja sistem/aplikasi yang spesifik sesuai tugas instansi dan data/informasi yang bisa didapatkan dari tempat lain • ***Sedang*** ***Ada sejumlah proses kerja sistem/aplikasi yang sangat spesifik dan data/informasi yang sulit didapatkan dari tempat lain***

	• Tinggi Proses kerja sistem/aplikasi merupakan aset nasional dan data/ informasi penting berskala nasional • Kritis Proses kerja sistem/aplikasi yang merupakan rahasia negara dan data/informasi penting yang bersifat strategis
5.	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda? Jawaban: • Minim Tidak ada dampak terhadap kinerja karena hanya digunakan untuk mempermudah sejumlah kecil pekerjaan rutin, pencatatan, penyimpanan salinan dokumen, dll. • Rendah Agak mengganggu kinerja karena digunakan untuk menunjang kegiatan rutin. • Sedang Berdampak pada tingkat layanan masyarakat karena digunakan untuk membantu penyelenggaraan layanan publik atau tugas utama instansi • ***Tinggi*** ***Mengganggu tersedianya layanan masyarakat karena digunakan sebagai komponen utama penyelenggaraan layanan publik dan tugas utama instansi, sulit untuk digantikan proses manual.*** • Kritis Tidak tersedianya layanan masyarakat karena digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi yang bersifat nasional dan strategis.

6.	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda? Jawaban: • Minim Sistem beroperasi secara individu, tidak terkait dengan sistem lainnya • Rendah Sistem beroperasi secara terintergasi dengan sistem lainnya, tetapi ketersediaannya tidak mengganggu fungsi sistem lain tersebut. • Sedang Sistem beroperasi secara terintergasi dengan sistem lainnya, gangguan ketersediaan akan mengganggu sistem lain tersebut. • ***Tinggi*** ***Sistem harus beroperasi secara terintergasi dengan sistem lainnya, dan gangguan ketersediaan akan sangat mengganggu sistem lain tersebut.*** • Kritis Sistem merupakan bagian/komponen penting dari sistem lainnya, dan gangguan ketersediaan mengganggu layanan yang berskala nasional
7.	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi pemerintah lainnya atau terhadap ketersediaan sistem pemerintah berskala nasional? Jawaban: • Minim Tidak ada dampak apapun • Rendah Dampaknya tidak berarti, hanya mengakibatkan terganggunya ketersediaan sejumlah kecil data/proses umum • Sedang Gangguan yang dapat menghambat pekerjaan atau

	layanan publik, hilangnya data/informasi publik dengan jumlah yang cukup besar • ***<u>Tinggi</u>*** ***<u>Gangguan terhadap layanan publik yang bersifat nasional, hilangnya data publik dalam jumlah sangat besar</u>*** • Kritis Gangguan terhadap layanan publik yang bersifat strategis, terkait data/informasi rahasia milik negara
8.	Tingkat sensitifitas pengguna sistem TIK di Instansi anda? Jawaban: • Minim Tidak peduli - jarang menggunakan • Rendah Membutuhkan layanan TIK, tetapi mudah mencari alternatif lain • Sedang Membutuhkan layanan TIK untuk menunjang pekerjaan rutin • Tinggi Sangat membutuhkan layanan TIK untuk tugas utama • ***<u>Kritis</u>*** ***<u>Sangat membutuhkan layanan TIK untuk menjalankan tugas instansi</u>***
9.	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya? Jawaban: • Minim Tidak ada kaitannya dengan kepatuhan terhadap Kebijakan, Peraturan/UU • ***<u>Rendah</u>*** ***<u>Ada sejumlah Kebijakan yang harus diikuti dalam</u>***

	penyelenggaraan layanan menggunakan sistem ini • Sedang Proses kerja sistem/aplikasi harus mematuhi sejumlah Kebijakan dan Peraturan internal atau eksternal • Tinggi Proses kerja sistem/aplikasi harus mengikuti Peraturan dan UU • Kritis Proses kerja sistem/aplikasi harus mematuhi sejumlah UU dan perangkat hukum terkait
10.	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda? Jawaban: • Minim Tidak ada dampak apapun • Rendah Dampaknya tidak signifikan, hanya mengakibatkan terganggunya atau terungkapnya sejumlah kecil data atau kegiatan/program kerja umum • Sedang Terungkapnya informasi yang sangat mengganggu program kerja, hilangnya data/informasi publik dengan jumlah yang cukup besar • ***Tinggi*** ***Terungkapnya informasi sensitif atau terbatas yang dapat berakibat pada gagalnya program kerja atau mengganggu kinerja/kredibilitas pemerintah*** • Kritis Hilangnya aset informasi penting berskala nasional atau terungkapnya informasi rahasia terkait keamanan negara

11.	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK? Jawaban: • Minim Sistem dapat dioperasikan sendiri dengan teknologi yang mudah ditemui di pasaran • Rendah Sistem dapat dioperasikan sendiri dengan dukungan teknisi eksternal, teknologi dengan spesifikasi yang tidak umum • ***Sedang*** ***Sistem harus dioperasikan dengan dukungan teknis dari pihak eksternal, teknologi dengan spesifikasi yang cukup spesifik*** • Tinggi Sistem tidak dapat dioperasikan tanpa dukungan teknis dari pihak eksternal, teknologi dengan spesifikasi yang sangat spesifik • Kritis Sistem hanya dapat dioperasikan dengan dukungan teknis dari pihak eksternal tertentu, teknologi dengan spesifikasi tinggi dan ketersediaan perangkat yang sangat terbatas
12.	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi? Jawaban: • Minim Hanya digunakan sebagai penunjang pekerjaan rutin (pencatatan, penyimpanan salinan dokumen umum, dll) - sistem relatif bersifat terbuka • Rendah Digunakan untuk menunjang sejumlah kegiatan tugas pokok, sistem hanya digunakan secara internal organisasi

	• ***Sedang*** ***Digunakan untuk membantu penyelenggaraan layanan publik atau tugas utama instansi, sistem digunakan secara internal dan terbatas*** • Tinggi Digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi, akses ke fungsi administrasi sistem atau basis data dibatasi untuk yang mempunyai wewenang • Kritis Digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi yang bersifat nasional dan strategis, akses ke fungsi administrasi sistem atau basis data dibatasi secara ketat, dengan wewenang dan pemantauan khusus

Lampiran B
Interview Protocol Mengenai Tata Kelola Keamanan Informasi di STIE Perbanas Surabaya

Hari/Tanggal	**: Kamis, 14 April 2016**
Pukul	**: 13:00**
Lokasi	**: Kampus 2 STIE Perbanas Surabaya**
Pewawancara	**: Radhifan Hidayat**
Narasumber	**: Hariadi Yutanto, S.Kom, M.Kom (Kasie TIK)**

Lampiran ini berisi pertanyaan dan jawaban untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi di STIE Perbanas Surabaya. Berikut ini merupakan form lampiran tersebut:

1. Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?

   Jawaban:
   Untuk masalah koordinasi, pimpinan selalu berkoordinasi terutama untuk masalah kebijakan yang akan diterapkan kedepannya, terutama yang akan dibahas pada rapat per semester, namun masalah spesifik keamanan informasi belum ada dan masih dalam perencanaan (*blueprint).*

2. Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?

Jawaban:
Untuk pengelolaan keamanan informasi merupakan tanggung jawab dari Divisi ICT internal, namun untuk peraturan tertulis sendiri belum ada dan masih dalam perencanaan (*blueprint)*.

3. Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?

Jawaban:
Untuk wewenang sendiri ada, namun untuk kebijakan yang mengatur secara detail masih dalam tahap penyusunan (*blueprint)*.

4. Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?

Jawaban:
Mengenai alokasi anggaran mengenai keamanan informasi sendiri nantinya akan direncanakan seiring dengan penyusunan (*blueprint)*.

5. Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?

Jawaban:
Selama ini STIE Perbanas belum berfokus disitu (pengamanan informasi), namun untuk spesifik ke-

-manajemen ada auditnya, tapi belum berfokus pada audit internal pada fokus spesifik seperti IT atau keamanan informasi, IT hanya secara umumnya saja, tapi secara khususnya belum seperti yang benar-benar berfokus pada IT security seperti ISO 27001 dll. Masih belum, sementara ini masih menggunakan ISO Quality Management 9001, namun untuk kedepannya STIE Perbanas ada rencana untuk melakukan peningkatan.

6. Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?

Jawaban:
Untuk persyaratan/standar spesifik yang mengacu pada keamanan informasi masih belum, secara jobdesk mengikuti tupoksi di jobdesk yang ditugaskan, tapi untuk kriteria keahlian khusus masih belum terdefinisi.

7. Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?

Jawaban:
Untuk kompetensi dan keahlian relatif sedang, karena belum ada penetapan standar yang menjadi acuan

8. Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?

Jawaban:
Untuk pelaksanaan sosialisasi yang dikumpulkan secara massal belum, tapi sosialisasi secara door-to-door sudah

maksudnya sosialiasasi secara personal ke unit kerja untuk menjaga password dsb. Itu sudah, tapi untuk sosialiasi skala besar dan dikumpulkan semua itu belum, tentang pentingnya keamanan itu belum

9. Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?

Jawaban:
Peningkatan kompetensi seperti pelatihan, seminar, workshop, sosialisasi tentang teknologi terkini ada diterapkan secara berkala pada waktu tertentu.

10. Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?

Jawaban:
Belum lama ini untuk pertama kalinya terjadi kejadian *hacking* dan *deface*, dan pada saat itu semua pihak yang terkait dikumpulkan, dan diminta klarifikasi, satu per satu diminta untuk melakukan *trace* darimana sumbernya, terus kurangnya apa, kendalanya apa, kendalanya dimana, kemudian setelah itu dicari solusinya dari masalah tersebut.

11. Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi?

Jawaban:
Terkait dengan keamanan informasi dan kaitannya dengan pihak eksternal, untuk selama ini belum dan baru kali ini dibantu dangan beberapa mahasiswa memberikan masukkan mengenai pentest (penetration testing) mengenai celah keamanan di dalam sistem STIE Perbanas Surabaya sendiri.

12. Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) sudah didefinisikan dan dialokasikan?

Jawaban:
Terdapat *blueprint* yang sedang disusun untuk periode 2016-2020 namun masih dalam tahapan penyusunan untuk saat ini, sebelumnya sebenarnya juga sudah ada blueprint yaitu untuk tahapan 2010-2015, untuk DRP juga dalam penyusunan, selanjutnya tahun ini ditargetkan akan selesai.

13. Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?

Jawaban:
Untuk laporan resmi ada dua yang terbagi dalam laporan semester dan laporan tahunan, khusus untuk aspek pengelolaan keamanan informasi sendiri hanya dilakukan pelaporan secara insidentil atau jika terjadi suatu insiden yang membutuhkan suatu perhatian khusus.

14. Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?

Jawaban:
Setelah insiden yang terjadi beberapa waktu lalu masalah keamanan menjadi poin penting, setelah terjadi insiden baru menjadi pertimbangan, walaupun dalam gambaran keseluruhannya masih belum jelas, namun untuk gambarannya tahun ini pengembangan di fokuskan ke arah infrastruktur, tahun depan akan berfokus pada *disaster*, tahun ke tiga akan membahas masalah *security*. Karena ada pembangunan kampus dan juga kemaren ruang server juga ada kebakaran juga, jadi langkah selanjutnya pihak STIE Perbanas Surabaya membenahi infrastruktur (server yang terbakar dsb.), disaat infrastruktur di benahi itu ada hack masuk, setelah itu untuk menanggulangi hack juga masih membenahi infrastruktur dan kemudian dilanjutkan dengan fokus penyusunan disaster recovery plan, kemudian di tahun ke tiga di rencanakan STIE Perbanas akan berfokus *pure* pada *security*.

15. Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?

Jawaban:
Untuk aspek pengamanan informasi sampai saat ini masih belum ada program khusus, dalam perencanaan.

16. Apakah Instansi anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi?

Jawaban:
Untuk pendefinisiannya masih belum ada, namun sudah ada perencanaan penyusunan untuk kedepannya.

17. Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?

Jawaban:
Program penilaian pengamanan informasi masih belum ada, hanya penilaian pegawai yang diselenggarakan secara internal, penilaian berbasis kompetensi PA (Personal Appraisal).

18. Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi?

Jawaban:
Untuk pendefinisiannya masih belum ada, namun sudah ada perencanaan penyusunan untuk kedepannya.

19. Apakah Instansi anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?

Jawaban:
Untuk undang-undang atau perangkat hukum terkait pengamanan informasi hanya sekedar mengetahui saja, kemudian untuk tahapan implementasi masih belum berjalan secara maksimal.

20. Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?

Jawaban:
Di STIE Perbanas Surabaya sendiri untuk kebijakan keamanan informasi spesifik menyangkut pelanggaran hukum masih belum ada. namun sudah ada perencanaan penyusunan untuk kedepannya.

Lampiran C
Interview Protocol Mengenai Pengelolaan Risiko Keamanan Informasi di STIE Perbanas Surabaya

Hari/Tanggal	**: Kamis, 14 April 2016**
Pukul	**: 13:00**
Lokasi	**: Kampus 2 STIE Perbanas Surabaya**
Pewawancara	**: Radhifan Hidayat**
Narasumber	**: Hariadi Yutanto, S.Kom, M.Kom (Kasie TIK)**

Lampiran ini berisi pertanyaan dan jawaban untuk mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi di STIE Perbanas Surabaya. Berikut ini merupakan form lampiran tersebut:

1. Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?

   Jawaban:
   Sampai saat ini belum ada standar atau program kerja mengenai pengelolaan risiko secara umum maupun yang spesifik mengenai keamanan informasi.

2. Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?

   Jawaban:
   Belum ada.

3. Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi,

tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?

Jawaban:
Belum ada.

4. Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?

Jawaban:
Belum ada.

5. Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?

Jawaban:
Belum ada.

6. Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?

Jawaban:
Belum ada.

7. Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?

Jawaban:
Belum ada.

8. Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?

Jawaban:
Belum ada.

9. Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?

Jawaban:
Belum ada.

10. Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?

Jawaban:
Belum ada.

11. Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?

Jawaban: Belum ada.

12. Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya?

Jawaban: Belum ada.

13. Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?

Jawaban: Belum ada.

14. Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?

Jawaban: Belum ada.

15. Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?

Jawaban: Belum ada.

Lampiran D
Interview Protocol Mengenai Kerangka Kerja Pengelolaan Keamanan Informasi di STIE Perbanas Surabaya

Hari/Tanggal	**: Kamis, 14 April 2016**
Pukul	**: 13:00**
Lokasi	**: Kampus 2 STIE Perbanas Surabaya**
Pewawancara	**: Radhifan Hidayat**
Narasumber	**: Hariadi Yutanto, S.Kom, M.Kom (Kasie TIK)**

Lampiran ini berisi pertanyaan dan jawaban untuk mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya di STIE Perbanas Surabaya. Berikut ini merupakan form lampiran tersebut:

1. Apakah kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?

   Jawaban:
   Kebijakan? Setelah terjadi insiden *hack* baru ada niat penyusunan, dan blueprint serta *disaster recovery plan (DRP)*, di targetkan tahun ini harus selesai.

2. Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?

   Jawaban:
   Kebijakan terkait keamanan informasi belum ditetapkan.

3. Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?

Jawaban:
Kebijakan terkait keamanan informasi masih belum ditetapkan.

4. Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?

Jawaban:
Kebijakan terkait keamanan informasi belum ditetapkan.

5. Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?

Jawaban:
Kebutuhan mitigasi masih dalam tahap perencanaan.

6. Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?

Jawaban:
Untuk insiden yang terjadi sendiri dilaporkan secara berkala dalam laporan semester dan tahunan, untuk penjagaan kerahasiaan telah dilakukan sosialisasi-

-walaupun untuk aspek tata tertib dalam pelaksanaannya masih belum berjalan secara keseluruhan dan masih belum tertulis.

7. Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?

Jawaban:
Untuk penegakan secara tegas belum terlaksana karena kebijakan keamanan informasi itu sendiri masih belum terdefinisi, hanya sebatas komunikasi in person saja.

8. Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?

Jawaban:
Dalam aspek keamanan informasi belum tersedia prosedur resmi.

9. Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggungjawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan melaporkannya?

Jawaban:
Kalau untuk prosedur operasional dalam mengelola security patch masih belum.

10. Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?

Jawaban:
Prosesnya biasanya sudah ada dan disusun dalam program kerja tahun 2015, disususun dalam tahapan apa saja yang perlu dikembangkan, termasuk nanti butuhnya apa itu sudah ada program kerjanya, kemudian fokus pengembangan pada tahun lalu 2015 sedang dikembangkan aplikasi contohnya E-ticketing, aplikasi bidder itu sudah ada, hanya saja pada program kerja pada tahun ini security tidak ada, walaupun di tengah-tengah jalannya program kerja ini ada musibah tentang keamanan itu tadi.

11. Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (compensating control) dan jadwal penyelesaiannya?

Jawaban:
Ada beberapa kegagalan implementasi dan biasanya tidak digunakan, tapi rata-rata semua jalan.

12. Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?

Jawaban:
Belum, untuk kerangka kerja yang spesifik STIE Perbanas Surabaya masih belum menggunakan.

13. Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?

Jawaban:
Belum.

14. Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?

Jawaban:
Belum.

15. Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?

Jawaban:
Belum, karena DRP nya sendiri masih dalam tahap penyusunan.

16. Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?

Jawaban:
Ya, biasanya QoP (Quality of Procedure) yang di evaluasi, ada banyak aspek QoP, prosedur untuk permintaan user dan password, permintaan web, prosedur untuk permintaan pengembangan software dan aplikasi, prosedur untuk proses maintenance dan ada dokumennya, dokumen yang paling sering berjalan dan berlanjut

sampai sekarang seperti mantain jaringan, maintain wireless, dan maintain komputer lab, kelas, persiapan kuliah, maintain server dan yang untuk banyak komplain menggunakan checklist. Proses monitoring per project? Usulan dari program anggaran yang disetujui, program kerja yang disetujui, terus di bulan berapa dibuat usulan tim dan terakhir implementasi dan laporan. Yang menjadi poin perhatian maintain QoP? terlaksananya business process, karena kebanyakan layanan based on IT harus berjalan dan tidak boleh ada masalah atau terhenti karena ada SLA (Service Level Agreement) jadi ada target sasaran mutu yang menjanjikan, contoh komputernya dalam sebulan tidak boleh mati berapa lama.

17. Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?

Jawaban:
Langkah penanggulangannya biasanya dilakukan evaluasi yang nantinya disajikan dalam laporan per semester, kendala itu terjadi karena apa? Terus solusinya karena apa? Contohnya jika hardware fisiknya yang bermasalah maka dapat dilakukan usulan entah itu penambahan atau perubahan apa, contoh kita butuh investasi karena harddisknya mati atau apa yang berarti usulan, jadi nanti ada kendalanya apa tak terpenuhi atau-tidak tercapai, tidak tercapai karena apa? Terus solusinya bagaimana? Maka ditambahkan dengan melakukan pembelian apa? Jadi seperti itu.

18. Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?

Jawaban:
Kira-kira untuk kemutakhiran penerapan teknologi informasi? Terdapat divisi riset dan development yang mengikuti perkembangan teknologi terkini yang mendukung visi misi dari STIE Perbanas itu sendiri, jadi mengikuti arahnya kemana karena divisi IT disini merupakan unit supporting.

19. Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?

Jawaban:
Untuk strategi penerapan keamanan informasi masih berupa sosialisasi door-to-door, jadi sebatas lisan, tapi secara tertulis kita punya kebijakan apa dan tidak boleh apa saja masih belum tertulis.

20. Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?

Jawaban:
Untuk audit external baru ISO tapi ya itu tidak berfokus kepada IT atau keamanan informasi, hanya berfokus pada manajemen.

21. Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?

Jawaban:
Untuk spesifik keamanan informasi sendiri belum didefinisikan.

22. Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?

Jawaban:
Belum.

23. Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?

Jawaban:
Untuk audit yang dilaporkan kepada pimpinan organisasi masih dari pihak eksternal dan audit yang dilakukan tidak mengacu spesifik pada keamanan informasi.

24. Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?

Jawaban:
Aspek anggaran? Ada analisa berdasarkan laporan, kenapa butuh ini? Karena apa? Biasanya memang harus ada analisa, contoh: penambahan bandwidth karena apa? Biasanya ada laporan rekomendasi apa?

25. Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah diterapkan secara efektif?

Jawaban:
Program keamanan informasi itu sendiri belum ditetapkan di STIE Perbanas.

26. Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?

Jawaban:
Untuk *roadmap*/*blueprint* diadakan atau disusun selama 5 tahun sekali.

Lampiran E
Interview Protocol Mengenai Pengelolaan Aset Informasi di STIE Perbanas Surabaya

Hari/Tanggal	**: Kamis, 14 April 2016**
Pukul	**: 13:00**
Lokasi	**: Kampus 2 STIE Perbanas Surabaya**
Pewawancara	**: Radhifan Hidayat**
Narasumber	**: Hariadi Yutanto, S.Kom, M.Kom (Kasie TIK)**

Lampiran ini berisi pertanyaan dan jawaban untuk mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya di STIE Perbanas Surabaya. Berikut ini merupakan form lampiran tersebut:

1. Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?

   Jawaban:
   Terdapat daftar inventaris.

2. Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?

   Jawaban:
   Pengelolaan dan pengklasifikasian aset? Diintegrasikan dalam sistem, masuk sisfo.

3. Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut?

Jawaban:
Ada, semua terekam di sisfo login jam berapa, melakukan apa saja, melakukan update apa saja.

4. Apakah tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?

Jawaban:
Tentang pengelolaan perubahan terhadap sistem biasanya mengikuti perubahan pelaporan EPSBED (Evaluasi Program Studi Berbasis Evaluasi Diri) dari dikti atau bidder itu baru dilakukan perubahan, selain itu tidak ada kebijakan baru dari pemerintah dikti khususnya, pengembangan yang banyak, contoh sekarang harus ada SKPI (Surat Keterangan Pendamping Ijazah) terus kalau perubahan divider sekarang ada laporan per semester EPSBED.

5. Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?

Jawaban:
Terdapat SOP atau QoP yang dijalankan secara konsisten.

6. Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?

Jawaban:
Untuk upgrade inventaris IT ke daftar aset ada di bagian umum, untuk inventaris umum fisik dan hardware, di TIK biasanya menginventaris software-software , secara fisik aset milik perbanas ada di yayasan dan bagian umum (BAU) yang berada di kampus 1.

7. Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda?

Jawaban:
Untuk sosialisasi secara individual telah diterapkan secara door-to-door.

8. Tata tertib penggunaan komputer, email, internet dan intranet?

Jawaban:
Dulu ada, Cuma terjadi banyak perubahan, emailnya banyak berubah, belum diperbaharui.

9. Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI?

Jawaban:
Untuk tata tertib spesifik terkait penggunaan aset belum ada.

10. Peraturan pengamanan data pribadi?

Jawaban:
Ada sosialisasi secara individual telah diterapkan secara door-to-door.

11. Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya?

Jawaban:
Ada pengelolaan identitas, namun untuk kebijakan username dan password masih belum ada.

12. Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi?

Jawaban:
Untuk kebijakan user name dan password masih belum ada.

13. Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data?

Jawaban:
Tidak ada retensi, hanya saja jika ada karyawan yang tidak lagi bekerja di bidangnya maka akunnya akan di disable dan di hapus, tidak ada dokumen formal, bagian yang memegang dan mengelola akun e-mail adalah bagian SDM.

14. Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya?

Jawaban:
Data sensitif yang mungkin digunakan adalah pelaporan pelaporan jumlah mahasiswa, pelaporan EPSBED dari dikti, laporan kerja dosen yang digunakan pihak eksternal.

15. Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi?

Jawaban:
Ada sewaktu ada insiden di bagian ICT.

16. Prosedur back-up uji coba pengembalian data (restore)?

Jawaban:
Backup dilakukan setiap hari, kemudian restore dilakukan jika terdapat masalah saja, contoh jika ada kasus kehilangan data apa, dilakukan trace terlebih dahulu, hilangnya kapan? kapan di buat? Setelah itu kita kembalikan.

17. Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya?

Jawaban:
Untuk pengamanan fisik? Yang di gembok laptop di ruang laboratorium, ruang server di kunci, ruang backup di divisi ICT dan yang memegang kunci hanya pihak IT dan pihak teknisi.

18. Proses pengecekan latar belakang SDM?

Jawaban:
Untuk pengecekan latar belakang SDM, ada kualifikasi.

19. Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib?

Jawaban:
Belum ada.

20. Prosedur penghancuran data/aset yang sudah tidak diperlukan?

Jawaban:
Tidak dilakukan.

21. Prosedur kajian penggunaan akses (user access review) dan langkah pembenahan apabila terjadi ketidak sesuaian (non-conformity) terhadap kebijakan yang berlaku?

Jawaban:
Penggunaan akses sudah diatur, tidak ada dokumen tertulis, tetapi secara teknis sudah semua, jadi apakah suatu sub unit itu boleh mengakses apa saja, apa yang tidak boleh, itu ada.

22. Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?

Jawaban:
Daftar informasi yang harus di backup? Tidak ada daftar informasi spesifik yang harus di backup, namun backup dilakukan pada semua server, berkaitan dengan database dan data di backup semua.

23. Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?

Jawaban:
Untuk rekaman pelaksanaan keamanan informasi sendiri belum dilakukan secara detail, namun untuk klasifikasi hak akses telah dilakukan.

24. Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?

Jawaban:
Tidak ada prosedur spesifik terhadap hubungan dengan pihak ketiga, hanya terkadang pihak SMK yang melakukan magang.

25. Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?

Jawaban:
Ada petugas security, dan daftar kunjungan serta kartu parkir.

26. Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?

Jawaban:
Ada terutama ruang server, ruang kelas, dan tiap ruangan.

27. Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?

Jawaban:
Perlindungan Infrastruktur IT dari dampak lingkungan? Sudah semenjak ada kejadian.

28. Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?

Jawaban:
Untuk kelistrikan jarang terjadi listrik mati, sudah disiapkan UPS dan Genset.

29. Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?

Jawaban:
Belum ada.

30. Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?

Jawaban:
Untuk fasilitas pendukung yang dapat menanggulangi risiko kebakaran sudah ditempatkan di beberapa titik utama di seluruh kampus.

31. Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?

Jawaban:
Proses maintenance dan perawatan IT? Maintenance server utama dilakukan setiap hari seperti cek derajat, dulu maintain dilakukan 6 bulan sekali, kemudian setelah dilakukan penataan ulang (kabel dsb.) maintain harian hanya dilakukan seperti pengecekan suhu untuk kelas lab perkuliahan dilakukan rutin 3 bulan sekali, menjelang UTS, menjelang UAS, untuk maintenance wifi 2 minggu sekali.

32. Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?

Jawaban:
Untuk aturan di ruang server, untuk peraturan tertulis belum ada, namun tanggung jawab terletak pada pemegang kunci.

33. Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)?

Jawaban:
Penataan kearsipan? Untuk ICT ada arsip, seperti dokumen permintaan, seperti user dan password dll.

34. Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?

Jawaban:
Pemantauan oleh Satuan Pengamanan (Satpam).

Lampiran F
Interview Protocol Mengenai Teknologi Dan Keamanan Informasi di STIE Perbanas Surabaya

Hari/Tanggal	**: Kamis, 14 April 2016**
Pukul	**: 13:00**
Lokasi	**: Kampus 2 STIE Perbanas Surabaya**
Pewawancara	**: Radhifan Hidayat**
Narasumber	**: Hariadi Yutanto, S.Kom, M.Kom (Kasie TIK)**

Lampiran ini berisi pertanyaan dan jawaban untuk mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya di STIE Perbanas Surabaya. Berikut ini merupakan form lampiran tersebut:

1. Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?

   Jawaban:
   Dalam penerapan perlindungan internet, ada pembatasan akses terhadap sistem, setiap pemakai sistem diberi otorisasi yang berbeda-beda. Setiap pemakai dilengkapi dengan nama pemakai dan password. Kemudian untuk *proxy* tidak, hanya *firewall* saja.

2. Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?

Jawaban:
Ada, jaringan di segmentasi dengan adanya authentikasi login lewat WPA/WP, dan mahasiswa tidak dapat mengakses jaringan dosen.

3. Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan?

Jawaban:
Ada.

4. Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?

Jawaban:
Belum.

5. Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?

Jawaban:
Jika secara rutin masih belum namun dilakukan secara insidensial saja, dalam perencanaan.

6. Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?

Jawaban:
Ada monitoring yang kemudian jika ada kebutuhan lebih lanjut akan diajukan pada laporan berikutnya.

7. Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?

Jawaban:
Dulu ada proxy, sharp, tapi setelah ada insiden kebakaran belum dibangun lagi.

8. Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?

Jawaban:
Dalam perencanaan.

9. Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?

Jawaban:
Log dianalisa.

10. Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?

Jawaban:
Ada.

11. Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?

Jawaban:
Belum.

12. Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?

Jawaban:
Ada.

13. Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama?

Jawaban:
Pergantian password masih belum rutin, by case saja.

14. Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?

Jawaban:
Ada.

15. Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login,dan penarikan akses?

Jawaban:
Untuk pembatasan waktu akses, ada session.

16. Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?

Jawaban:
Untuk jaringan nirkabel menggunakan id dan diberikan password.

17. Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?

Jawaban:
Belum, berdasarkan serangan yang terjadi belakangan ini maka sedang di rencanakan.

18. Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?

Jawaban:
Menggunakan versi terbaru.

19. Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?

Jawaban:
Untuk antivirus menggunakan eScan dan ada lisensinya.

20. Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis?

Jawaban:
Antivirus di update secara rutin, namun untuk rekaman hasil analisa belum ada.

21. Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?

Jawaban:
Kasus kena virus ada, namun tidak terlalu parah, dan juga semua port usb di blokir.

22. Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?

Jawaban:
Sistem informasi Mahasiswa, staff, masing-masing per unit, Akademik, Kemahasiswaan, Keuangan, Humas, Perpustakaan, masing masing unit ada dan terintegrasi.

23. Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba?

Jawaban:
Belum ada.

24. Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?

Jawaban:
Pihak independen belum ada terlibat dalam kemanan informasi.

Lampiran G
Bukti Pendukung

Foto G-1

Kamera CCTV di beberapa tempat di gedung A & B

Foto G-2

Smoke detector di beberapa tempat di gedung A & B

Foto G-3

Fire extinguisher di beberapa tempat di gedung A & B

Foto G-4

Selang hydrant di beberapa tempat di gedung A & B

Foto G-5

Alarm peringatan di setiap laboratorium komputer

Foto G-6

Peringatan larangan merokok di dalam gedung

Foto G-7

Buku Tamu & Satuan Pengamanan (SATPAM) di Kampus A & B

Foto G-8

Foto pengamanan ruang server

Foto G-9

Foto Ruang Server

Foto G-10

Foto Backup Server

Foto G-11

Lisensi Antivirus e-Scan

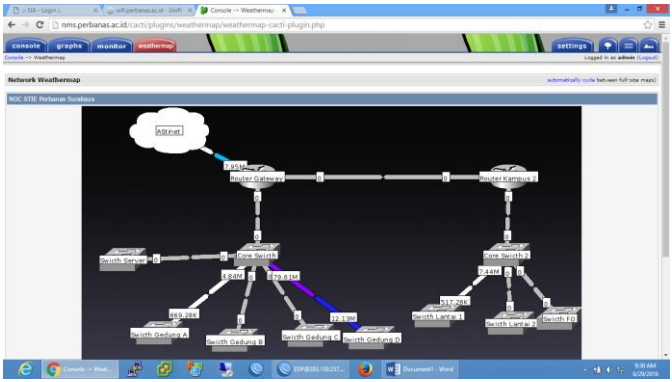
Foto G-12

Tampilan sisfo.perbanas.ac.id/perbanas

Foto G-13

Mapping Wifi STIE Perbanas Surabaya

Foto G-14



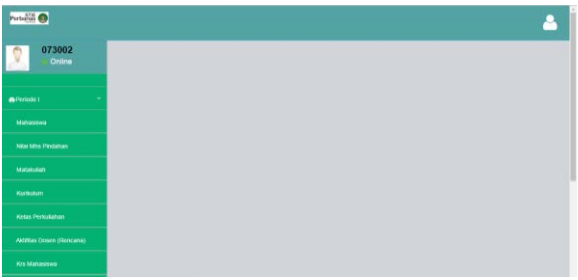
Mapping Network STIE Perbanas Surabaya

Foto G-15

simas_log_id	id_mhs	simas_log_session	simas_log_cin	simas_log_cout	simas_log_type	simas_log_ip	simas_log_os	simas_log_browser	simas_l
621cb9a3809b17c27492fb1a1b785ce	4002	fb7dfa664ea9afefac7c564bc4caa4e5	2009-08-21 07:03:00	NULL	M	125.164.65.57	unknown	unknown	unknown
809e7fbeb21a6d9135f438d1c1a72a3	6106	50a93c6259c23479495f6cc0ac54206a	2009-08-21 07:04:33	NULL	M	222.124.156.201	unknown	unknown	unknown
9676d2815912da22b524d1c7fb292f8	5152	a845ec672a77e17ca6dff9ab23fb73	2009-08-21 07:08:04	NULL	M	124.195.65.19	unknown	unknown	unknown
7558b4231eee07838dfe8c6a7b54c53	6282	c3b00f1e86dcd5af0a070c3ed5ed4b3e	2009-08-21 07:20:26	NULL	M	125.164.119.106	unknown	unknown	unknown
ca98c7838abcabbf462d25a63a8feff	7320	4588e6660341ce690f398250fbd81c94	2009-08-21 07:22:02	NULL	M	222.124.228.7	unknown	unknown	unknown
859dd39b4e2523aeeffeee2fb64b94a	6781	4148ac6487d9fbbf2132cddb3891d584	2009-08-21 07:25:52	NULL	M	94.246.126.99	unknown	unknown	unknown
3781feebc96f032cf71882bcf0e6b3e	5294	6f5dd37b1c8982ddeea4c9518d71aa9f	2009-08-21 07:42:45	NULL	M	202.70.55.165	unknown	unknown	unknown
ec9600352dcf9682570dd8defa763de	6743	f8cae5973e796a5efc406ff833c2f9e1	2009-08-21 07:45:28	NULL	M	114.59.212.71	unknown	unknown	unknown
687924056b9634a190044c9832058a5	5910	fd8bda5df122d94991a65b394a23cb26	2009-08-21 06:53:31	2009-08-21 07:49:41	M	125.164.138.198	unknown	unknown	
bd97a3a16d0222a6d4061380d836b8d	6066	daaaf3c35a1883e3228a8eb0a75314f2	2009-08-21 07:50:12	NULL	M	125.167.50.184	unknown	unknown	unknown
5e6c20aaab88983f75e517aaa25a8c3	5294	cbbd0579de7775ee8e7f5f4f3e042c8a	2009-08-21 07:55:35	NULL	M	61.94.212.201	unknown	unknown	unknown
df2780a1a540b2edbddba23cdbcc53c	3256	6ea9062f8312b86680ca65e2acb16ec	2009-08-21 07:56:28	NULL	M	125.164.207.112	unknown	unknown	unknown
7febf60ef48c8dedc7614601106253f	6283	a4480ce3eaefdc10c29a96f33be69244	2009-08-21 09:02:30	NULL	M	106.189.142.171	unknown	unknown	unknown
daf0f78187063ba79d015331b63113f	5849	335f59ed9541c9680cf8e5748f9976aa	2009-08-21 09:06:00	NULL	M	125.164.9.63	unknown	unknown	unknown
a8ec4fd832303f4408ca82e2910c5aa	6769	1471092562f0b5da05d6d728e68df7fc	2009-08-21 09:13:02	NULL	M	125.164.85.103	unknown	unknown	unknown
5946c505fdfd6a3fca6c64c89f4d3be	6514	241f2f1272b54dfcbf7754393909cc9a	2009-08-22 10:58:36	NULL	M	125.164.212.6	unknown	unknown	unknown
fd6035b7d470110230b48ef3522c7b5	6008	6ed0e7314a174830d47b879830a6628f	2009-08-21 09:26:11	NULL	M	125.164.7.26	unknown	unknown	unknown
997b97d6b880cc771d63970b61a38bc	6480	b9e4df2022038a4cf17356b1ebcd5b26	2009-08-21 08:25:16	NULL	M	202.93.36.71	unknown	unknown	unknown
a503f4941367c142659e3f967fc658a	6781	cbe0cf75c2873d33a9908a9405f77a28	2009-08-21 06:39:11	NULL	M	125.167.58.105	unknown	unknown	unknown
e765afb18fb03cd05b2bd111775cf92	5775	09d03c7b2599f5bca1dfed6d25c34625	2009-08-21 08:00:29	2009-08-21 08:32:15	M	125.164.134.148	unknown	unknown	
088b1f2a06802936ba21c4274047f5b	5775	09d03c7b2599f5bca1dfed6d25c34625	2009-08-21 08:20:58	2009-08-21 08:32:15	M	125.164.134.148	unknown	unknown	
3b9a00eb16aa8878ab3922d4bffc4f0	5641	f98978e5dc0106a6638c287b51bd0680	2009-08-21 09:00:00	NULL	M	202.70.55.162	unknown	unknown	unknown
f41a50b7eecb6a47cbcbaf3cb0cf004	6290	582c0cef47fef46ed7696d79f1078eb	2009-08-21 09:14:36	NULL	M	125.164.11.112	unknown	unknown	unknown
138cb1095b684a1de25c8e055debe3f	6769	1471092562f0b5da05d6d728e68df7fc	2009-08-21 09:17:28	NULL	M	125.164.85.103	unknown	unknown	unknown
e7fc95d13ced8ad71487b375f00696a	5980	4f0f66c9fb0bf00ade9b18d12a056d97	2009-08-21 09:25:04	2009-08-21 09:28:50	M	125.164.151.53	unknown	unknown	
68ec63e6d0468ea6157b098738f487b	3691	06e08558a0d308f10719b2c9359f8677	2009-08-21 08:24:53	2009-08-21 09:31:00	M	202.70.55.163	unknown	unknown	
19c2051e6e9489c5032f2dc4a26c84d	6071	60d482a3384339430eb213ff966e281f	2009-08-22 10:31:17	2009-08-22 11:47:40	M	125.164.65.244	unknown	unknown	
2750674c9778edbc1fc3ba0fc8bdce5	6140	50dfc11589901247e9824fa1fd2146ff	2009-08-21 06:14:56	NULL	M	222.124.224.59	unknown	mozilla	1024x76
fdf5e044cceef8bfa68e303599084e4	6516	d62d9436aaa25e70fed8f062fb8826f4	2009-08-21 06:28:01	2009-08-21 06:30:58	M	202.70.55.160	unknown	mozilla	
8ee4e54456f6a3e30785ecec9624265	5957	4e49f4a75aba848caa6f18cfe8d1a9dc	2009-08-21 06:25:11	NULL	M	125.164.212.72	unknown	mozilla	1024x76

Log aktivitas user sisfo.perbanas.ac.id

Foto G-16



Halaman Login sisfo.perbanas.ac.id

Foto G-17

No	SASARAN MUTU	CARA PENGUKURAN & MEDIA MONITORING	TARGET	HASIL PENGUKURAN							Keterangan (Tercapai / Tidak)	PIC
				Base	Mid							
				Agt 13	Sep 13	Okt 13	Nop 13	Des 13	Jan 14	Feb 14		
1	*Service Level Agreement* (SLA) koneksi internet	Contoh Perhitungan SLA : • 1 Bulan = 30 hari = 720 jam merupakan total 100% layanan • 95% * 720 jam = 684 Jam, merupakan jaminan (SLA) • 5% * 720 jam = 36 Jam, merupakan jaminan atas kegagalan koneksi internet dalam 1 bulan maksimal 36 jam	95%, artinya kegagalan koneksi jaringan sebesar 5% dalam 1 periode pengukuran	NA	100%	100%	100%	100%	100%	100%	Tercapai	Nurhadi Hariadi Y.
2	SLA jaringan kabel LAN	Idem nomor 1, jaminan atas kegagalan akses ke jaringan kabel LAN dalam 1 bulan maksimal 36 jam	95%, artinya kerusakan jaringan kabel LAN sebesar 5% dalam 1 periode pengukuran	NA	100%	100%	100%	100%	100%	100%	Tercapai	Nurhadi Hariadi Y.
3	SLA jaringan wifi (hotspot)	Idem nomor 1, jaminan atas kegagalan akses ke wifi dalam 1 bulan maksimal 36 jam	95%, artinya kegagalan koneksi wifi sebesar 5% dalam 1 periode pengukuran	NA	100%	100%	100%	100%	100%	72%	Tercapai	Nurhadi Hariadi Y.
4	SLA jaringan antara kampus 1 dengan kampus 3	Idem nomor 1, jaminan atas kerusakan koneksi antar kampus dalam 1 bulan maksimal 36 jam	95%, artinya kerusakan jaringan antar kampus sebesar 5% dalam 1 periode pengukuran	NA	100%	100%	100%	100%	100%	100%	Tercapai	Nurhadi Hariadi Y.
5	SLA server SISFO	Idem nomor 1, jaminan atas kegagalan akses ke server SISFO dalam 1 bulan maksimal 36 jam	95%, artinya kegagalan koneksi ke server SISFO sebesar 5% dalam 1 periode pengukuran	NA	100%	100%	100%	100%	100%	100%	Tercapai	Nurhadi Hariadi Y. M. Yunus
6	SLA server domain	Idem nomor 1, jaminan atas kegagalan akses ke server domain dalam 1 bulan maksimal 36 jam	95%, artinya kerusakan server domain sebesar 5% dalam 1 periode pengukuran	NA	100%	100%	100%	100%	100%	94,5%	Tercapai	Nurhadi Hariadi Y.
7	SLA server SAP & Oracle	Idem nomor 1, jaminan atas kegagalan proses SAP & Oracle dalam 1 bulan maksimal 36 jam	95%, artinya kegagalan proses SAP & Oracle sebesar 5% dalam 1 periode pengukuran	NA	100%	100%	100%	100%	100%	100%	Tercapai	Nurhadi Hariadi Y.
8	SLA software & aplikasi laboratorium, ruang kelas, civitas	Idem nomor 1, jaminan atas kegagalan akses software & aplikasi di lab, ruang kelas & civitas dalam 1 bulan maksimal 36 jam	95%, artinya kerusakan software aplikasi sebesar 5% dalam 1 periode pengukuran	NA	100%	100%	100%	100%	100%	100%	Tercapai	Nurhadi Hariadi Y.
9	SLA aplikasi SISFO	Idem nomor 1, jaminan atas ketidakwenaan data dan kerusakan aplikasi SISFO dalam 1 bulan	95%, artinya kesalahan proses SISFO sebesar 5% dalam 1 periode pengukuran	NA	100%	100%	100%	100%	100%	100%	Tercapai	Nurhadi M. Yunus

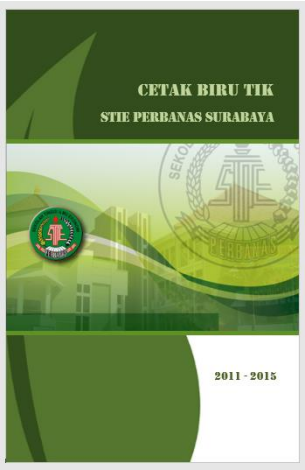
Capaian Sasaran Mutu Unit Kerja TIK

Foto G-18

NO	NAMA AKTIVITAS	NAMA BIAYA	Nama Barang	Rencana anggaran yang dibutuhkan	Periode						Capaian	Keterangan
					2013				2014			
					09	10	11	12	01	02		
1	Pengembangan tata kelola sarana-prasarana	Pembelian PC untuk server oracle	PC Core i7	54.000.000				V	V		Realokasi, Server	Oracle tidak menggunakan PC, tetapi diulicoba di Server. Saat ini sedang silicoba untuk perkuliahan s.d. April 2014
		HR Tim Kepanitiaan (7 orang)	HR Tim pengembangan Oracle	10.000.000					V	V	Progress	
	Pengembangan tata kelola sarana-prasarana	HR Tim Kepanitiaan (10 orang)	HR Tim Pengembangan Fasilitas Lab Bank Syariah & Akuntansi Perbankan	5.000.000		V	V	V			Tercapai	Oktober 2013 dikembangkan dan sudah diulicoba untuk perkuliahan setelah UTS
2	Pengembangan Website/SISFO	HR Tim Kepanitiaan (12 orang)	HR Tim pengembangan SISFO EISS	5.000.000							Belum	
3	Pengembangan Website/SISFO	HR Tim Kepanitiaan (11 orang)	HR Tim pengembangan SISFO DSS	25.000.000							Belum	Akan dikembangkan melalui Hibah. Aktifitas dialihkan ke pengembangan SISFO SDM
4	Pengembangan Website/SISFO	HR Tim Kepanitiaan (7 orang)	HR Tim webometric	20.000.000	V	V	V	V	V	V	Tercapai, belum dilaporkan	Pengembangan teknologi dan metode Webo telah dilakukan. Pada Webo januari 2014, STIE Perbanas menempati ranking 88
5	Pengembangan SDM	Akomodasi & transportasi pelatihan eksternal	Akomodasi & transportasi pelatihan eksternal	3.000.000	V			V	V	V	Tercapai, ada 4 seminar yang diikuti	TIK telah menprimkan untuk mengikuti berbagai seminar yang bersifat Gratis dan di Surabaya. Pengeluaran belum ada
		Biaya pendaftaran seminar/workshop	Biaya pendaftaran seminar/workshop	4.000.000	V			V	V	V		
		Tiket perjalanan dinas	Tiket perjalanan	3.000.000	V			V	V	V		
6	Penyelenggaraan seminar internal	HR Instruktur pengembangan internal	HR Instruktur & Asisten	900.000					V		Progress	Dilaksanakan bulan Maret untuk sosialisasi SPT
		Konsumsi pengembangan skill	Konsumsi pelatihan	750.000					V		Progress	

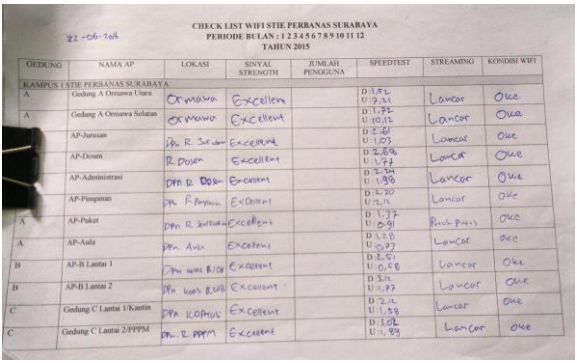
Capaian Sasaran Anggaran TIK

Foto G-19



Dokumen Cetak Biru (*Blueprint*) TIK STIE Perbanas Surabaya

Foto G-20



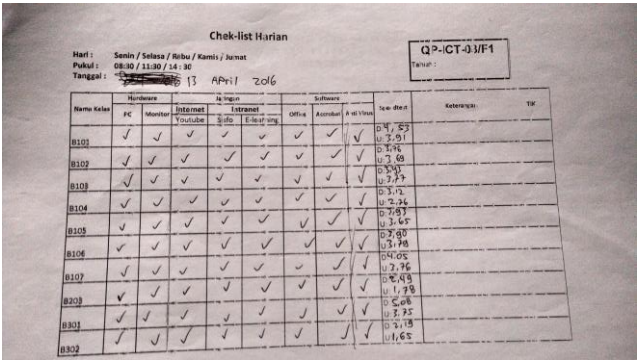
CHECK LIST WIFI STIE PERBANAS SURABAYA
PERIODE BULAN : 1 2 3 4 5 6 7 8 9 10 11 12
TAHUN 2015

22-06-2015

GEDUNG	NAMA AP	LOKASI	SINYAL STRENGTH	JUMLAH PENGGUNA	SPEEDTEST	STREAMING	KONDISI WIFI
KAMPUS I STIE PERBANAS SURABAYA							
A	Gedung A Ornawa Utara	Ornawa	Excellent		D:1,82 U:2,31	Lancar	Oke
A	Gedung A Ornawa Selatan	Ornawa	Excellent		D:1,72 U:10,12	Lancar	Oke
	AP-Jurusan	Dpn R. Jurusan	Excellent		D:2,61 U:1,03	Lancar	Oke
	AP-Dosen	R. Dosen	Excellent		D:2,89 U:1,71	Lancar	Oke
	AP-Administrasi	Dpn R. Dosen	Excellent		D:2,54 U:1,96	Lancar	Oke
	AP-Pimpinan	Dpn R. Pimpinan	Excellent		D:2,20 U:2,15	Lancar	Oke
	AP-Paket	Dpn R. Sirkulasi	Excellent		D:1,77 U:0,91	Buruk Putus	Oke
A	AP-Aula	Dpn. Aula	Excellent		D:1,80 U:0,27	Lancar	Oke
B	AP-B Lantai 1	Dpn Kom B.108	Excellent		D:2,57 U:0,58	Lancar	Oke
B	AP-B Lantai 2	Dpn Kom B.208	Excellent		D:3,11 U:1,97	Lancar	Oke
C	Gedung C Lantai 1/Kantin	Dpn KOPMA	Excellent		D:2,16 U:1,58	Lancar	Oke
C	Gedung C Lantai 2/PPPM	Dpn. R. PPPM	Excellent		D:1,02 U:1,89	Lancar	Oke

***Checklist* Maintenance Wifi Bulanan**

Foto G-21



Chek-list Harian

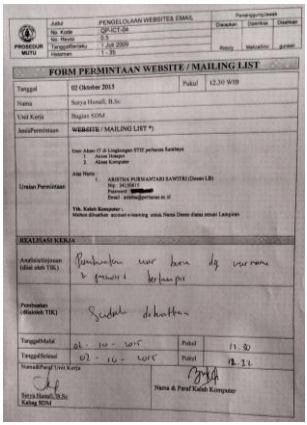
QP-ICT-03/F1

Hari : Senin / Selasa / Rabu / Kamis / Jumat
Pukul : 08:30 / 11:30 / 14 : 30
Tanggal : [redacted] 13 April 2016

Nama Kelas	Hardware		Jaringan			Software			Kecepatan	Keterangan TIK
	PC	Monitor	Internet Youtube	Istranet Sidfo	Istranet E-learning	Office	Acrobat	Anti Virus		
B101	√	√	√	√	√	√	√	√	D 9,53 U 3,91	
B102	√	√	√	√	√	√	√	√	D 2,96 U 3,68	
B103	√	√	√	√	√	√	√	√	D 3,01 U 3,77	
B104	√	√	√	√	√	√	√	√	D 3,12 U 3,26	
B105	√	√	√	√	√	√	√	√	D 7,87 U 3,65	
B106	√	√	√	√	√	√	√	√	D 7,80 U 3,78	
B107	√	√	√	√	√	√	√	√	D 4,05 U 2,76	
B203	√	√	√	√	√	√	√	√	D 2,48 U 1,78	
B301	√	√	√	√	√	√	√	√	D 5,08 U 2,85	
B302	√	√	√	√	√	√	√	√	D 2,13 U 1,65	

***Checklist* Maintenance Kecepatan Internet Per-Kelas Harian**

Foto G-22



PROSEDUR MUTU

Judul : PENGELOLAAN WEBSITE& EMAIL
No. Kode : QP-ICT-06
No. Revisi : 0.5
Tanggal berlaku : 1 Juli 2009
Halaman : 1 - 35

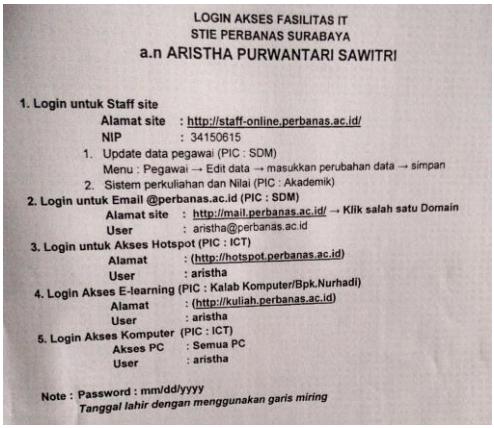
Penanggung jawab: Direktur | Diperiksa | Disahkan

FORM PERMINTAAN WEBSITE / MAILING LIST

Tanggal	02 Oktober 2015	Pukul	12.30 WIB
Nama	Surya Hendi, B.Sc		
Unit Kerja	Bagian SDM		
JenisPermintaan	WEBSITE / MAILING LIST *)		
Uraian Permintaan	User Akun IT di Lingkungan STIE perlunya Sandiket 1 Akses Hakpor 2 Akses Komputer Atas Nama : 1 [redacted] ARISTIA PURWANTARI SAWITRI (Dosen LB) Hp : 0[redacted] Password : [redacted] Email : aristia@perbanas.ac.id Ttk. Kabit Komputer : Mohon dibuatkan account e-learning untuk Nama Dosen diatas sesuai Lampiran		
REALISASI KERJA			
Analisis/Usulan (diisi oleh TIK)	Pembuatan user baru dg username & password terlampir		
Pembuatan (diisikan TIK)	Sudah dibuatkan		
TanggalMulai	02 - 10 - 2015	Pukul	13.30
TanggalSelesai	02 - 10 - 2015	Pukul	13.31
Nama&Paraf Unit Kerja	Surya Hendi, B.Sc Kabag SDM	Nama & Paraf Kabit Komputer	

Form Permintaan Website / Mailing List

Foto G-23



LOGIN AKSES FASILITAS IT
STIE PERBANAS SURABAYA
a.n ARISTHA PURWANTARI SAWITRI

1. Login untuk Staff site
   - Alamat site : http://staff-online.perbanas.ac.id/
   - NIP : 34150615
   1. Update data pegawai (PIC : SDM)
      Menu : Pegawai → Edit data → masukkan perubahan data → simpan
   2. Sistem perkuliahan dan Nilai (PIC : Akademik)
2. Login untuk Email @perbanas.ac.id (PIC : SDM)
   - Alamat site : http://mail.perbanas.ac.id/ → Klik salah satu Domain
   - User : aristha@perbanas.ac.id
3. Login untuk Akses Hotspot (PIC : ICT)
   - Alamat : (http://hotspot.perbanas.ac.id)
   - User : aristha
4. Login Akses E-learning (PIC : Kalab Komputer/Bpk.Nurhadi)
   - Alamat : (http://kuliah.perbanas.ac.id)
   - User : aristha
5. Login Akses Komputer (PIC : ICT)
   - Akses PC : Semua PC
   - User : aristha

Note : Password : mm/dd/yyyy
Tanggal lahir dengan menggunakan garis miring

Dokumen Pembagian Hak Akses Untuk Staff

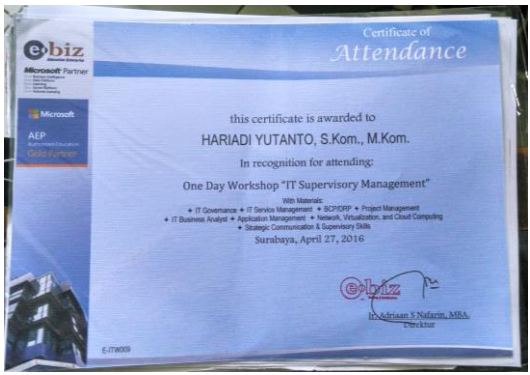
Foto G-24

Unit 240 TIK

USULAN RKAT PERIODE 2016-2017

Dokumen Usulan Anggaran TIK Tahunan

Foto G-25

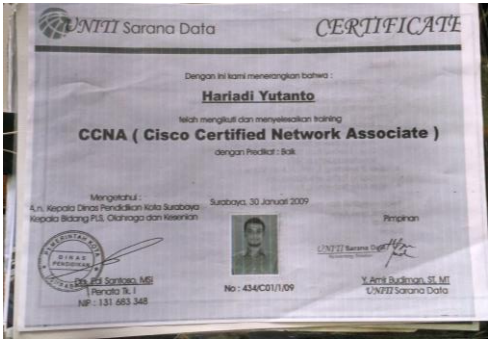


Sertifikat Workshop IT Management

Foto G-26

Sertfikat Workshop Pelatihan Virus Terbaru

Foto G-27



Sertifikat Workshop & Pelatihan CCNA

BAB VII
KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan yang menjawab rumusan masalah, beserta saran yang bermanfaat sebagai masukkan bagi peneliti selanjutnya.

7.1. Kesimpulan

Berdasarkan hasil dan pembahasan yang dilakukan pada bab sebelumnya maka didapakan beberapa kesimpulan berikut ini:

- Untuk tingkat kematangan per-area diketahui pada area Tata Kelola berada pada level I+, area Pengelolaan Risiko berada pada level I, area Kerangka Kerja berada pada level I+, area Pengelolaan Aset berada pada level II, dan area Teknologi berada pada level II. Dimana tingkat kematangan masih dalam rentang level I s/d II, dan batasan minimal yang harus dicapai agar dapat melakukan sertifikasi ISO adalah III.
- Nilai kelengkapan keamanan informasi yang didapatkan dari lima area dalam Indeks KAMI didapatkan hasil penilaian sebesar 252 (dari total nilai keseluruhan 588) dan berada pada level I.
- Hasil tersebut menunjukkan bahwa sebagian besar proses keamanan informasi yang ada pada STIE Perbanas Surabaya belum dilakukan secara rutin dan belum sesuai dengan standar prosedur yang ada. Berdasarkan standar dari ISO/IEC 27001:2005 maka pengelolaan keamanan informasi di STIE Perbanas Surabaya masih harus diperbaiki kembali, terlebih pada area Pengelolaan Risiko yang memiliki skor paling rendah dibandingkan area evaluasi lainnya,

diikuti dengan area Kerangka Kerja dan area Tata Kelola.

7.2. Saran

Berdasarkan penelitian yang telah dilakukan, berikut ini merupakan saran secara singkat yang diberikan untuk meningkatkan kelima area pengamanan Indeks Keamanan Informasi (KAMI):

- Untuk penelitian selanjutnya sebaiknya peneliti menggunakan standar penilaian Indeks Keamanan Informasi (KAMI) versi terbaru dari Kementerian Kominfo agar dapat menyesuaikan dengan perkembangan kebutuhan, relevansi serta teknologi terbaru.
- Diperlukan adanya petunjuk teknis secara detail mengenai proses penilaian pada Indeks KAMI guna memahami perolehan skor yang didapat maupun untuk perbaikan serta pengembangan proses penilaian untuk kedepannya.

DAFTAR PUSTAKA

[1] Kementerian Komunikasi dan Informatika, "Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta," 8 May 2014. [Online]. Available: http://kominfo.go.id/. [Accessed 18 February 2016].

[2] Republik Indonesia, Undang-undang No. 11 Tahun 2008 Pasal 15 ayat 1 tentang Dasar Hukum Penerapan Tata Kelola Keamanan Informasi, Jakarta: Sekretariat Negara, 2008.

[3] Republik Indonesia, Peraturan Pemerintah No. 82 Tahun 2012 pasal 14 ayat 1, Jakarta: Sekretariat Negara, 2012.

[4] Kementerian Komunikasi dan Informasi, SIARAN PERS NO. 83/PIH/KOMINFO/11/2013, Jakarta: Kementerian Komunikasi dan Informasi, 2013.

[5] Kementerian Komunikasi dan Informasi, SE Menteri Kominfo No. 5 bulan Juli 2011, Jakarta: Kementerian Komunikasi dan Informasi, 2011.

[6] W. A. Mahrens, Measurement and Evaluation in Education and Psychology, 1978.

[7] J. Crawford, Evaluation of Libraries and Information Services, London: Aslib, The Association for Information Management and Information Management International, 2000.

[8] H. Umar, Evaluasi Kinerja Perusahaan, Jakarta: PT Gramedia Pustaka Utama, 2002.

[9] ISO/IEC 27001:2005, Information Technology -- Security Techniques -- Information Security Management System -- Requirement, ISO/EC, 2005.

[10] M. E. &. M. H. J. Whitman, Management of Information Security, USA: Course Technology, 2010.

[11] Kementerian Komunikasi dan Informatika, "Indeks Keamanan Informasi (KAMI)," 23 October 2013. [Online]. Available: http://kominfo.go.id/index.php/content/detail/3326/Indeks-Keamanan-Informasi--KAMI-

/0/kemanan_informasi#.VsTa9ct_zDc. [Accessed 18 February 2016].

[12] Leveraging Technology In Education, IT Governance, 2003.

[13] C. S. C. a. T. I. G. Institute, COBIT (3rd Edition) Management Guidelines, IT Governance Institute, 2000.

[14] M. Jaccard, The Objective Is Quality, CRC Press, 2013.

[15] J. W. Creswell, Qualitative inquiry and research design: choosing among five traditions, Thousand Oaks: Sage Publications, 1998.

[16] R. Yin, Case Study Research Design and Method, Newbury Park: Sage, 1989.

[17] R. Yin, Case study research: Design and methods (3rd ed.), Thousand Oaks: CA: Sage, 2003.

[18] STIE Perbanas, "Departemen Teknologi Informasi Komunikasi," [Online]. Available: http://www.perbanas.ac.id/bagian-administrasi/departemen-teknologi-informasi-komunikasi.html. [Accessed 18 February 2016].

[19] STIE Perbanas, "Sekilas Perbanas," [Online]. Available: http://www.perbanas.ac.id/fakta-perbanas/sekilas-perbanas.html. [Accessed 18 February 2016].

[20] STIE Perbanas, "Visi & Misi," [Online]. Available: http://www.perbanas.ac.id/fakta-perbanas/visi-misi-a-budaya.html. [Accessed 18 February 2016].

BIODATA PENULIS

RADHIFAN HIDAYAT, lahir pada 1 Juni 1994 di kota Jambi. Penulis merupakan anak pertama dari Ir. M. Sidik Yulianto, MM dan Nunung Sudarti. Penulis telah menempuh pendidikan formal di SDN 177 Kota Jambi, SMPN 1 Kota Jambi, SMA Titian Teras Jambi, dan akhirnya penulis masuk menjadi mahasiswa program sarjana jurusan Sistem Informasi Institut Teknologi Sepuluh Nopember (ITS) angkatan 2011. Pada akhir masa perkuliahan di jurusan Sistem Informasi ITS, penulis memilih untuk mengerjakan tugas akhir di Laboratorium Manajemen Sistem Informasi (MSI). Penulis mengambil topik mengenai evaluasi keamanan informasi dibawah bimbingan Dr. Apol Pribadi S, S.T., M.T. dan Hanim Maria Astuti, S.Kom. M.Sc. Selain memiliki kesukaan pada kegiatan alam dan musik penulis juga sempat mengikuti kegiatan organisasi Mahasiswa Tanggap Bencana ITS (Mahagana) pada divisi Pelaporan Bencana kemudian penulis juga aktif berorganisasi dalam Ikatan Mahasiswa Jambi di Surabaya (IMABIS). Penulis juga pernah menjalani Kerja Praktik selama tiga bulan di PT. Telekomunikasi Indonesia Witel Sumatera Barat pada Divisi Business Service (DBS) dan terlibat dalam perancangan Masterplan Pariaman Smart City. Untuk kepentingan penelitian penulis dapat dihubungi melalui e-mail: radhifan.hidayat@gmail.com