AUDIT KEAMANAN INFORMASI SIMAK *ONLINE* UNIVERSITAS INDO GLOBAL MANDIRI PALEMBANG BERDASARKAN STANDAR ISO/IEC 27001:2005

SKRIPSI

Sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer dalam bidang Sistem Informasi

Oleh

YENI RAHAYU
NIM. 14540170

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI RADEN FATAH
PALEMBANG
2018

HALAMAN PENGESAHAN

AUDIT KEAMANAN INFORMASI SIMAK *ONLINE* UNIVERSITAS INDO GLOBAL MANDIRI PALEMBANG BERDASARKAN STANDAR ISO/IEC 27001:2005

OLEH:

YENI RAHAYU
NIM. 14540170

Telah dipertahankan di depan sidang penguji skripsi
Pada tanggal 07 Desember 2018
dan dinyatakan memenuhi syarat untuk memperoleh gelar
Sarjana Komputer dalam bidang Sistem Informasi

Dosen Pembimbing I	Dosen Pembimbing II
Rusmala Santi, M. Kom	**Muhamad Kadafi, M.Kom**
NIP. 197911252014032002	**NIDN: 0223108404**

Mengetahui,
Ketua Program Studi Sistem Informasi
Fakultas Sains dan Teknologi
UIN Raden Fatah Palembang

Ruliansyah, M. Kom.
NIP.19751122006041003

PERSETUJUAN
TIM PENGUJI SKRIPSI

Judul Skripsi	: Audit Keamanan Informasi Simak *Online* Universitas Indo Global Mandiri Palembang Berdasarkan Standar ISO/IEC 27001:2005
Nama	: Yeni Rahayu
NIM	: 14540170
Program	: Sarjana (S1) Fakultas Sains dan Teknologi

Telah disetujui oleh tim penguji sidang skripsi.

1. Ketua : Rusmala Santi, M.Kom
   NIP. 197911252014032002

2. Sekertaris : Muhamad Kadafi, M.Kom
   NIDN: 0223108404

3. Penguji I : Ruliansyah, M. Kom
   NIP. 19751122006041003

4. Penguji II : Reza Ade Putra, M.Cs
   NIP. 198701021018011001

Diuji di Pelembang pada tanggal 7 Desember 2018
Waktu : 16.00-17.00 WIB
Hasil/IPK : B/3,46
Predikat : Sangat Memuaskan

Dekan,
Fakultas Sains dan Teknologi
UIN Raden Fatah

Dr. Dian Erlina, S.Pd. M.Hum.
NIP. 197301021999032001

HALAMAN PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama	: Yeni Rahayu
Tempat dan tanggal lahir	: 08 Desember 1996
Program Studi	: Sistem Informasi
NIM	: 14540170

Menyatakan dengan sesungguhnya bahwa:

1. Seluruh data, informasi, interpretasi serta pernyataan dalam pembahasan dan kesimpulan disajikan dalam Skripsi ini, kecuali yang disebutkan sumbernya ditulis dalam daftar pustaka adalah merupakan hasil pengamatan, penelitian, pengolahan, serta pemikiran saya dengan pengarahan dari para pembimbing yang ditetapkan.
2. Skripsi yang saya tulis ini adalah asli, bukan jiplakan dan belum pernah diajukan untuk mendapatkan gelar akademik, baik di UIN Raden Fatah maupun perguruan tinggi lainnya.
3. Apabila dikemudian hari ditemukan adanya bukti ketidakbenaran dalam pernyataan tersebut diatas, maka saya bersedia menerima sanksi akademis berupa pembatalan gelar yang saya peroleh melalui pengajuan karya ilmiah ini.

Demikian pernyataan ini dibuat dengan penuh kesadaran dan dapat dipertanggungjawabkan.

Palembang, 29 November 2018

Yang Membuat pernyataan,

Yeni Rahayu

NIM. 14540170

MOTTO

Even Though You Know How to Walk Backwards, Keep Trying to Step Forward

"Barang Siapa Menempuh Sebuah Jalan Untuk Menuntut Ilmu maka Allah Akan Memdahkan Untuk Jalan Menuju Syurga"

(HR. Muslim No.2699)

"Jika Engkau Berada Pada Waktu Sore Maka Jangan Menunggu Hingga Pagi dan Jika Engkau Berada Pada Waktu Pagi Maka Jangan Menunggu Hingga Sore. Manfaatkan Masa Sehatmu Sebelum Masa Sakitmu. Manfaatkan Masa Hidupmu Sebelum Datang Kematianmu."

(HR. Al-Bukhari)

Reach the Hereafter, Then the World Will Follow

PERSEMBAHAN

Kepada Tuhan yang Maha Esa, Allah SWT yang telah melimpahkan rahmat,hidayahnya dan kemudahan yang telah engkau berikan. Segala puji syukur senantiasa terpanjatkan kepada-Mu.

Shalawat beserta salam selalu tercurahkan kepada kekasih Allah, Nabi Agung, baginda Muhammad SAW.

Terimakasih kepada yang tersayang Ayahandaku Ngatiran dan Ibundaku Rumiati yang selalu memberikan do'a, cinta, kasih dan sayang serta pengorbanan baik materil maupun moril.

Terimakasih kepada yang tersayang dan yang selalu kurindukan Kakek Nangku Legiman dan Nenek Dokku Sukarni serta Om, Tante, Adek dan semua sanak saudaraku yang ada di pulau sebrang, Jawa Timur yang selalu memberikan semangat, doa dan dukungan terhadapku. Yang selalu bilang "Sekolah yang bener dan sungguh-sungguh biar cepet lulus Mbak Iyen dan cepet pulang ke Jawa".

Untuk Adikku tersayang Dwi Setiawati yang terus memberikan semangat dan yang sering banyak tanya "kapan ujian, kapan wisuda, entar kalau wisuda aku mau kesitu" dan yang sering minta beliin ini itu. Tapi karna bawelnya itulah yang buat rindu.

Kepada sahabat-sahabatku tersayang Geng WG, Sri Paiza alias Mpok Ijo, Suchi Andara Rezki alias Aneue Queue, Yiying alias Iyong, dan Yulianti alias Mak Mbing (Mak kami di WG, hihi...). Terimakasih atas kebersamaannya, semangat dan dukungan kalian hingga sampai saat ini semoga kita tetap solid dan menjadi sahabat Dunia Akhirat Insha Allah. Aamiin

Kepada Big Family's Information System F 2014 (SI F), kelas tergokil, terkocak…ter…ter… pokoknya, terimakasih atas kebersamaannya selama kurang lebih 4 tahun, yang saling menyemangati dan mendukung satu sama lain. Semoga tetap solid dan sukses terus kedepannya untuk kita semua. Setiap pertemuan pasti ada perpisahan, sedih ketika harus berpisah, bakalan rindu canda tawa dan kegokilan kalian. Sampai bertemu dengan kesuksesan masing-masing nantinya.

Terimakasih kepada teman-teman seperjuangan khususnya Sistem Informasi angkatan 2014, tetap semangat dan sukses terus untuk kita kedepannya.

Terimakasih kepada teman-teman KKN khususnya Kelompok 34, khususnya kepada Nadiah Fitriana dan Siti Yayu Rahayu yang selalu menyemangati dan saling mendukung. Sukses terus untuk kedepannya untuk kita semua.

Almamaterku UIN Raden Fatah alembang, Alumni SD-SMP-MA, Agama, Bangsa, dan Negara Indonesia.

AUDIT OF INFORMATION SECURITY SIMAK ONLINE INDO GLOBAL MANDIRI PALEMBANG UNIVERSITY BASED ON STANDARD ISO / IEC 27001: 2005

ABSTRACT

Academic Information System (SIMAK) Online The University of Indo Global Mandiri Palembang has never carried out an information security audit, causing organization to find it difficult to know the suitability of information security systems with established security procedures and standards. This study audits information security using the ISO / IEC 27001: 2005 standard which is a standard document of the Information Security Management System (ISMS). Auditing is obtained from the results of interviews, observations, and examination of existing data and evidence. Auditing results are based on 11 clauses of ISO / IEC 27001: 2005, information security on SIMAK Online The University of Indo Global Mandiri Palembang has implemented 83% of information security controls, but its implementation is still not optimal. The results of the information security audit show that there is still information security control that is not in accordance with the ISO / IEC 27001: 2005 standard so that recommendations are given for improving information security going forward.

Keywords: Audit, ISO / IEC 27001: 2005, Simak Online

AUDIT KEAMANAN INFORMASI SIMAK ONLINE UNIVERSITAS INDO GLOBAL MANDIRI PALEMBANG BERDASARKAN STANDAR ISO/IEC 27001:2005

ABSTRAK

Sistem Informasi Akademik (SIMAK) *Online* Universitas Indo Global Mandiri Palembang belum pernah dilakukan audit keamanan infomasi sehingga menyebabkan organisasi kesulitan mengetahui kesesuaian sistem keamanan infomasi dengan prosedur dan standar keamanan yang telah ditetapkan. Penelitian ini mengaudit keamanan informasi menggunakan standar ISO/IEC 27001:2005 yang merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI). Pengauditan didapatkan dari hasil wawancara, pengamatan, dan pemeriksaan data dan bukti yang ada. Hasil pengauditan berdasarkan 11 klausul ISO/IEC 27001:2005, keamanan informasi pada SIMAK *Online* Universitas Indo Global Mandiri Palembang telah mengimplementasikan sebanyak 83% terhadap kontrol keamanan informasi, namun pada penerapannya masih kurang optimal. Hasil audit keamanan informasi menunjukkan bahwa masih adanya kontrol keamanan informasi yang belum sesuai dengan standar ISO/IEC 27001:2005 sehingga diberikan rekomendasi untuk perbaikan keamanan informasi kedepannya.

Kata Kunci: Audit, ISO/IEC 27001:2005, Simak Online

KATA PENGANTAR

Puji dan syukur penulis kehadirat Allah SWT karena akhirnya skripsi ini bisa terselesaikan dengan baik dan tepat pada waktunya.

Skripsi yang penulis buat dengan judul Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Berdasarkan Standar ISO/IEC 27001:2005 dibuat sebagai salah satu syarat untuk menyelesaikan studi di program studi sistem informasi Fakultas Sains dan Teknologi.

Dalam Penyusunan skripsi ini banyak ditemukan kesulitan-kesulitan dan hambatan-hambatan, namun berkat inayah Allah SWT, serta bantuan dari berbagai pihak segala kesulitan dan hambatan tersebut dapat diatasi, sehingga skripsi ini dapat terselesaikan. Untuk itu, penulis mengucapkan terima kasih kepada yang terhormat:

1. Bapak Prof. Drs. H. Sirozi, MA.Ph.D, selaku Rektor Universitas Islam Negeri Raden Fatah Palembang
2. Ibu Dr. Dian Erlina, S.Pd. M.Hum, selaku Dekan Fakultas Sains dan Teknologi
3. Bapak Ruliansyah, M.Kom., selaku Ketua Program Studi Sistem Informasi
4. Ibu Rusmala Santi, M.Kom., selaku Pembimbing I yang telah memberikan bimbingan penulisan proposal ini.
5. Bapak Muhamad Kadafi, M.Kom., selaku Pembimbing II yang telah memberikan bimbingan penulisan proposal ini.
6. Bapak-bapak dan ibu-ibu dosen serta staf Fakultas Sains dan Teknologi UIN Raden Fatah Palembang.
7. Ayah, ibu, dan saudara-saudaraku yang telah mendukung dan memberikan motivasi.
8. Rekan-rekan seperjuangan Angkatan 2014 di Fakultas Sains dan Teknologi UIN Raden Fatah Palembang.
9. Almamaterku.

Akhirnya kepada semua pihak, penulis sertakan do'a semoga Allah SWT membalas pahala kebaikan yang telah diberikan agar berlipat ganda dan berkenan memberikan banyak manfaat bagi pembacanya.

Palembang, 29 November 2018

Yeni Rahayu

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Audit merupakan suatu proses pengumpulan, pemeriksaan, dan evaluasi bukti mengenai pernyataan tentang kegiatan suatu organisasi dengan tujuan untuk mengetahui apakah pelaksanaannya telah sesuai kriteria, ketetapan dan kebijakan yang telah ditetapkan. Audit dilakukan untuk memastikan apakah pengendalian yang sudah ada telah memadai dan dapat mengurangi resiko. Dengan audit dapat membantu dalam pengukuran tingkat keberhasilan kinerja pada suatu perusahaan atau organisasi dan hasil dari audit merupakan hasil temuan serta rekomendasi untuk organisasi atau perusahaan yang digunakan untuk pengembangan kinerja kedepannya

Audit sistem informasi yaitu proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah sistem mengamankan asset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumber daya secara efisien (Weber, 1999:10). Audit sistem informasi bertujuan untuk mengukur sejauh mana tingkat keberhasilan suatu sistem informasi pada suatu organisasi atau perusahaan. Dengan adanya audit sistem informasi agar suatu organisasi dan perusahaan lebih memperhatikan perkembangan sistem dan dapat mengevaluasi apakah sistem informasi yang diimplementasikan telah sesuai dengan kebijakan yang telah ditetapkan.

Dalam bidang audit sistem informasi banyak *framework* yang sering kali digunakan diantaranya COBIT, COSO, ITIL, ISO dan lain-lain. Pada penelitian ini salah satu metode yang akan digunakan yaitu metode ISO/IEC 27001:2005,

standar yang bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis resiko dan dirancang untuk menjamin kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai resiko dan memberi keyakinan tingkat keamanan informasi yang berkepentingan. Metode ini juga sangat fleksibel dikembangkan karena sangat tergantung akan kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai dan ukuran struktur organisasi.

Universitas Indo Global Mandiri Palembang sendiri telah menerapkan sistem informasi akademik berbasis *website* sebagai sarana penunjang kegiatan akademik. Dalam hal ini perguruan tinggi berusaha untuk meningkatkan efisiensi dan efektifitas kinerja dengan mengadopsi dan mengimplementasikan sebuah sistem informasi. Sistem yang telah diterapkan yaitu Sistem Informasi Akademik (SIMAK) yang berbasis *online*. Sistem informasi tersebut untuk menghadapi kendala administrasi akademik dan kemahasiswaan yang melibatkan antara mahasiswa, dosen, pegawai dan lain-lain. Informasi dapat diakses dari komputer mana saja yang tersambung dengan koneksi internet.

Karena penelitian dilakukan disuatu perusahaan atau organisasi yang semakin tinggi tingkat implementasi teknologi, sistem pengelolaan dalam keamanan infomasi menjadi sangat penting untuk dipahami dan diupayakan agar informasi dapat dikelola dengan benar, sehingga dapat lebih fokus dalam pencapaian visi dan misi suatu organisasi atau perusahaan. Selain itu, sistem informasi yang telah diterapkan tidak selalu dapat menjawab kebutuhan organisasi, terkadang telah memenuhi sebagian kebutuhan dari organisasi, disebabkan masih saja terjadi insiden *error*, kehilangan data suatu informasi, penyalahgunaan oleh

pihak-pihak yang tidak memiliki hak, keamanan terkait informasi yang dapat mengakibatkan pengelolaan teknologi informasi menjadi tidak efektif dan efisien. Untuk memastikan apakah sistem informasi yang ada telah diterapkan dengan baik atau sesuai prosedur atau standar keamanan yang telah ditetapkan dan untuk mempertahankan kelangsungan bisnis serta mengurangi ancaman serta resiko akibat kegiatan pengelolaan dan pemeliharaan data. Dengan permasalahan ini, penelitian yang ingin dilakukan di Universitas Indo Global Mandiri Palembang yaitu meneliti Sistem Informasi Akademik (SIMAK) yang telah dibangun dalam bentuk audit keamanan informasi yang bertujuan untuk mengetahui tingkat keamanan informasi suatu sistem informasi pada SIMAK tersebut.

Berdasarkan penjelasan yang diuraikan sebelumnya maka akan dilakukannya penelitian tentang audit keamananan informasi yang menggunakan ISO/IEC 27001:2005 dengan judul "Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001:2005".

1.2 Rumusan Masalah

Adapun rumusan masalah dari uraian latar belakang diatas sebagai berikut:

1. Bagaimana mengetahui tingkat keamanan simak *online* Universitas Indo Global mandiri Palembang berdasarkan standar ISO/IEC 27001:2005?
2. Bagaimana menyusun rekomendasi keamanan sistem informasi berdasarkan standar ISO/IEC 27001:2005?

1.3 Batasan Masalah

Agar pembahasan ini terarah dan tidak menyimpang dari rumusan masalah, maka penulis membatasi pada:

1. Sistem yang diaudit adalah Simak *Online* pada Universitas Indo Global Mandiri Palembang dengan menggunakan Standard ISO/IEC 27001:2005.
2. Studi kasus dilakukan pada Universitas Indo Global Mandiri Palembang dengan pengguna sistem pada divisi IT sebagai responden.
3. Data-data yang digunakan dalam analisis dan pembahasan masalah adalah data yang diperoleh dari hasil observasi, dokumentasi, studi kepustakaan dan wawancara.

1.4 Tujuan Penelitian

Tujuan dari penelitian yang dilakukan di Universitas Indo Global Mandiri Palembang sebagai berikut :

1. Mengetahui tingkat keamanan simak *online* Universitas Indo Global Mandiri Palembang berdasarkan standar ISO/IEC 27001:2005
2. Membuat rekomendasi berdasarkan hasil audit keamanan informasi simak *online* Universitas Indo Global Mandiri Palembang

1.5 Manfaat Penelitian

Evaluasi dari hasil audit yang akan dihasilkan dapat memberikan manfaat sebagai berikut :

1. Audit *Information Security Management System* (ISMS) memberi pemahaman yang lebih baik mengenai aset informasi dan proses manajemen keamanan informasi yang diperlukan.
2. Audit sistem informasi membantu mengarahkan implementasi sistem manajemen keamanan informasi berdasarkan kepada pertimbangan resiko.
3. Menghasilkan dokumen temuan dan rekomendasi dari hasil audit keamanan informasi Simak *Online* Universitas Indo Global Mandiri Palembang yang dapat digunakan sebagai dokumentasi pengembangan sistem yang ada.

BAB II

LANDASAN TEORI DAN TINJAUAN PUSTAKA

2.1 Landasan Teori

Teori yang membahas keilmuan yang mendasari masalah yang diteliti, yang terdiri dari teori-teori dasar dan teori-teori khusus.

2.1.1 Audit

Audit secara umum merupakan sebuah kegiatan yang melakukan pemeriksaan untuk menilai dan mengevaluasi sebuah aktivitas atau objek seperti implementasi pengendalian internal pada sistem informasi akuntansi yang pekerjaannya ditentukan oleh manajemen atau proses fungsi akuntansi yang membutuhkan *improvement*.

Menurut Mulyadi (2012), audit adalah Suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara obyektif mengenai pernyataan-pernyataan tentang kegiatan dan kejadian ekonomi, dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan.

Berdasarkan pengertian-pengertian diatas, penulis menyimpulkan bahwasannya audit adalah kegiatan pemerikasaan untuk menilai dan evaluasi objek untuk menetapkan tingkat kesesuaian pernyataan dengan kriteria yang telah ditetapkan

2.1.2 Audit Sistem Informasi

Audit sistem informasi sendiri merupakan proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah sistem mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumber daya secara efisien (Weber, 1999:10).

Audit sistem informasi (SI) sebagai kegiatan tersendiri, terpisah dari audit keuangan. Sebetulnya audit SI pada hakekatnya merupakan salah satu dari bentuk audit operasional, tetapi kini audit SI sudah dikenal sebagai satu satuan jenis audit tersendiri yang tujuan utamanya lebih untuk meningkatkan IT *governance* yaitu komitmen, kesadaran dan proses pengendalian manajemen organisasi terhadap sumber daya sistem informasi. Sebagai suatu audit operasional terhadap manajemen sumber daya informasi, yaitu efektivitas, efisiensi dan ekonomis tidaknya unit fungsional sistem informasi pada suatu organisasi atau pengelolaan sistem informasi pada suatu organisasi (Gondodiyoto, 2014:444).

Berdasarkan pengertian audit sistem informasi menurut beberapa ahli, penulis menyimpulkan bahwa audit sistem informasi adalah suatu proses untuk pengumpulan dan penilaian bukti-bukti mengenai pernyataan atau kegiatan terhadap efektivitas, efisiensi dan ekonomisnya fungsional dari suatu sistem informasi.

2.1.3 Fungsi dan Tujuan Audit Sistem Informasi

Fungsi dari adanya audit sistem informasi, untuk memastikan apakah sistem informasi telah dirancang dan diterapkan sesuai dengan prosedur dan standar yang telah ditetapkan. Audit juga dilakukan untuk memastikan apakah

pengendalian yang telah ada sudah memadai dan dapat mengurangi resiko yang dihadapi (Gondodiyoto, 2014:10).

Sedangkan tujuan audit teknologi informasi (*audit objectives*) lebih ditekankan pada beberapa aspek penting, yaitu pemeriksaan dilakukan untuk dapat menilai : (a) apakah sistem komputerisasi suatu organisasi atau perusahaan (*system effectiveness*), (c) apakah sistem terkomputerisasi tersebut sudah memanfaatkan sumber daya secara efesien (*efficiency*), dan (d) apakah terjamin konsistensi dan keakuratan datanya (*data integrity*) (Gondodiyoto, 2014:474)

2.1.4 Tahapan Audit Sistem Informasi

Dalam melaksanakan audit sistem informasi, auditor harus melaksanakan tahap-tahap audit. Menurut Gallegos dalam bukunya "*Audit and Control of Information System*" tahapan audit yaitu :

1. Perencanaan (*Planning*), tahap perencanaan yang dilakukan adalah menentukan ruang lingkup, objek yang akan diaudit, standar evaluasi dari hasil audit dan komunikasi dengan manajemen pada organisasi yang bersangkutan dengan menganalisi visi, misi, sasaran dan tujuan objek yang diteliti serta strategi, kebijakan-kebijakan yang terkait dengan pengolahan investigasi.
2. Pemeriksaan lapangan (*Field Work*), tahap ini yang dilakukan adalah pengumpulan informasi yang dilakukan dengan cara mengumpulkan data dengan pihak-pihak yang terkait. Hal ini dapat dilakukan dengan menerapkan berbagai metode pengumpulan data yaitu : wawancara, kuesioner ataupun survei ke lokasi penelitian.

3. Pelaporan (*Reporting*), setelah proses pengumpulan data maka akan didapat data yang akan diproses dari hasil audit.
4. Tindak lanjut (*Follow Up*), tahap yang dilakukan adalah memerikan laporan audit berupa rekomendasi tindakan perbaikan kepada manejemen objek yang diteliti, untuk selanjutnya wewenang perbaikan menjadi tanggung jawan manajemen apakah akan diterapkan atau hanya menjadi acuan untuk perbaikan di masa yang akan datang. (Armansyah, 2017)

2.1.5 ISO/IEC 27001 : 2005

ISO/IEC 27001:2005 yang merupakan standar sistem informasi yang diterbitkan *International Organization for Standardization* dan *International Electronical Comission* pada bulan Oktober 2005 untuk menggantikan standard BS7799-2. ISO/IEC 27001 ini terus mengalami pembaharuan. Standar ini dibuat sebagai model untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan dan perbaikan. Manajemen Keamanan Informasi (SMKI) merupakan keputusan strategis. Desain dan penerapan SMKI dari suatu organisasi dopengaruhi kebutuhan dan sasaran organisasi. Standar ini dan sistem pendukungnya diperkirakan akan berubah dari waktu ke waktu. ISO/IEC 27001 memberikan gambaran umum mengenai kebutuhan perusahaan/organisasi dalam usahanya untuk mengimplementasikan konsep-konsep keamanan informasi. Penerapan ISO/IEC 27001 disesuaikan dengan tujuan, sasaran dan kebutuhan organisasi (ISO/IEC 27001:2005, 2005).

Aspek-aspek keamanan informasi dalam suatu organisasi :

1. *Confidentiality* adalah keamanan informasi seharusnya menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu.
2. *Integrity* adalah keamanan sistem informasi seharusnya menjamin kelengkapan sistem informasi dan menjaga dari korupsi, kerusakan atau ancaman lain yang menyebabkan berubahnya informasi dari aslinya.
3. Menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya ganguan dan tidak dalam format yang tidak bisa digunakan. (Rosmiati,2016)

Sumber : Rosmiati **(2016)**

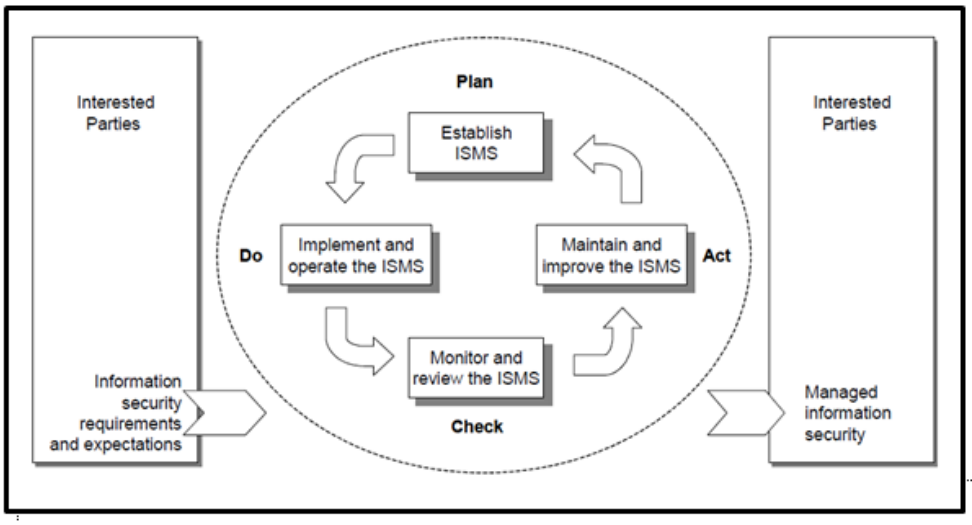
Gambar 2.1 Aspek Keamanan Sistem Informasi

Standar ini mengadopsi *"Plan-Do-Check-Act"* (PDCA) model, yang digunakan untuk mengatur semua proses Standar Manajemen Keamanan Informasi (SMKI). Penerapan model PDCA juga akan mencerminkan prinsip-prinsip sebagaimana diatur dalam pedoman OECD (2002) yang mengatur keamanan sistem informasi. Standar ini memberikan model untuk menerapkan prinsip-prinsip dalam

pedoman yang mengatur penilaian resiko, desain keamanan dan implementasi, manajemen keamanan dan penilaian.

Dalam model PDCA, keseluruhan proses SMKI dapat dipetakan seperti pada gambar berikut :

Sumber : ISO/IEC (2005)



Gambar 2.2. Model PDCA Proses SMKI

Dari Gambar 2.2 yaitu uraian dari Model PDCA (*Plan, Do, Check* dan *Act*) :

1. *Plan* (Penetapan SMKI), menetapakan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk pengelolaan resiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai edngan kebijakan dan sasaran organisasi secara menyeluruh.
2. *Do* (penerapan dan pengoperasian SMKI), menerapkan dan mengoperasikan kebijakan, pengendalian, proses dan prosedur SMKI.
3. *Check* (pemantauan dan pengkajian SMKI), mengakses dan apabila berlaku, mengukur kinerja proses terhadap kebijakan, sasaran SMKI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian

4. *Act* (peningkatan dan pemeliharaan SMKI), mengambil tindakan korektif dan pencegahan berdasarkan hasil internal audit SMKI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SMKI.

2.1.6 Gap Analysis

Teknik analisis yang digunakan pada penelitian ini adalah *Gap Analysis* (Analisa Kesenjangan) yaitu perbandingan kinerja aktual dengan kinerja potensial atau yang diharapkan. Analisa ini juga mengidentifikasi tindakan-tindakan apa saja yang diperlukan untuk mengurangi kesenjangan atau mencapai kinerja yang diharapkan dimasa yang akan datang.

Gap Analysis dilakukan untuk mengetahui kondisi kesenjangan keamanan informasi. Berbagai temuan audit dianalisa dengan membandingkan fakta yang ada di lapangan dengan standar yang berlaku yaitu ISO/IEC 27001:2005. Kondisi yang tampak pada temuan hasil audit dibuat analisa dampak dan rekomendasi untuk meningkatkan keamanan informasi sesuai target yang ingin dicapai. (Bramantiyo, 2016)

2.1.7 Alat dan Bahan Audit

Alat-alat yang dipakai dalam mengaudit sistem informasi yaitu :

1. Microsoft Office adalah perangkat lunak paket aplikasi perkantoran buatan Microsoft Windows dan Mac OS X. Beberapa aplikasi didalam microsoft office yang terkenal adalah Excel, Word, dan PowerPoint.

2. Kamera adalah alat untuk pengambilan objek berupa gambar atau video untuk didokumentasikan biasanya tersimpan dalam bentuk format jpg, jpeg, mp4, mkv, dan lainnya.
3. *Recording* adalah alat perekam untuk pengambilan objek berupa suara, disimpan dan didokumentasikan dalam bentuk suara biasanya tersimpan dalam bentuk format aac, m4a dan lainnya.

Jenis bahan bukti yang dapat dikategorikan dengan beberapa cara didalam melakukan audit yaitu sebegai berikut :

1. Fakta / bukti hasil analisis. Kesimpulan aditor yang didasarkan bukti audit yang berasal dari hasil pemikiran yang terkait dengan kenyataan atau fakta yang relevan.
2. Bukti langsung/ tidak langsung. Bukti audit yang bersifat fakta atau dokumen sah yang langsung terkait dengan kegiatan pemeriksaan audit sistem informasi. Sedangkan bukti tidak langsung adalah kesimpulan auditor berdasarkan bahan bukti tertentu
3. Bukti utama (primer)/sekunder. Bahan utama/sekunder yaitu data yang bersifat utama seperti mengenai data Sistem Informasi, surat perjanjian, surat penelitian dan surat balasan lainnya yang bersifat resmi.
4. *Testimonial Evidence.* Informasi yang diperoleh dari pihak atau orang tertentu dalam bentuk tulis maupun lisan (atau bersifat hasil analisis). Bukti ini diperoleh melalui hasil wawancara).

2.2 Tinjauan Pustaka

Penelitian sebelumnya pernah dilakukan oleh Kementrian Pemuda dan Olahraga dengan judul "Audit Keamanan Informasi Kemenpora". Dilaksanakan audit IS terdapat beberapa kendala seperti dukungan manajemen puncak yang penuh, petugas TI yang minim pengalaman, dan keterbukaan dokumen dari vendor yang sebelumnya menjalin kerjasama dengan kemenpora dalam pengembangan sistem, semua itu harus segera diminimalisasi dan diselesaikan dengan segera dan menyeluruh. Keamanan informasi kemenpora harus mencapai level tertinggi sesuai dengan kebutuhan dan kemampuan yang dimiliki olehnya. Dari hasil auditnya yaitu level keamanan informasi di lingkungan Kemenpora yang maksimal baik ditingkat pusat dan daerah diharapkan menjadi motivasi bagi perkembangan Kemenpora ke depan. Hal ini diharapkan secara tidak langsung dapat menjadi tolak ukur bagi instansi lainnya.

Beberapa penelitian selanjutnya yang dilakukan oleh Bramantiyo Eko Putro dengan judul "Analisa *Control Assesment Audit* pada klausul A.5 *Security Policy* hingga klausul A.9 *Physical And Environment Security* Telkom Flexi Kebon Sirih Jakarta Pusat Menggunakan ISO/IEC 27001". Yang melatarbelakangi dilakukan penelitiaannya yaitu Kemenkominfo sebagai lembaga yang berwenang mengenai keamanan informasi di Indonesia menyadari mengenai keamanan informasi di instansi pemerintah dan swasta banyak yang belum memiliki atau sedang menyusun kerangka kerja keamanan informasi sesuai standar ISO/IEC 27001. Oleh karena itu, penting bagi perusahaan di Indonesia untuk melakukan audit keamanan data digital berdasarkan standar yang berlaku. Audit keamanan data digital yang sesuai dengan standar ISO/IEC 27001 juga kurang menjadi perhatian

utama bagi Telkom Flexi yang bergerak dalam bisnis informasi dan teknologi. Dalam hasil audit yang dilaksanakan yaitu kinerja pengelolaan keamanan informasi Telkom Flexi Kebon Sirih telah dilaksanakan bagian *Risk and Business Continuity*. Pengelolaan keamanan informasi yang berkaitan dengan perlindungan data digital, *Gap Analysis* yang dilakukan terhadap pengelolaan keamanan informasi Telkom Flexi ditemukan beberapa temuan yang masih belum sesuai dengan standar ISO/IEC 27001. Rekomendasi yang disarankan yaitu manajemen Telkom Flexi perlu meningkatkan perlindungan *Phsycal and environment* dengan mendesain gedung yang menggunakan tembok tahan api, meminimumkan getaran pada gedung, merapikan dan melindungi seluruh kabel baik berkaitan dengan pengolahan informasi ataupun tidak dan perlu melaksanakan audit dengan standar yang berlaku yaitu standar ISO/IEC 27001. Sebaiknya audit dilaksanakan dalam interval yang telah direncanakan.

Penelitian selanjutnya yaitu oleh Riawan Arbi Kusuma dengan judul "Audit Keamanan Sistem Informasi Berdasarkan Standard SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Negeri Sunan Kalijaga Yogyakarta". Penelitiannya dilatar belakangi dengan mengingat pentingnya pengamanan suatu informasi yang harus mencakup sekurang-kurangnya prosedur pengendalian dokumen, prosedur pengendalian rekaman, prosedur pengendalian informasi, prosedur tindakan perbaikan dan pencegahan, prosedur pengamanan insiden dan prosedur pemantauan maka dilakukannya audit sistem informasi. Hasil penelitiannya, menunjukkan bahwa perencanaan audit untuk kegiatan penelitian audit sistem informasi dengan maturity level saat ini berada pada angka 1,85 dan kemudian dibulatkan menjadi 2 yaitu *Repeatable but Intuitive,* artinya pada

pengamanan sistem informasi pada Sistem Informasi akademik UIN Sunan Kalijaga Yogyakarta yang dikelola UPT PTIPD telah distandardkan tetapi belum didokmentasikan. Semua proses pengaman sistem informasi untuk SIA baru sebatas mengikuti pola yang teratur dimana prosedur serupa diikuti pegawai lainnya tetapi tidak ada pelatihan formal sebelumnya dan tidak ada standard prosedur yang digunakan sebagai acuan. Saran dari audit dalam penelitiannya yaitu, perlu ditingkatkannya kesadaran dari pimpinan perusahaan serta *stakeholder* mengenai pentingnya keamanan informasi dalam mendukung tercapainya visi misi perusahaan.

Beberapa peneliti selanjutnya oleh Reza Zulfikar, dkk dengan judulnya "Audit Keamanan Informasi Studi Kasus : PT. XYZ". Yang melatarbelakangi penelitiannya yaitu keamanan informasi PT.XYZ dinilai masih lemah. Selain itu monitoring dan evaluasi dari pihak yang berwenang di nilai masih kurang, sehingga kriteria keamanan informasi belum terpenuhi. Kurangnya monitoring dan evaluasi ini menjadi salah satu penyebab masalah belum terpenuhinya kriteria keamanan pada PT.XYZ. Hasil dari penelitian yakni kebijakan prosedur, instruksi da dokumentasi keamanan informasi yang ada dan berlaku di PT.XYZ belum dikaji ulang dan cakupannya belum komprehensif mengatur aspek keamanan dari ISO 27001/ISMS. Dan rekomendasi yang diberikan oleh peneliti adalah sebaiknya dilakukan sosialisasi dan program kepedulian keamanan direncakan dan dilakukan pelatihan terkait keamanan informasi serta menyusun kebijakan keamanan informasi yang komprehensif berdasarkan praktik terbaik lainnya sesuai kebutuhan organisasi.

Berbeda dengan penelitian Devi Puspitasari yang judulnya "Audit Sistem Manajemen Keamanan Sistem Informasi Menggunakan ISO SNI 27001 Pada Sistem Informasi Apotek Sanata Dharma". Penelitiaannya dilatarbelakangi karena pada Apotek bukan berarti tidak perlu adanya pengamanan sistem, untuk menjaga keamanan informasinya perlu dilakukan audit keamanan informasi. Yang hasilnya yaitu proses audit sistem informasi Apotek Sanata Dharma dengan penilaian maturity 1,8 (*Repeatable bt Intuitive*) yang artinya proses mengikuti pola yang teratur dimana prosedur serupa diikuti pegawai/karyawan lainnya tetapi tidak ada pelatihan formal sebelumnya dan tidak ada standard prosedur yang digunakan sebagai acuan. Peneliti juga memberikan rekomendasi untuk peningkatan keamanan sistem informasi Apotek Sanata Dharma sesuai dengan standard ISO/SNI 27001 yaitu Pada klausul kontrol pengelolaan asset perlu dibuat kebijakan tentang pengelolaan aset dan disosialisasikan kepada karyawan.

Penelitian selanjutnya yang dilakukan oleh Danastri Rasmona Windirya dengan judulnya "Audit Keamanan Sistem Informasi pada Instalasi Sistem Informasi Manajemen RSUD Bangil Berdasarkan ISO 27002". Yang melatarbelakangi penelitiannya yaitu pengelolaan Instalasi SIM-RS yang kurang terlayani degan cepat dengan instalasi SIM-RS yang disimpan tiba-tiba hilang atau rusak sehingga data yang akan disampaikan tidak lengkap atau utuh dan data instalasi yang disampaikan tidak sesuai dengan kenyataan yang ada atau tidak valid sehingga membuat pihak instalasi SIM-RS kerja dua kali untuk mendapatkan kesesuaian laporan data yang ada. Hasil dari penelitian yaitu SIM-RS Bangil telah berhasil dilakukan sesuai dengan standar ISO 27002 pada kontrol keamanan aset, keamaan sumber daya manusia, keamanan fisik dan lingkungan, kontrol akses dan

akuisi sistem informasi, pembangunan dan pemeliharaan. Hasil pemeriksaan kontrol keamanan audit diperoleh tingkat kedewasaan 3,22 yaitu pro aktif artinya sebagian besar proses keamanan suda diterapkan. Dan saran yang diberikan yaitu instalasi SIM-RS di RSUD Bangil harus segera menerapkan kebijakan dan prosedur untuk mengatasi insiden kelemahan keamanan informasi.

Berdasarkan referensi dari beberapa penelitian yang telah dilaksanakan sebelumnya, maka perbedaan yang dimiliki dan diusulkan penulis yaitu audit keamanan informasi simak online pada Universitas Indo Global Mandiri Palembang berdasarkan standard ISO/IEC 27001:2005 dengan 11 klausul dan kontrol keamanan yang lengkap, bertujuan untuk mengetahui keamanan informasi apakah sistem informasi yang diterapkan sesuai dengan standar atau prosedur yang telah ditetapkan. Teknik analisa yang digunakan yaitu *gap analysis* yaitu teknik analisa yang berfungsi untuk melihat kesenjangan dari kondisi yang ada di lapangan dan kondisi ideal yang sesuai dengan standard ISO/IEC 27001:2005. Dari hasil temuan audit tersebut kondisi yang tampak akan dianalisa dampak dan rekomendasinya. Hasil penelitian dari audit keamanan informasi ini berupa evaluasi yang kemudian menghasilkan rekomendasi perbaikan sistem pengendalian internal yang ada pada sistem informasi akademik pada Universitas Indo Global Mandiri Palembang.

BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah deskriptif yaitu penelitian yang dimaksudkan untuk mengumpulkan informasi mengenai status suatu gejala yang ada, yaitu keadaan gejala menurut apa adanya pada saat penelitian dilakukan tanpa bermaksud membuat kesimpulan yang berlaku untuk umum dan generelasi (Fenti, 2017:88).

Penelitian deskriptif merupakan penelitian bukan eksperimen, karena tidak dimaksudkan untuk menguji hipotesis tertentu. Dalam penelitian deskriptif, setelah data dari seluruh responden atau sumber data lainnya terkumpul maka selanjutnya akan dilakukan analisis data. Kegiatan analisis data adalah mengelompokkan data berdasarkan variabel dan jenis responden, mentabulasi data, berdasarkan variabel dari responden, menyajikan data tiap variabel yang diteliti, dan melakukan perhitungan untuk menjawab rumusan masalah.

Teknik analisis data penelitian deskriptif yang diambil yakni analisis data data penelitian deskriptif yang bersifat non statistif yaitu analisis data dengan teknik analisis deskriptif kualitatif. Dimana analisis data dengan teknik analisis deskriptif kualitatif adalah analisis yang menggunakan tolok ukur. Analisis deskriptif kualitatif sejajar dengan penilaian karena mengarah pada predikat. Analisis deskriptif kualitatif merupakan penelitian yang bertujuan untuk menilai sejauh mana variabel yang diteliti telah sesuai dengan tolok ukur yang sudah ditetapkan.

3.2 Lokasi Penelitian

Lokasi penelitian dilakukan di Universitas Indo Global Mandiri Jl. Jenderal Sudirman No.629 KM. 4, 20 Ilir D. IV, Ilir Tim. I, Kota Palembang Sumatera Selatan 30129.

3.3 Alat dan Bahan Audit Sistem Informasi

Alat-alat yang digunakan dalam penelitian ini diantaranya :

1. Microsoft Office
2. Kamera
3. Alat perekam (*Handphone*)

Jenis bahan bukti yang dapat dikategorikan dengan beberapa cara didalam melakukan audit yaitu sebagai berikut :

5. Fakta / bukti hasil analisis, berupa hasil penyebaran wawancara kepada responden, dokumentasi, dan data tertulis lainnya
6. Bukti langsung, berupa surat balasan penelitian, data hasil observasi, dan data pegawai.
7. Bukti utama (primer)/sekunder, berupa data sistem informasi akademik, data pegawai, dan surat-surat penting lainnya.
8. *Testimonial Evidence*, berupa rekaman wawancara atau data lainnya yang bersifat analisis.

3.4 Metode Pengumpulan Data

Dalam hal ini metode penelitian yang digunakan adalah metode dengan cara mengumpulkan dan menggambarkan data mengenai keadaan secara langsung dari

lapangan atau tepatnya yang menjadi objek penelitian untuk mendapatkan data secara relevan.

Teknik pengumpulan data yang dilakukan dalam mencari dan mengumpulkan data serta mengolah informasi yang diperlukan menggunakan beberapa metode sebagai berikut:

1. Observasi (*observation*) merupakan teknik atau pendekatan untuk mendapatkan data primer dengan cara mengamati langsung obyek datanya. (Jogiyanto, 2008:89). Dalam hal ini akan dilakukan pengamatan secara langsung di Universitas Indo Global Mandiri Palembang atau pada objek yang diteliti dan meminta data kepada stakeholder.
2. Wawancara (*interview*) telah diakui sebagai teknik pengumpulan data/fakta yang penting dan banyak dilakukan dalam pengembangan sistem informasi. Wawancara memungkinkan analis sistem sebagai pewawancara (*interviewer*), dalam hal ini memberikan pertanyaan kepada pegawai bagian divisi IT yakni Badan Penunjang Teknis (BPT) Universitas Indo Global Mandiri Palembang.
3. Studi Kepustakaan, metode ini dilakukan dengan cara mengumpulkan, membaca, dan mempelajari data-data yang ada dari berbagai media, seperti buku-buku, hasil karya tulis, jurnal-jurnal penelitian, atau artikel-artikel dari internet yang berhubungan dengan masalah yang dibahas (Indrajani, 2015:1). Pengumpulan data yang dilakukan secara langsung dari sumber-sumber lain seperti membaca dan mempelajari buku dan jurnal yang berkaitan dengan penelitian ini.
4. Dokumentasi, menurut Margono (1997: 187) dokumentasi merupakan mengumpulkan data melalui peninggalan tertulis, seperti arsip-arsip dan buku-

buku tentang pendapat, teori atau hukum yang berhubungan dengan masalah penelitian. Dokumen yang diperlukan antara lain terkait objek penelitian.

3.5 Peran dan Tanggung Jawab Manajemen Aset Infomasi

Fokus *Auditee* atau pihak yang diaudit mengenai keamanan informasi terhadap simak *online* Universitas Indo Global Mandiri Palembang sebagai berikut:

Tabel 3.1 *Roles and Responsibilities*

JABATAN	KLAUSUL PEGENDALIAN AUDIT	*Auditee*
DIM (Director Information Manajemen)	ISO 27001 Klausul A.5 dan A.7	KASI bagian Biro Penunjang teknis
CIO (Chief Information Officer)	ISO 27001 klausul A.8, A.14, dan A.15	Kepala bagian Biro Penunjang Teknis
ISO (Information Security Officer)	Iso 27001 Klausul A.6, A.9, A.10, A.11 dan A.12	Bagian Teknisi, *Hardware* dan Jaringan

Dari Tabel 3.1, penentuan fokus *auditee* dikelompokkan berdasarkan jabatan yang disesuaikan dengan ISO/IEC 27001:2005. Untuk *jobdesk* yang ada di UIGM dapat dilihat dilampiran IV halaman 150. Berikut penjelasan peran dan tanggung jawab pada aset manajemen informasi menurut ISO 27001 Implementer's Forum (2009)

1. ***Director Information Management*** **(Direktur Manajemen Informasi)**

Manajemen informasi memastikan bahwa sumber daya manusia suatu organisasi dikelola sebagai aset perusahaan dan membantu dalam menetapkan arah strategis manajemen informasi dalam organisasi. Mereka menyediakan dukungan dan kepemimpinan kepada petugas yang bertanggung jawab untuk mengelola sumber informasi. Tanggung jawab DIM diantaranya yaitu :

a. Memberikan saran yang berkaitan dengan praktik manajemen informasi.

b. Berkontribusi pada arah strategis manajemen informasi termasuk dalam kebijakan, standar, pedoman dan prosedur.
c. Membantu unit bisnis untuk mengidentifikasikan kebutuhan dan persyaratan informasi.
d. Bekerja dengan *Chief Information Officer* untuk merencanakan dan mengimplementasikan sistem dan mengelola aset informasi biro secara efektif.

2. *Chief Information Officer* (Kepemilikan Delegasi)

CIO memiliki wewenang untuk mewakili organisasi untuk perlindungan dan keamanan aset informasi sebagai kepemilikan aset informasi didelegasikan kepada peran organisasi. CIO sebagian bersama dengan tanggung jawab yang ditentukan kepada petugas, kontraktor, pihak ketiga dengan operasional dan tanggung jawab. Tanggung jawab CIO diantaranya yaitu

b. Pemutakhiran daftar inventaris aset informasi
c. Mengidentifikasi tingkat klasifikasi aset informasi
d. Menentukan dan menetapkan perlindungan untuk memastikan kerasahasiaan, integritas, ketersediaan aset informasi
e. Menilai dan memantau upaya perlindungan untuk memastikan kepatuhan dan laporan ketidakpatuhan
f. Otorisasi akses kepada mereka yang memiliki kebutuhan bisnis informasi
g. Memastikan akses dihapus dari mereka yang tidak memiliki kebutuhan bisnis informasi.

3. ***Information Security Officer*** **(Petugas Keamanan Informasi)**

Petugas keamanan informasi bertanggung jawab untuk mengembangkan dan menerapkan kebijakan keamanan inforasi yang dirancang untuk melindungi informasi dan mendukung dalam segala hal. Sistem informasi dari hak akses yang tidak sah, penggunaan, penggunaan, korupsi atau penghancuran. Tanggung jawab ISO diantaranya yaitu :

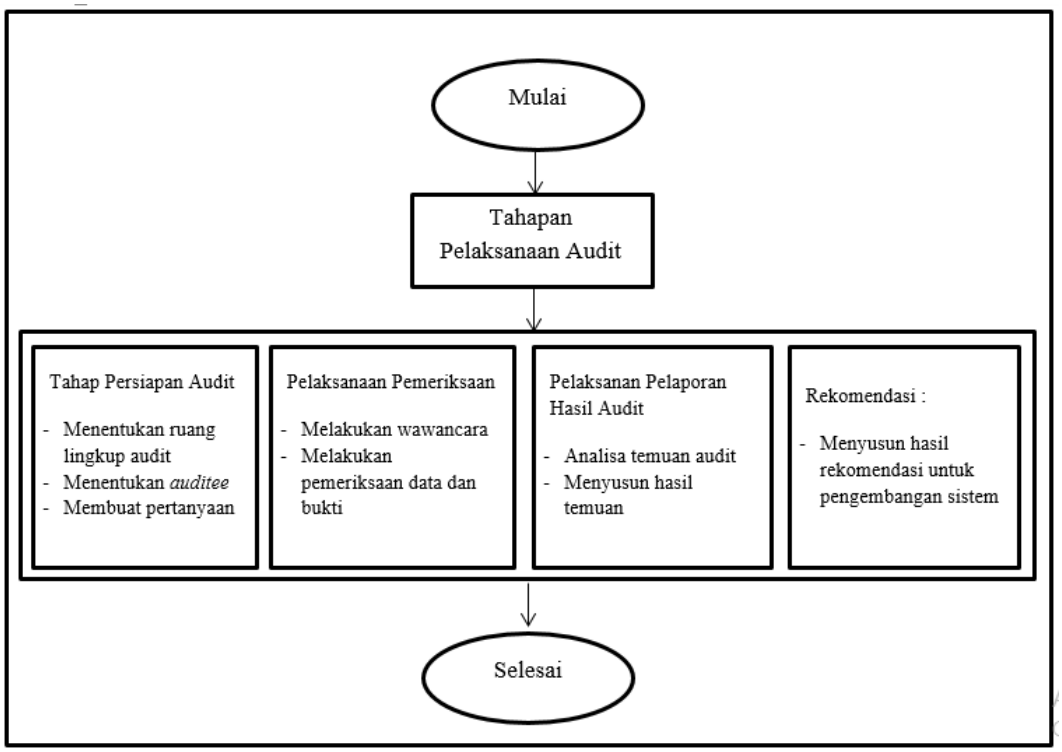
a. Mengembangkan kebijakan, prosedur, dan standar untuk memastikan keaanan, kerahasiaan, dan privasi informasi yang konsisten dengan informasi organisasi kebijakan keamanan.
b. Memantau dan melaporkan kejadian intrusi informasi dan mengaktifkan strategi mencegah insiden lebih lanjut.
c. Bekerja dengan penjaga informasi untuk memastikan bahwa aset informasi telah ditugaskan klasifikasi keamanan yang sesuai.
d. Pemeliharaan aset yang telah ditentukan pemilik aset.
e. System restart dan pemulihan sistem
f. Menerapkan setiap perubahan yang sesuai dengan prosedur manajemen perubahan.
g. Percadangan informasi.
h. Pemutakhiran daftar inventaris aset informasi.
i. Mengidentifikasi tingkat klasifikasi aset informasi.
j. Menentukan dan menerapkan perlindungan yang tepat untuk memastikan kerahasiaan, integritas, dan ketersediaan aset informasi.
k. Menilai dan memantau upaya perlindungan untuk memastikan kepatuhan dan laporan ketidakpatuhan.

l. Otorisasi akses kepada mereka yang memiliki kebutuhan bisnis untuk informasi.

m. Memastikan akses dihapus dari mereka yang tidak lagi memiliki kebutuhan bisnis informasi.

3.6 Tahapan Penelitian

Dalam melakukan penelitian ini, penulis melakukan langkah-langkah penelitian audit sistem informasi Universitas Indo Global Mandiri Palembang di ilustrasikan sebagai berikut :



Gambar 3.2 Tahapan Penelitian

Pada gambar 3.2 menggambarkan penelitian ini dilakukan dengan beberapa tahapan, yaitu :

5. Tahap persiapan audit
    a. Menentukan ruang lingkup audit yaitu menentukan ruanglingkup dan batasan sesuai dengan organisasi, lokasi, aset dan teknologi yang terkait dengan pelaksanaan audit
    b. Menentukan *auditee* yaitu memilih *auditee* berdasarkan klausul yang telah ditetapkan.
    c. Membuat pertanyaan yaitu membuat daftar pertanyaan berdasarkan pernyataan kontrol pengendalian audit. Pertanyaan tersebut akan dijadikan acuan dalam melakukan wawancara pada pihak yang telah ditentukan sebelumnya.

2. Tahap pelaksanaan dan pemeriksaan
    a. Melakukan wawancara yaitu melakukan wawancara berdasarkan pertanyaan yang telah dibuat pada pihak yang telah ditentukan sebelumnya.
    b. Melakukan pemeriksaan data dan bukti yaitu melaksanakan pemeriksaan dengan melakukan wawancara dan observasi langsung kepada *auditee* sesuai dengan ruang lingkup klausul, bukti adanya implementasi keamanan di perusahaan tersebut untuk mendapatkan temuan mengenai fakta terkait permasalahan yang ada.
3. Pelaksanaan pelaporan hasil
    a. Analisa temuan audit yaitu menganalisa hasil temuan audit dengan menggungan ceklist *gap analysis* untuk melihat kesenjangan implementasi

keamanan informasi dengan embandingkan fakta yang ada dilapangan dengan standar yang berlaku pada ISO/IEC 27001:2005. Kondisi yang tampak pada temuan hasil audit akan di analisa dampak dan rekomendasinya untuk meningkatkan keamanan sesuai dengan target.

b. Menyusun data hasil temuan audit yaitu menilai secara umum hasil untuk pengkjian Sistem Manajemen Keamanan Informasi (SMKI) dari hasil pemeriksaan dan analisa yang telah dilakukan

4. Rekomendasi, hasil pengujian dan penilaaian terhadap sistem yang telah diaudit dan memberikan rekomendasi atau saran untuk pengembangan sistem informasi kedepannya yang lebih baik.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Gambaran Umum Objek Penelitian

4.1.1 Sejarah Singkat Organisasi

Universitas Indo Global Mandiri Palembang (UIGM) didirikan berdasarkan Keputusan Menteri Pendidikan Nasional Indonesia nomor 83/D/0/2008 tanggal 20 Mei 2008, hasil dari mergerantara Sekolah Tinggi Manajemen Informatika & Komputer (STMIK) IGM dengan Sekolah Tinggi Teknologi Palembang (STTP) IGM. Pada awalnya UIGM terdiri dari 3 Fakultas, yaitu :

1. Fakultas Komputer terdiri dari Program Studi Teknik Informatika (S1), Sistem Informasi (S1), Teknik Komputer (D3), Manajemen Informatika (D3), Komputerisasi Akuntansi (D3);

   Saat ini Program Studi Teknik Komputer ditingkatkan dari D3 menjadi S1 Sistem Komputer, sedangkan untuk Komputerisasi Akuntansi tidak dilanjutkan, menyesuaikan dengan kebutuhan pasar.
2. Fakultas Teknik terdiri dari Program Studi Teknik Sipil (S1), Teknik Aritektur (S1), Perencanaan Wilayah dan Kota (S1), Survey dan Pemetaan (D3).
3. Fakultas Ekonomi terdiri dari Program studi Manajemen (S1) dan Akuntansi (S1)

Dengan berjalannya waktu, untuk memenuhi permintaan pasar secara bertahap dikembangkan beberapa Program Studi yang tergabung dalam 2 Fakultas, yaitu

1. Fakultas Ilmu Pemerintahan dan Budaya, terdiri dari program Studi Ilmu Pemerintahan dan Desain Komunikasi Visual (DKV).
2. Fakultas Keguruan Ilmu Pendidikan yang terdiri dari Program Studi Bahasa Inggris dan Matematika.

Untuk sementara Program Studi Matematika belum dijalankan mengingat keterbatasan minat dari masyarakat. Dengan demikin Unversitas IGM memiliki 5 Fakultas dengan 14 Program Studi. Program Studi dimaksud akan terus dievaluasi, dibuka atau ditutup akan disesuaikan dengan kebutuhan pasar.

Secara umum, target pendidikan yang hendak dicapat pada masing-masing tingkatan Program Studi yaitu :

1. Program S2 bertujuan menghasilkan Sarjana yang memiliki kemampuan mengembangkan berbagai hipotesa dari berbagai permasalahan yang dihadapi dan membuktikan sesuai dengan profesi ilmunya, untuk dijadikan referensi dalam menyelesaika masalah yang sama dikemudian hari.
2. Program S1 bertujuan menghasilkan Sarjana yang mempunyai kemampuan menganalisis suatu permasalahan dengan mengembangkan alternatif solusinya serta dapat mengimplementasikannya sesuai bidang ilmu yang dimiliki.
3. Program D3 bertujuan menghasilkan tenaga profesional Ahli Madya (Amd) yang mempunyai kemampuan teknis dan wawasan untuk mengimplementasikan keahliannya sesuai bidang ilmu yang dimiliki.

4.1.2 Visi dan Misi Organisasi

Dimulai dari cita-cita yang sederhana untuk mengabdi dalam dunia pendidikan, akhirnya menginspirasi untuk terus berarya membawa Lembaga IGM ke kancah Dunia Global, masuk dalam 500 Universitas terbaik di dunia pada pertengahan abad ke 21. Untuk memenuhi mimpi tersebut, dalam jangka satu dasawarsa kedepan, UIGM telah memformulasikan visi dan misinya sebagai berikut :

1. Visi

Adapun visi Universitas Indo Global Mandiri Palembang adalah Menjadi Universitas yang menghasilkan SDM professional dan integritas, untuk mengisi dan menciptakan peluang kerja.

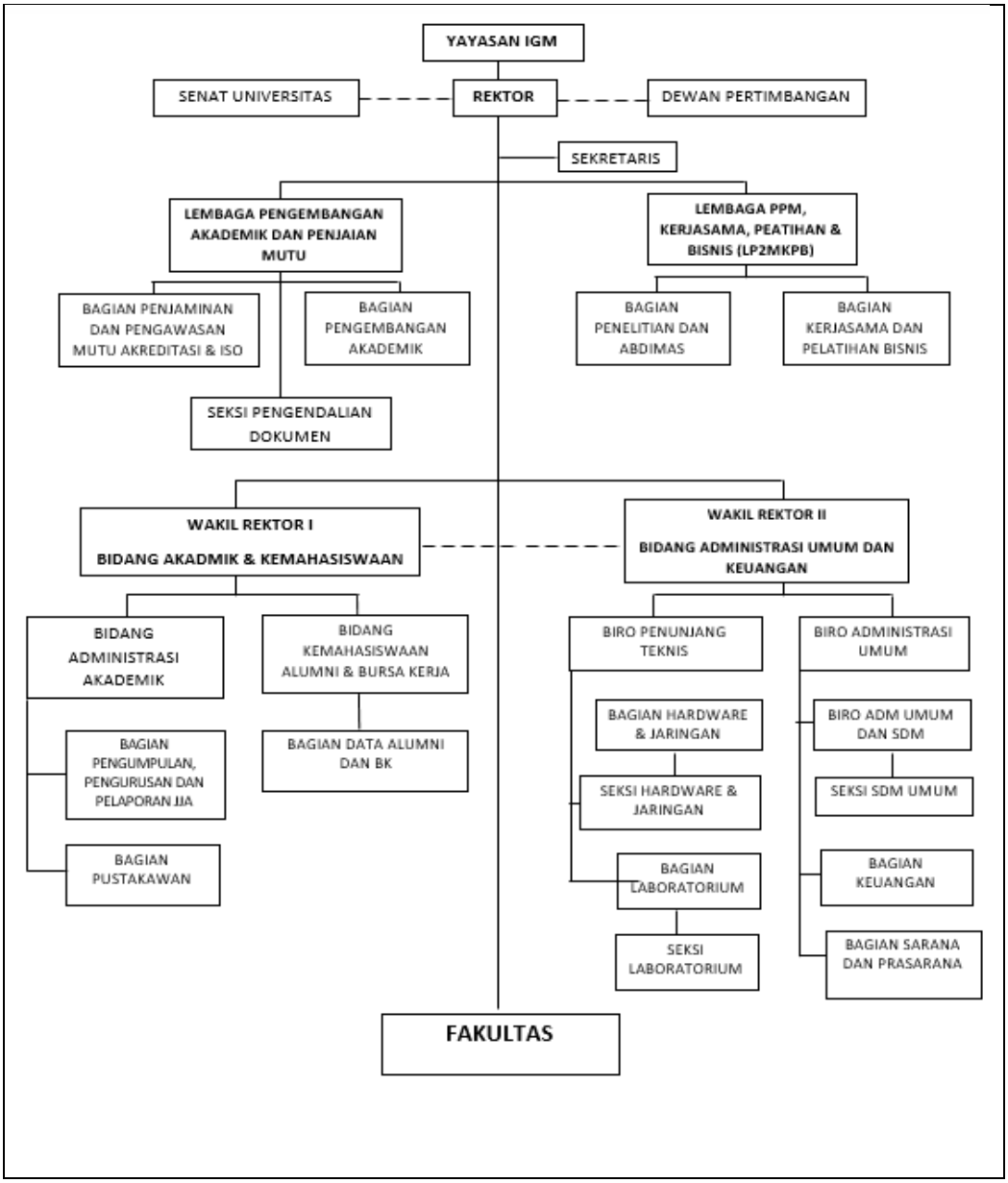
2. Misi

Adapun Misi Universitas Indo Global Mandiri Palembang adalah

1. Tersedianya sarana dan prasarana pendidikan yang *up to date* untuk menunjang proses belajar dan mengajar
2. Tersedianya tenaga pendidikan yang memiliki kualifikasi dan kompetensi yang diperlukan serta memiliki pengetahuan dan atau pengalaman dalam melaksanakan Tridharma Perguruan Tinggi.
3. Terbangunnya kerjasama dengan para pemangku kepentingan (stakeholder) yang dapat memberikan nilai tambah dalam pengembangan proses pembelajaran.
4. Terbangunnya kurikulum kewirausahaan sehingga dapat meningkatkan kreativitas mahasiswa dan jiwa kewirausahaan.
5. Terbangunnya karakter yang kuat dan berintegritas.

4.1.3 Struktur Organisasi

Struktur organisasi menunjukkan kerangka dan susunan perwujudan pola hubungan-hubungan diantara setiap fungsi, bagian yang menunjukkan kedudukan, tugas dan tanggung jawah yang berbeda-beda dalam suatu organisasi. Berikut struktur organisasi di Universitas Indo Global Mandiri Palembang :



Sumber : Universitas Indo Global Mandiri Palembang

Gambar 4.1 Struktur Organisasi Universitas Indo Global Mandiri Palembang

4.2 Penentuan Ruang Lingkup Objek

Ruang lingkup adalah apa saja yang akan dinilai dan sejauh mana penilaian terhadap keamanan informasi dilakukan. Dalam penelitian ini, ruang lingkup yang akan diteliti adalah sistem informasi akademik (simak *online*) Universitas Indo Global Mandiri Palembang, meliputi organisasi, lokasi, aset dan teknologi yang beruhubungan dengan simak *online.*

Adapun ruang lingkup yang dimaksud diatas antara lain :

1. Organisasi, yaitu Unversitas Indo Global Mandiri Palembang sebagai pemilik dan pengelola sistem informasi akademik (simak *online*).
2. Lokasi, yaitu Ruang Badan Pelaksanaan Teknis (BPT) dan Ruang Keamanan Jaringan dan Hardware.
3. Aset dan teknologi, yaitu :
    a. *Brainware* merupakan pemakai yang mengoperasikan perangkat komputer. *Brainware* dalam sistem informasi akademik Unversitas Indo Global Mandiri Palembang, sebagai berikut :
        (1) Pegawai
        (2) Dosen
        (3) Mahasiswa

b. *Hardware* merupakan komponen yang membangun struktur sebuah komputer. *Hardware* pada penerapan sistem informasi akademik Universitas Indo Globa Mandiri Palembang sebagai berikut :

(1) *Hardisk* 1

(2) TB

(3) RAM 32 GB

(4) IBM PC

(5) Dengan 8 PC dalam ruangan BPT (Biro Penunjang Teknis) dan 2 PC serta 3 laptop dalam ruangan *Hardware* dan Jaringan

c. *Software* merupakan program komputer yang berisi data-data dan informasi yang digunakan untuk melakukan perintah pada sistem yang ada pada komputer. *Software* pada penerapan sistem informasi Universitas Indo Global Mandiri Palembang sebagai berikut :

(1) *Operating System* : Linux

(2) *Tools* : Xampp, Notepad ++, DW (*Dreamweaver*), MySQL

d. Jaringan Komputer adalah jaringan komunikasi yang memungkinkan antar komputer untuk saling terhubung. Jaringan komputer yang digunakan pada Universitas Indo Global Mandiri Palembang adalah *Internet Service Provider* (ISP) CBN.

e. Komunikasi Data merupakan proses pengiriman dan penerimaan data dari dua atau lebih *device*. Komunikasi data pada Universitas Indo Global Mandiri Palembang sebagai berikut :

(1) Komputer

(2) Laptop

(3) *Handphone*

4.3 Penentuan Peran dan Tanggung Jawab Aset Informasi

Penentuan *Roles and Responsibility* (Peran dan Tanggung Jawab Aset Informasi) pemetaan fokus *auditee* dapat dilihat pada tabel 4.1. Lebih lengkapnya dapat dilihat pada lampiran II halaman 71.

Audit Charter

Project ID : ISO/IEC27001:2005-Audit-01

Project Name : Information Security Audit

Auditor : Yeni Rahayu

Project Description :

Penelitian berkaitan dengan keamanan informasi menggunakan standar ISO/IEC 27001:2005, yang berfokus pada klausul organisasi keamanan informasi, pengelolaan aset, keamanan sumber daya manusia, keamanan fisik dan lingkungan, manajemen operasi dan komunikasi, dan pengendalian akses.

Tabel 4.1 *Audit Charter*

JABATAN	**KLAUSUL PEGENDALIAN AUDIT**	***Auditee***
DIM (Director Information Manajemen)	ISO 27001 Klausul A.5 dan A.7	KASI bagian Biro Penunjang teknis
CEO (Chief Information Officer)	ISO 27001 klausul A.8, A.14, dan A.15	Kepala bagian Biro Penunjang Teknis
ISO (Information Security Officer)	Iso 27001 Klausul A.6, A.9, A.10, A.11 dan A.12	Bagian Teknisi, *Hardware* dan Jaringan

Berdasarkan tabel 4.1, tanggung jawab manajemen aset informasi berdasarkan ISO/IEC 27001:2005 yang disesuaikan dengan organisasi terkait yang akan dilaksanannya audit keamanan informasi.

4.4 Membuat Pertanyaan

Langkah selanjutnya adalah membuat pertanyaan. Pertanyaan disesuaikan berdasarkan pelaksanaan kontrol yang ada pada ISO/IEC 27001:2005. Berikut pertanyaan yang dibuat pada klausul 5 mengenai kebijakan keamanan pada tabel 4.2. Untuk selengkapnya dapat dilihat pada lampiran II halaman 73 dan hasil jawaban pertanyaan dapat dilihat pada lampiran III halaman 121.

Tabel 4.2 List Pertanyaan Klausul ISO/IEC 27001:2005

NO	KLAUSUL	KODE	PERTANYAAN
	Klausul A.5.1.1	Q1	Apakah sudah ada keijakan keamanan informasi?
		Q2	Apakah sudah terdokumentasi kebijakan keamanan informasi tersebut?
		Q3	Apakah dokumen kebijakan tersebut sudah dipublikasikan kepada seua pihak terkait?
		Q4	Apakah kebijakan tersebut sudah disosialisasikan dalam bentuk yang relevan, mudah diakses, dan dimengerti?
	Klausul A.5.1.2	Q5	Jika terjadi perubahan kebijakan, apakah kebijakan tersebut tetap disesuaikan dengan kefektifan yang berkelanjutan?
		Q6	Apakah perubahan kebijakan tersebut akan dikomunikasikan kepada semua pihak?
		Q7	Apakah ada pernyataan komitmen manajemen serta dukungan terhadap tujuan dan prinsi keamanan informasi?
		Q8	Apakah semua pegawai telah benar-benar memahami keamanan informasi?
		Q9	Apakah kebijakan keamanan informasi sudah dilakukan tinjauan ulang funa mengantisipasi setiap perubahan yang mempengaruhi analisa resiko, seperti kerawanan?
		Q10	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal?
Dan seterusnya...			

Sumber : Badan Standardisasi Nasional ISO/IEC 27001:2005 IDT

Dari daftar tabel 4.2 diatas adalah daftar pertanyaan yang akan diajukan dalam melakukan wawancara terkait keamanan informasi pada SIMAK *Online*

Universitas Indo Global Mandiri yang telah disesuaikan dengan sasaran pengendalian dari kontrol semua klausul yang tercantum pada dokumen SNI ISO/IEC 27001:2005

4.5 Pelaksanaan Pengoperasian Keamanan Informasi

Pada tahap ini langkah yang dilakukan yaitu melakukan pendahuluan audit sistem informasi, melakukan proses pemeriksaan data dan bukti dan melakukan wawacara terhadap responden terkait keamanan informasi.

4.5.1 Hasil Pemeriksaan Data dan Bukti

Hasil pemeriksaan data dan bukti dengan melakukan wawancara, hasil pengimplementasian sistem keamanan simak *online* berdasarkan kontrol pengendalian ISO/IEC 27001:2005. Untuk lebih lengkapnya tabel 4.3 dapat dilihat pada lampiran II halaman 86.

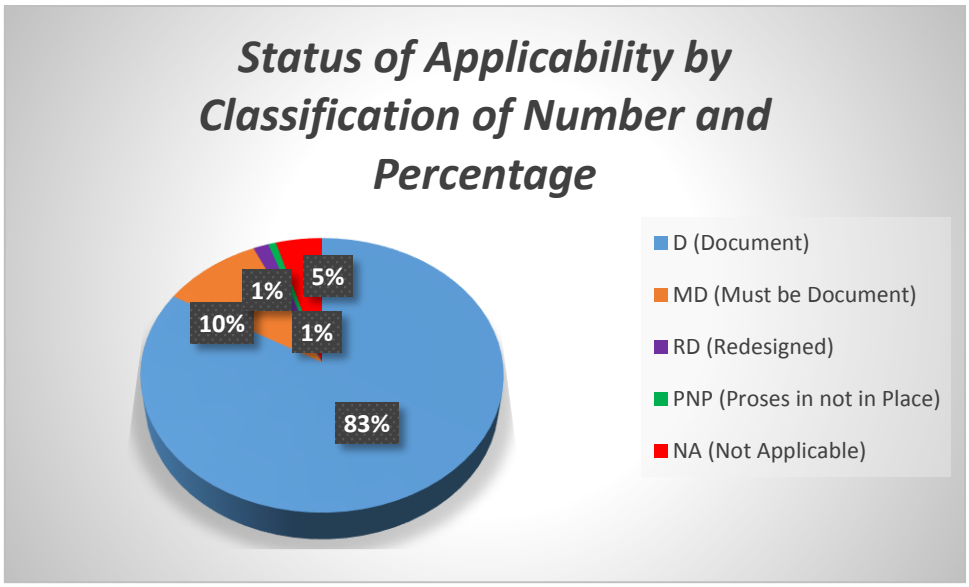
Tabel 4.3 *Statement Of Applicability* (SOA)

A.5 Kebijakan Keamanan		
ISO/IEC 27001:2005	**Aplicable**	**Exclusion Statement**
A.5.1.1 Dokumen Kebijakan Keamanan Informasi	D	Kebijakan keamanan informasi tetap menggunakan kebijakan keamanan informasi yang masih berlaku
A.5.1.2 Kajian Kebijakan Keamanan Informasi	D	Tetap disesuaikan, dikomunikasikan dan ditinjau ulang kebijakan keamanan inofrmasi apabila terjadi perubahan kebijakan
Dan seterusnya...		

Dari hasil tabel 4.3, didapat hasil implementasi terkait keamanan informasi yang telah diterapkan di Universitas Indo Global Mandiri Palembang berdasarkan implementasi dari semua klausul dan semua kontrol ISO/IEC

27001:2005. Bahwasannya, setiap klausul keamanan informasi telah diimplementasikan, hanya beberapa klausul dari setiap kontrol seperti pada klausul A.6. Organisasi Keamanan Informasi, pada kontrol A.6.1.6 tentang kontak dengan pihak berwenang, A.7 Pengelolaan aset pada kontrol A.7.2.2 tentang pelabelan dan penanganan informasi, A.9 Keamanan fisik dan lingkungan, pada kontrol A.9.1.1 tentang parameter keamanan fisik, A.10 Manajemen pelayanan jasa pihak ketiga, pada kontrol A.10.5.1 tentang *back-up* informasi, A.10.7.1 tentang manajemen media yang dapat dipindahkan, A.10.7.2 tentang pemusnahan media. A.10.8.1 tentang kebijakan prosedur pertukaran informasi, dan lain-lainnya. Dapat dilihat pada tabel selengkapnya di lampiran 8.

Berikut diagram *chart* hasil presentasi status implementasi dari setiap kontrol keamanan informasi



Gambar 4.2 Diagram *Status Of Applicability* (SOA)

Berdasarkan gambar 4.2, didapatkan presentasi hasil implementasi dari tiap kontrol keamanan informasi ISO/IEC 27001:2005 terhadap implementasi dari

sistem informasi Universistas Indo Global Mandiri Palembang. Didapat hasil 83% dari kontrol keamanan informasi telah diimplementasikan, 10% dokumen kebijakan masih dalam perencanaan dan akan diterapkan, 1% kontrol pelu ditinjau ulang, 1% kontrol proses tidak berada di tempatnya atau tidak diimplementasikan dan 5% kontrol tidak diimplemetasikan di SIMAK *Online* Universitas Indo Global Mandiri Palembang.

Jadi, secara garis besar implementasi keamanan informasi pada simak *online* Universitas Indo Global Mandiri telah diimplementasikan berdasarkan standar keamanan informasi ISO/IEC 27001:2005

4.6 Pelaksanaan Pelaporan Hasil Audit

Hasil dari audit yang telah dilaksanakan pada Unviersitas Indo Global Mandiri, langkah selanjutnya yaitu menganalisa hasil temuan dengan ceklist *gap analysis* dan menyusun hasil penilaian dari pengujian yang telah dilakukan.

4.6.1 Analisa Temuan berdasarkan Ceklist *Gap Analysis*

Analisa *Gap Analysis* untuk mengetahui kondisi kesenjangan keamanan informasi di Universitas Indo Global Mandiri. Hasil temuan dari audit akan dianalisa dengan membandingakan fakta yang ada dilapangan dengan standar yang berlaku yaitu ISO/IEC 27001:2005. Kondisi yang tampak pada temuan hasil audit akan dianalisa dampak dan rekomendasiya untuk peningkatan keamanan. Hasil temuan berdasarkan ceklist *gap analysis* dapat dilihat pada tabel 4.4 dan lebih lengkapnya dapat dilihat pada lampiran II halaman 98.

Tabel 4.4 *Gap Analysis : Status of ISO 27001 Implementation*

A.5 Kebijakan Keamanan				
ISO/IEC 27001:2005	**Status**	***Look for***	***Findings***	**Rekomendasi**
A.5.1.1 Dokumen Kebijakan Keamanan Informasi	D	Adanya dokumen kebijakan yang telah terdokumentasi	Kebijakan keamanan informasi tetap menggunakan kebijakan keamanan informasi yang masih berlaku	Peningkatan pemeliharaan dokumen kebijakan yang telah ada dan tetap diberlakukannya kebijakan tersebut
A.5.1.2 Kajian Kebijakan Keamanan Informasi	D	Adanya dokumen yang telah terdokumentasi	Tetap disesuaikan, dikomunikasikan dan ditinjau ulang kebijakan keamanan inofrmasi apabila terjadi perubahan kebijakan	Perlu peninjauan ulang yang lebih baik ketika terjadi perubahan kebijakan yang berlaku
Dan seterusnya...				

Kode Status :

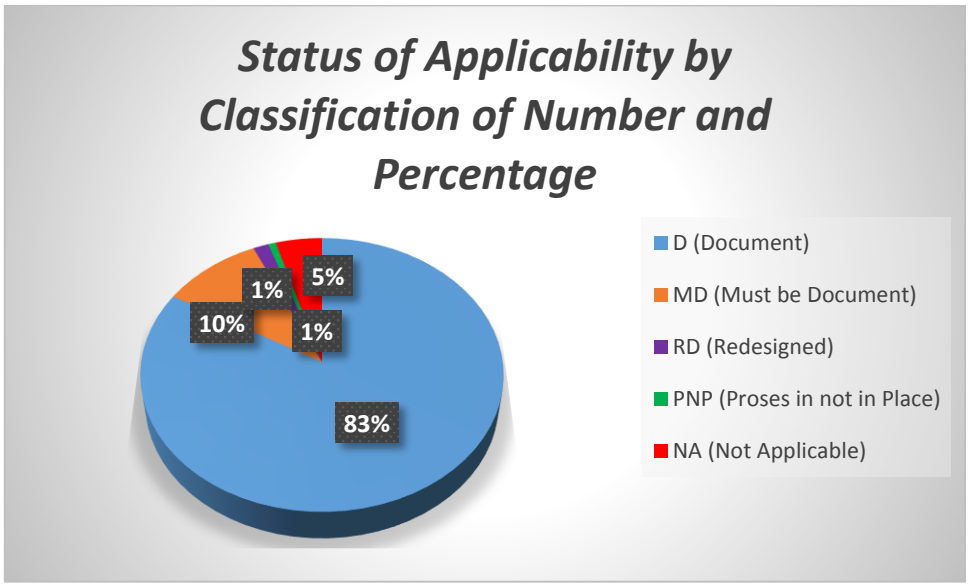
D : Documented (Kontrol di dokumentasikan atau diimplementasikan)

MD : Must be Document (Kontrol masih dalam proses dokumentasi atau perencanaan)

RD : Redesigned (Kontrol tidak terpenuhi sesuai standar atau perlu didesain ulang)

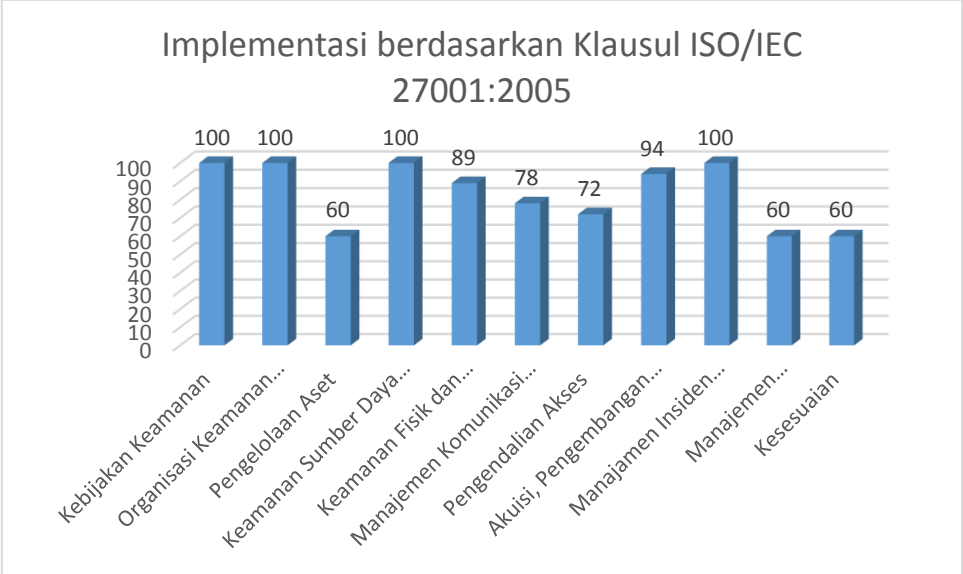
PNP : Proses is not in Place (Kontrol tidak ada di tempat atau di implementasikan)

NA : Not Applicable (Tidak diterapkan sama sekali)



Gambar 4.3 Diagram *Status Of Applicability* (SOA)

Berdasarkan gambar 4.2, secara garis besar implementasi keamanan informasi pada simak *online* Universitas Indo Global Mandiri telah diimplementasikan mencapai 83% implementasi kontrol keamanan berdasarkan standar ISO/IEC 27001:2005



Gambar 4.4 Diagram Batang berdasarkan Klausul ISO/IEC 27001:2005

Berdasarkan gambar 4.4, menunjukkan pemenuhan implementasi dari setiap klausul ISO/IEC 27001:2005 yang menghasilkan bahwa hampir semua klausul keamanan informasi hampir terpenuhi dan mencapai pemenuhan yang optimal seperti pada klausul A5 mengenai kebijakan keamanan informasi, A.6 mengenai organisasi keamanan informasi, dan A.13 mengenai manajemen insiden keamanan informasi yang mencapai tingkat optimal.

Berdasarkan hasil dari analisa kesenjangan sistem informasi temuan kondisi keamanan informasi saat ini dan kondisi ideal berdasarkan pengendalian ISO/IEC 27001:2005 didapatkan temuan kesenjangan pada beberapa klausul yaitu pada klausul organisasi keamanan infromasi terdapat temuan kesenjangan pada klausul organisasi keamanan informasi yaitu : tidak adanya dokumentasi dan perjanjian secara tertulis dengan terkait kontak dengan pihak yang berwenang.

Pada klausul pengelolaan aset terdapat temuan kesenjangan pada pengelolaan aset yaitu : belum adanya prosedur dan pencatatan terhadap inventaris aset dan tidak adanya prosedur untuk pelabelan terhadap infromasi yang bersifat rahasia

Pada klausul keamanan fisik dan lingkungan terdapat temuan kesenjangan pada klausul keamanan fisik dan lingkungan yaitu : kurang diperhatikannya daerah kawasan terkait sistem informasi seperti pintu masuk yang hanya menggunaan pintu biasa dalam ruangan tersebut belum dilengkapi dengan pengamanan yang lebih ketat seperti pemakaian pinti dengan kartu gesek atau pin.

Pada klausul manajemen pelayanan jasa pihak ketiga terdapat temuan kesenjangan pada klausul manajemen pelayanan jasa pihak ketiga yaitu : tidak adanya fasilitas back up dan salinan backup yang memadai untuk memulihkan

sistem jika terjadi ancaman atau bencana, tidak adanya prosedur pemindahan media apabila media tidak lagi digunakan, dan tidak adanya prosedur yang terdokumentasi dari kebijakan dalam penggunaan fasilitas.

Pada klausul pengendalian akses terdapat temuan kesenjangan pada klausul pengendalian akses yaitu : belum adanya alokasi password untuk mengendalikan proses manajemen, belum adanya kebijakan clear desk terhadap kertas dan media yang dipindahkan, belum didentifikasi peralatan secara otomatis untuk mendeteksi koneksi lokasi dan peralatan, tidak ada prosedur log on yang aman, dan sesi otomatis aktif juga belum diterapkan.

Pada klausul keamanan dalam proses pengembangan dan pendukung terdapat temuan kesenjangan pada klausul keamanan dalam proses pengembangan dan pendukung yaitu : tidak adanya evaluasi kerawanan teknis dari sistem informasi.

Pada kalusul manajemen keberlanjutan bisnsis terdapat temuan kesenjangan pada klausul keberlanjutan bisnis yaitu : tidak adanya kerangka kerja tunggal untuk rencana bisnis kedepan, belum adanya pengujian terlebih dahulu terhadap pemutakhiran proses bisnis lebih lanjut.

Dan pada kalusul kesesuaian terdapat temuan kesenjangan pada klausul kesesuaian yaitu : belum adanya persyaratan perundang-undangn kontrak secara resmi,belum diterapkan persyaratan kontrak dalam penggunaan materi dan produk perangkat lunak, tidak adanya rekaman untuk merekam data pnting terkait penghancuran dan pemalsuan kontrak, dan tidak adanya perjanjian pengendalian kriptografi.

4.7 Hasil Temuan untuk Pengkajian Sistem Manajemen Keamanan Informasi

Hasil temuan dari dilaksanakannya audit keamanan informasi didapat temuan dari setiap klausul berdasarkan kontrol keamanan ISO/IEC 27001:2005 untuk pengkajian sistem keamanan informasi. Berdasarkan hasil wawancara, analisa dan pemeriksaan data dan bukti terkait keamanan informasi, didapatkan hasil temuan bahwa keamanan informasi pada simak *online* Universitas Indo Global Manidri Palembang telah mencapat target 83% implementasi keamanan informasi berdasarkan semua klausul ISO?IEC 27001:2005. Dan hasil dari keseluruhan kontrol keamanan informasi terdapat beberapa kontrol keamanan yang telah mencapai tingkatan optimal dalam penerapan keamanan informasinya. Akan tetapi, ada beberapa kontrol yang belum mencepai tingkat optimal dikarenakan belum sepenuhnya terimpleentasikan keamanan informasi yang baik berdasarkan standar keamanan informasi ISO/IEC 27001:2005. Berikut hasil uraian temuan dari setiap klausul :

4.7.1 Klausul A.5 Kebijakan Keamanan

Klausul kebijakan keamanan informasi untuk memberikan arahan manajemen dan dukungan utuk keamanan informasi menurut persyaratan bisnis dan hukum dan regulasi yang relevan pada klausul kebijakan keamanan informasi yang dinilai pada kontrol ini adalah Telah diadakannya prosedur kebijakan keamanan informasi dan didokumentasikan prosedur tersebut. Kebijakan keamanan telah

disesuaikan dengan keefektifan yang berkelanjutan dan jika terjadi perubahan pada kebijakan dikomunikasikan pada pihak terkait. Komitmen dan dukungan manajemen terhadap tujuan dan prinsip keamanan informasi.dan kebijakan keamanan informasi telah ditinjau ulang secara berkala jika terjadi perubahan atau terjadwal.

4.7.2 Klausul A.6 Organisasi Keamanan Infomasi

Organisasi keamanan informasi yang dinilai pada kontrol ini adalah pada bbjektif A.6.1 komitmen manajemen terhadap keamanan informasi yang mempunyai sasaran yaitu untuk mengelola keamanan informasi dalam organisasi. Pada komitmen manajemen terhadap keamanan informasi telah mendukung secara aktif keamanan dalam organisasi. Akan tetapi kegiatan keamanan tidak dikoordinasi oleh wakit-wakil bagian organisasi. Tanggung jawab keamanan dan manajemen fasilitas pengolahan informasi telah ditetapkan. Persyaratan dan perjanjian kerahasiaan organisasi dilindungi dan dikaji secara regular. Dalam hubungan dengan pihak berwenang UIGM tidak adanya kontak dengan pihak berwenang yang terpelihara. Akan tetapi organisasi pendekatan organisasi untuk mengelola informasi telah dikaji dan diterapkan.

Pada objektif A.6.2 pihak eksternal yang mempunyai sasaran yaitu untuk memelihara keamanan informasi organisasi dan fasilitas pengolahan yang diakses, diolah, dikomunikasikan oleh pihak eksternal. Temuan yang didapat yaitu telah di identifikasi resiko terhadap organisasi dan fasilitas pengolahan dari proses bisnis yang melibatkan pihak ketiga. Persyaratan keamanan teridentifikasi sebelum

memberikan hak akses kepada pelanggan informasi. Adanya persyaratan dan perjanjian pihak ketiga

4.7.3 Klausul A.7 Pengelolaan Aset

Pada klausul pengelolaan aset yang dinilai pada kontrol ini adalah pada objektif kontrol A.7.1 tanggung jawab terhadap aset yang mempunyai sasaran yaitu untuk mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi. Temuan yang didapat yaitu perlu identifikasi dan pencatatan untuk dokumentasi inventaris aset (aset informasi, aset piranti lunak, aset fisik dan layanan) serta perlu disusun dan dipelihara terhadap aset tersebut. Pengklasifikasian lokasi keamanan aset yang sudah terdokumentasi jika terjadi kehilangan atau kerugian. Adanya pembagian sub bagian yang bertanggung jawab dalam mengontrol dan memihara keamanan informasi inventaris aset serta dilakukan pengecekan inventaris secara berkala setiap bulannya. Dan adanya peraturan penggunaan aset, pengelolaan dan pengklasifikasian aset yang telah terdokumentasikan

Pada objektif kontrol A.7.2 klasifikasi informasi yang mempunyai sasaran yaitu untuk memastikan bahwa informasi menerima tingkat perlindungan yang tepat. Temuan yang didapat yatu klasifikasi informasi pengelolaan aset dengan tingkat perlindungan yang tepat dan perlunya prosedur dan pelabelan serta penanganan informasi yang bersifatarahasia atau penting.

4.7.4 Klausul A.8 Keamanan Sumber Daya Manusia

Pada keamanan sumber daya manusia yang dinilai pada kontrol ini adalah pada objektif A.8.1 sebelum dipekerjakan yang mempunyai sasaran yaitu

untuk memastikan bahwa pegawai, kontraktor dan pengguna pihak ketiga memahami tanggung jawab sesuai dengan perannya dan untuk mengurangi resiko pencurian, kecurangan atau penyalahgunaan fasilitas. Hasil temuan yang didapat yaitu kebijakan keamanan informasi terkait tanggung jawab dan peran pegawai. Belum terlaksananya menurut hukum dan undang-undang yang berlaku terkait verifikasi latar belakang calon pegawai dan persetujuan penandatangan kontrak telah ditetapkan

Pada objektif kontrol A.8.2 Selama bekerja yang mempunyai sasaran yaitu untuk memastikan bahwa semua pegawai, kontraktor, dan pengguna pihak ketiga telah peduli terhadap ancaman dan masalah keamanan informasi, tanggung jawab dan pertanggung-gugatan mereka dan ketersediaan perlengkapan yang memadai untuk mendukung kebijakan keamanan informasi selama bekerja dan untuk mengurangi resiko kesalahan manusia. Temuan yang didapat yaitu telah ditetapkan prosedur keamanan informasi kepada peawai. Prosedur pelatihan dan pendidikan kepada pegawai sesuai perannya dan kebijakan pendisiplinan telah didokumentasikan.

Pada objektif kontrol pengakhiran atau perubahan pekerjaan yang mempunyai sasaran yaitu untuk memastikan bahwa pegawai, kontraktor dan pengguna pihak ketiga keluar dari organisasi atau adanya perubahan pekerjaan dengan cara yang sesuai. Temuan yang didapat yaitu danya kebijakan pengakhiran atau perubahan pekerjaan, telah ditetapkannya peraturan apabila pegawai, kontraktor dan pihak ketiga dalam mengembalikan aset organisasi yang digunakan apabila telah berakhir perjanjian dan peraturan penghapusan hak akses dan fasilitas pegawai ketika pekerjaan berakhir.

4.7.5 Klausul A.9 Keamanan Fisik dan Lingkungan

Keamanan fisik dan lingkungan yang dinilai disini adalah pada Objek kontrol A.9.1 area yang aman yang mempunyai sasaran yaitu untuk mencegah akses fisik oleh pihak yang tidak berwenang, kerusakan dan interferensi terhadap lokasi dan inofrmasi organisasi. Temuan yang didapat yaitu adanya pintu masuk yang belum dikendalikan dengan kartu atau PIN guna untuk meminimalisir pencurian atau kesalahan dalam penggunaan fasilitas. Keamanan fisik untuk kantor fasilitas lainnya. Telah disesdiakannya ruangan khusus sebagai kendali sistem informasi. Pembatasan hak akses terhadap pihak luar. Perlindungan terhadap ancaman luar seperti kebakaran, ledakan dan bencana lain dan penempatan ruangan yang nyaman dan aman.

Pada objektif kontrol A.9.2 keamanan peralatan yang mempunyai sasaran yaitu untuk mencegah kehilangan, kerusakan, pencurian atau gangguan aset da interupsi terhadap kegiatan organisasi. Temuan yang didapat yaitu penempatan server dan peralatan informasi lainnya di tempat yang aman, pembatasan akses pada pihak yang tidak berwenang dan perlindungan peralatan seperti kabel dilindungi dari kegagalan catu daya dan tersedianya peralatan pendukung seperti UPS dan pembangkit listrik

4.7.6 Klausul A.10 Manajemen Komunikasi dan Operasi

Manajemen komunikasi dan operasi yang dinilai disini adalah pada objek kontrol A.10.1 prosedur operasional dan tanggung jawab yang mempunyai sasaran yaitu untuk memastikan pengoperasian fasilitas pengolahan informasi secara benar dan aman. Temuan yang didapat yaitu *Maintenace* server dilakukan

dengan aman agar terhindar dari kesalahan operasi. Pegawai teknis khusus yang menangani masalah kerusakan atau kesalahan teknis. Perubahan terhadap pengolahan sistem informasi sudah dikendalikan dan dicatat serta disosialisasikan kesemua pihak. Dan pemisahan *job desk*, pengawasan dan pemantauan terhadap insiden penyalahgunaan sistem

Pada Objektif Kontrol A.10.2 Manajemen Pelayanan Jasa Pihak Ketiga yang mempunya sasaran yaitu untuk menetapkan dan memelihara tingkat keamanan informasi dan pelayanan jasa yang sesuai dengan perjanjian pelayanan jasa pihak ketiga. Temuan yang didapat yaitu perjanjian terhadap pihak ketiga terhadap layanan jasa telah diterapkan, dioperasikan, dan dipelihara. Salinan *back-up* dan piranti perangkat lunak dilakukan secara berkala. Akan tetapi perlunya dikaji ulang dan diaudit secara regular mengenai jasa, laporan dan rekaman pantauan dari pihak ketiga

Pada objektif kontrol A.10.3 perencanaan dan keberterimaan sistem yang mempunyai sasaran yaitu untuk mengurangi resiko kegagalan sistem. Temuan yang didapat yaitu telah diadakannya pengujian terhadap sistem yang *upgrade* atau versi baru. Pemantauan sumber daya tidak disesuaikan untuk pemenuhan kapasitas mendatang.

Pada objektif kontrol A.10.5 *back-up* yang mempunyai sasaran yaitu untuk memelihara integritas dan ketersediaan informasi dan fasilitas pengeolaan informasi. Temuan yang didapat yaitu tidak ada fasilitas untuk *back-up* dan prosedur pemulihan yang terdokumentasi dan media *back-up* diuji secara berkala.

Pada objektif kontrol A.10.6 manajemen keamanan jaringan yang mempunyai sasaran yaitu untuk memastikan erlindungan informasi dalam jaringan

dan perindungan infrastruktur pendukung. Temuan yand didapat yaitu adanya penerapan kontrol jaringan untuk keamanan data dalama jaringan dan petugas khusus dalam menanganinya. Penerapan mekanisme pengamanan jaringan dan identifiasi titik jaringan yang rawan terhadap serangan. Mekanisme recovery yang diterapkan guna menanggulangi penyerangan serta fitur keamanan yang teridentifikasi

Pada objektif kontrol A.10.7 penanganan media yang mempunyai sasaran yaitu untuk mencegah engungkapan, modifikasi, pemindahan atau pemusnahan aset yang tidak sah dan gangguan kegiatan bisnis. Temuan yang didapat yaitu terdapat prosedur manajemen pemindahan media yang telah terdokumentasi. Tidak adanya tindakan pemusnahan media apabila tidak lagi diperlukan dan belum diterapannya prosedur tersebut. Adanya prosedur untuk penanganan dan penyimpanan informasi guna melindungi dair penyalahgunaan dan telah terdokumentasi sistem untuk melindungi akses yang tidak sah

Pada objektif kontrol a.10.8 pertukaran informasi yang mempunyai sasaran yaitu untuk memelihara keamanan informasi dan perangkat lunak yang diperlukan dalam suatu organisasi dang dengan setiap entitas eksternal. Teuan yang didapat yaitu perlunya kebijakan prosedur dan pengendalian untuk melindungi pertukaran informasi dengan semua jenis fsilitas komunikasi. Adanya perjanjian terhadap pihak eksternal atau organisasi dalam pertukaran informasi. Persediaan media untuk memuat informasi terhadap hak akses yang tidak sah atau penyalahgunaan

Pada objektif kontrol A.10.10 pemantauan yang mempunyai sasaran yaitu untuk mendeksi kegiatan pengolahan informasi yang tidak sah. Temuan yang

didapat yaitu log untuk merekam kegiatan dan kejadian kemanan informai dan pemantauan akses serta prosedurnya. Fasilitas log yang telah dilindungi dari gangguan dan akses yang tidak sah. Pencatatan log kegiatan administrator an operator sistem jika terjadinya kesalah dan telah diambil tindakan untuk menangggulanginya.

4.7.7 Klausul A.11 Pengendalian Akses

Pengendalian akses yang dinilai disini adalah pada objektif kontrol A.11.1 persyaratan bisnis untuk pengendalian akses yang mempunyai sasaran :yaitu untuk mengendalikan akses kepada informasi. Temuan yang didapat yaitu kebijakan prosedur pengendalian akses yang telah terdokumentasi berdasarkan persyaratan bisnis dan keamanan untuk aksesdan prosedur pendaftaran dan pemberian atau pencabutan hak akses terhadap sistem informasi

Pada objektif kontrol A.11.2 manajemen akses pengguna yang mempunyai sasaran yaitu untuk memastikan akses oleh pengguna yang sah dan untuk encegah pihak yang tidak sah pada sistem informasi. Temuan yang didapat ayitu perlu adanya alokasi password untuk mengendalikan manajemen formal dan poeninjauan terhadap hak akses secara regular menggunakan proses formal

Pada objektif kontrol A.11.3 tanggung jawab pengguna yang mempunyai sasaran yaitu untuk mencegah akses pengguna yang tidak sah dan ganggun atau pencurian atas informasi dan fasilitas pengolahan informasi. Temuan yang didapat yaitu pedoman disyaratkannya pengamanan yang baik dalam pemilihan password. Perlu adanya kebijakan *clear desk* terhadap media penyimpanan yang dapat dipindahkan untuk fasilitas pengolahan informasi

Pada objektif kontrol A.11.4 pengendalian akses jaringan yang mempunyai sasaran yaitu untuk mencegah akses yang tidak sah ke dalam layanan jaringan. Temuan yang didapat yaitu pengguna hanya diberikan akses terhadap layanan yang telah diberikan kewenangan penggunaannya secara spesifik. Perlindugnan pengendalian secara fisik dan *logical* terhadap *diacnotic* dan *confguration port.* Perlu pengendalian *routing* yang diterapkan ke dalam jarigan untuk memastikan bahwa koneksi komputer dan aliran informasi tidak melanggar kebijakan pengendallian akses

Pada objektif kontrol A.11.5 pengendalian akses sistem operasi yang mempunyai sasaran yaitu untuk mencegah akses yang tidak sah masuk ke dalam sistem operasi. Temuan yang didapat yaitu perlu prosedur *log-on* yang aman. Adanya user id untuk pengguna personal dan teknik validasi dalam setiap user id yang terdaftar dan telah danya sistem manajemen *password*

Pada objektif kontrol A.11.6 pengendalian akses aplikasi dan informasiyang mempunyai sasaran yaitu untuk mencegah akses yang tidak sah terhadap informasi pada aplikasi. Temuan yang didapat yaitu pembatasan kepada pengguna terdahap akses informasi dan sistem yang sensitif memiliki lingkungan komputasi yang diisolasi

4.7.8 Klausul A.12 Akuisi, Pengembangan dan Pemeliharaan Informasi

Pada klausul Akuisi, Pengembangan dan Pemeliharaan Informasi kontrol ini yang dinilai adalah pada objektif kontrol A.12.1 persyaratan keamanan informasi dari sistem informasi yang mempunyai sasaran yaitu untuk memastikan bahwa keamanan merupakan bagian yang utuh dari sistem informasi. Hasil

temuan yang didapat yaitu persyaratan bisnis untuk sistem infromasi dan dokumen persyaratan bisnis sistem informasi

Pada objektif kontrol A.12.2 pengolahan yang benar dari sistem informasi yang mempunyai sasaran yaitu untuk mencegah kesalahan, kehilangan, moifikasi yang tidak sah atau penyalahgunaan informasi dalam aplikasi. Hasiol temuan yang didapat yaitu prosedur validasi memasukkan data ke simak online. Prosedur merespon kesalahan validasi. Penggabungan pengecekan validasi untuk mendeteksi kerusakan. Pengendalian persyaratan untuk memastikan keaslian perlindungan integritas pesan. Dan telah diterapkan validasi dan identifikasi keluaran data.

Pada objektif kontrol A.12.3 pengendalian dengan cara kriptografi yang mempunyai sasaran yaitu untuk melindungi kerahasiaan, keaslian atau integritas informasi dengan cara kriptografi. Temuanyang didapat yaitu telah adanya kebijakan kriptografi dan penerapan kriptografi

Pada objektif Kontrol A.12.4 keamanan sistem file yang mempunyai sasaran yaitu untuk memastikan keamanan sistem file. Temuan yang didapat yaitu telah adanya prosedur pengendalian instalasi perangkat lunak dan pembatasan kode akses ke kode sumber program

Pada objektif kontrol A.12.5 keamanan dalam proses pengembangan dan pendukung yang mempunyai sasaran yaitu untuk memelihara keamanan perangkat lunak sistem dan informasi. Temuan yang didapat yaitu telah adanya prosedur pengendalian perubahan dalam sistem aplikasi. Penerapan prosedur pengendalian perubahan. Perlu adanya dokumentasi prosedur pengendalian perubahan dalam sistem. Peninjauan ulang dan pengujian perubahan sistem informasi. Pembatasan

modifikasi perangkat lunak. Pencegahan dari kebocora informasi. Pemantauan pengembangan perangkat lunak alih daya. Evaluasi kerawanan teknis dari sistem informasi dan pencegahan penanganan resiko kerawanan teknis

4.7.9 Klausul A.13 Manajemen Insiden Keamanan Informasi

Pada manajemen insiden keamanan informasi, yang dinilai pada kontrol ini adalah pada objektif kontrol A.13.1.1 pelaporan kejadian dan kelemahan keamanan informasi yang mempunyai sasaran yaitu untuk memastikan kejadian dan kelemahan keamanan informasi terkait dengan sistem informasi dikomunikasikan sedemikian rupa sehingga memungkinkan tindakan koreksi dilakukan yang tepat waktu. Temuan yang didapat yaitu pengambilan tindakan dan pelaporan ketika terjadi insiden keamanan dan pencatatan laporan setiap kelemahan keamanan.

Pada objektif kontrol A.13.2 manajemen keamanan informasi dan perbaikan yang mempunyai sasaran yaitu untuk memastikan pendekatan yang konsisten dan efektif diterapkan untuk manajemen insiden keamanan informasi. Temuan yang didapat yaitu telah adanya penetapan tanggung jawab manajemen terakit keamanan informasi. Mekanisme yang memungkinan jenis, volume dan biaya insiden keamanan. Pengumpulan bukti terkait orang atau rganisasi setelah insiden yang melibatkan tindakan hukum.

4.7.10 Klausul A.14 Manajemen keberlanjutan bisnis (*Business continuity management*)

Pada klausul manajemen kebrlanjutan bisnis, aspek yang dinilai pada kontrol ini adalah pada objektif kontrol A.14.1 aspek keamanan informasi dari manajemen keberlanjutan bisnis yang mempunyai sasaran yaitu untuk menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dari efek kegagalan utama sistem informasi atau bencana dan untuk memastikan keberlanjutannya secara tepat waktu. Temuan yang didapat yaitu pengembangan dan pemeliharaan keberlanjutan bisnis organisasi. Identifikasi kejadian yang memungkinkan ganguan terhadap proses bisnis. Perencanaan untuk memelihara atau mengembalikan operasi setelah terjadi gangguan. Pengembangan rencana ketersediaan informasi pada tingkat dan waktu yang disyaratkan setelah gangguan. Belum adanya kerangka tunggal dari keberlanjutan bisnis. Belum adanya pengujian dan pemeliharaan kerangka kerja tunggal. Tidak adanya pengujian dan pemutakhiran secara regular rencana keberlanjutan bisnis

4.7.11 Klausul A.15 Kesesuaian

Pada klausul kesesuaian, aspek yang dinilai adalah pada objektif kontrol A.15.1 Kesesuaian dengan persyaratan hukum yang mempunyai sasaran yaitu untuk mencegah pelanggaran terhadap undang-undang, peraturan perundang-undangan atau kewajiban kontrak dan setiap persyaratan keamanan. Temuan yang didapat yaitu belum ditetapkan statuta, peraturan, perundang-undangan dan persyaratan kontrak untuk memenuhi persyaratan hukum mengenai keamanan informasi. Belum terdokumentasi peraturan tersebut. Belum adaya prosedut untuk

kesesuaian dengan peraturan perundang-undangan dan persyaratan kontrak penggunaan materi berkenaan perangkat lunak. Tidak adanya perlindungan rekaman penting dari keahilangan, penghancuran dan pemalsuan. Perlindungan data dan kerahasiaan dan belum ada pengendalian kriptografi yang disesuaikan dengan undang-undang

Pada objektif kontrol A.15.2 pemenuhan terhadap kebijakan keamanan dan standar dan pemenuhan teknis yang mempunyai sasaran yaitu untuk memastikan pemenuhan sistem terhadap kebijakan dan standar keamanan organisasi. Temuan yang didapat yaitu manajer telah memastikan seluruh prosedur dalam lingkup tanggung jawab dilakukan secara berkala dan pengecekan secara regular pemenuhan teknis sistem informasi

Pada objektif kontrol A.15.3 Pertimbangan audit sistem informasi yang mempunyai sasaran yaitu untuk memasksimalkan keefektifan dari dan untuk meminimalkan interferensi kepada/dari prosed audit sistem informasi. Temuan yang didapat yaitu perencanaan dan persyaratan terkait kegiatan audit yang melibatkan penecekan pada sistem operasional dan telah adanya perlindungan terhadap akses alat audit sistem informasi.

4.8 Rekomendasi Kebijakan dan Prosedur Keamanan Informasi

Kebijakan, prosedur, intruksi dan dokumentasi yang direkomendasikan sesuai dengan hasil temuan audit keamanan informasi berdasarkan standar ISO/IEC 27001:2005. Hasil dari temuan pengkajian SMKI didapatkan bahwasannya terdapat beberapa kontrol keamanan informasi yang belum terpenuhi pengimplementasiannya berdasarkan standar kemanan informasi ISO/IEC

27001:2005. Dampak permasalahan pada kondisi saat ini pada keamanan infromasi Universitas Indo Global Mandiri Palembang dan rekomendasinya, dijelaskan pada tabel 4.5 dan lebih lengkapnya pada lampiran II halaman 117.

Tabel 4.5 Rekomendasi Kebijakan dan Prosedur Keamanan Informasi

Klausul ISO/IEC 27001:2005	**Permasalahan/kondisi saat ini**	**Rekomendasi**
A.5 Kebijakan Keamanan	Kebijakan keamanan informasi telah diterapkan, akan tetapi keamanan informasi belum disosialisasikan dalam bentuk yang relevan, mudah dimengerti dan mudah diakses	Sebaiknya kebijakan keamanan disosialisasikan dalam bentuk yang relevan, mudah dimengerti, dan mudah diakses
A.6 Organisasi Keamanan Informasi	Koordinasi wakil ari organisasi belum disesuaikan dengan perannya dalam kegiatan keamanan informasi, tidak terpeliharanya kontak dengan pihak berwenang dan kontak kelompok khusus atau forum ahli keamanan	a. Koordinasi wakil-wakil dari organisasi yang sesuai dengan perannya dalam kegiatan keamanan informasi b. Perlu dipelihara dengan kontak pihak yang berwenang c. Pemeliharaan kontak dengan kelompok khusus (*special interest*) atau forum ahli keamanan dan asosiasi profesi
A.7 Pengendalian Akses	Pada dokumeen inventaris aset belum adanya identifikasi dan pencatatan yang diterapkan, aset informasi dan prosedur pemberian tanda pelabelan serta penanganan informasi yang bersifat rahasia juga belum0020terpelihara dan diterapkan.	a. Identifikasi dan pencatatan untuk dokumentasi inventaris aset (aset informasi, aset piranti lunak, aset fisik dan layanan) b. Pemeliharaan terhadap aset informasi c. Prosedur dan tindakan pemberian tanda pelabelan serta penanganan informasi yang bersifat rahasia atau penting d. Dokumentasi prosedur pelabelan
Dan seterusnya...		

Berdasarkan tabel 4.5 dijelaskan bahwa terdapat masalah dari kondisi saat ini terkait keamanan informasi pada Universitas Indo Global Mandiri. Pencapaian pengimplementasian kontrol keamanan informasi mencapai 83% termasuk kedalam kategori mendekati optimal. Akan tetapi, terdapat beberapa kontrol keamanan yang belum terpenuhi dan belum diimplementasikan sepenuhnya sehingga munculnya permasalahan terkait keamanan. Untuk meningkatkan perbaikan dan pengembangan keamanan informasi untuk sistem informasi pada Universitas Indo Global Mandiri Palembang kedepannya yang lebih baik, maka dengan rekomendasi kebijakan dan prosedur harus terpenuhi guna untuk meminimalisir terjadinya ancaman, kerusakan dan pengamanan untuk keamanan informasi kedepannya yang lebih baik. Sehingga dapat mencapai target yang telah ditargetkan untuk keamanan informasi Universitas Indo Global Mandiri yang akan dicapai untuk meningkatkan keamanan, integritas, efektivitas dan efisensinya.

BAB V

PENUTUP

5.1 Simpulan

Penelitian ini melakukan audit keamanan informasi terhadap simak *online* di Universitas Indo Global Mandiri Palembang menggunakan standar ISO/IEC 27001:2005. Terkait dengan hasil audit keamanan informasi yang telah dilakukan, maka didapat temuan yaitu simak *online* Universitas Indo Global Mandiri telah mengimplementasikan kontrol keamananan informasi sebanyak 83%, namun masih terdapat kontrol keamanan informasi yang belum sepenuhnya diimplementasikan sesuai dengan ISO/IEC 27001:2005. Hal ini berarti bahwa keamanan informasi simak *online* belum sepenuhnya mencapai tingkat optimal yaitu 100% pengimplementasian pada seluruh kontrol keamanan ISO/IEC 27001:2005

5.2 Saran

Berdasarkan pembahasan dari hasil penelitian ini maka diajukan beberapa saran, yaitu :

1. Menerapan sistem informasi akademik pada Universitas Indo Global Mandiri disesuaikan dengan standar keamanan informasi untuk meningkatkan pengamanan terhadap aset, integritas, efektivitas dan efesiensi.
2. Mengadakan audit keamanan informasi secara berkala setiap tahunnya untuk mengetahui kondisi perkembangan dan pengelolaan keamanan informasi sehingga keamanan informasi selalu pada tingkatan optimal agar dapat menjaga aset informasi dengan baik.

DAFTAR PUSTAKA

Armansyah. 2017. *Audit Sistem Informasi Pelayanan PDAM (SIPL-PDAM) Menggunaka ITIL Version 3 Domain Service Transition dan Service Operation (Studi Kasus : PT Tirta Musi Palembang).* Tidak dipublikasikan. Skripsi. Fakultas Sains Dan Teknologi UIN Raden Fatah Palembang.

Badan Standardisasi Nasional. 2009. *SNI ISO/IEC 27001:2005*. Jakarta:BSNI

Chazar, C. 2015. *Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001 : 2005.* Volume VII. No.2. Jurnal Informasi.

Gondodiyoto, Sanyoto. *Audit Sistem Informasi + Pendekatan CobIT*. Jakarta:Mitra Wacana Media. ISBN:978-979-1092-11-1. 2014.

Hasibuan, Zaenal A. 2007. *Metodologi Penelitian Pada Bidang Ilmu Komputer dan Teknologi Informasi.* Jakarta: Universitas Indonesia.

Hikmawati, Fenti. 2017. *Metodologi Penelitian.* Depok: PT. Raja Grafindo Persada.

Jogiyanto. 2005. *Analisis & Desain*. Yogyakarta: ANDI OFFSET.

Kamat, Mohan. 2009. *Guideline for Roles & Responsibilities in Information Asset Management*. ISO 27001 Implementer's Forum

Kusuma, R.A. 2014. *Audit Keamanan Sistem Informasi Berdasarkan Standard SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta.* Tidak dipublikasikan. Skripsi. Universitas Islam Negeri Sunan Kalijaga.

Made, *dkk*. 2012. *Bakuan Audit Keamanan Sistem Informasi Kemenpora*. Jakarta. Kementerian Pemuda dan Olahraga Republik Indomesia.

Mulyadi.2012. *Auditting*. Jakarta: Salemba Empat

Puspitasari, D. 2005. *Audit Sistem Manaemen Keamanan Sistem Informasi Apotek Sanata Dharma*. Tidak dipublikasikan. Skripsi. Fakultas Teknik Informatika. Unviersitas Islam Sunan Kalijaga.

Putro, Bramantiyo E. 2016. *Analisa Control Audit pada Klausul A.5 Security Policy hingga Klausul A.9 Physical and Enviromental Security Telkom Flexi Kebon Sirih Jakarta Pusat menggunakan ISO/IEC 27001*. Vol. 88 No 1. Jurnal Informatika.

Rahayu, *dkk*.2017. *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI)*. Jakarta : Kementerian Komunikasi dan Informatika

Rosmiati, Imam Riadi.2016. *Analisis Keamanan Sistem Informasi Berdasarkan Kebutuhan Teknikal dan Operasional Mengkombinasikan Standard ISO*

27001: 2005 dengan Maturity Level (Studi Kasus : Kantor Biro Teknologi Informasi PT. XYZ). Magister Teknik Informatika Universitas Islam Indonesia Yogyakarta.

Windirya, Danastri R.2013. *Audit Keamanan Sistem Informasi pada Instalasi Sistem Informasi Manajemen RSUD Bangil berdasarkan ISO 27002*. Vol 3, No.2. Jurnal Sistem Informasi.

Zulfikar, *dkk*. 2013. *Audit Keamanan Informasi PT. XYZ.* Volume 4. No. 2. Jurnal Masyarakat Telematika dan Informasi.

LAMPIRAN I

Lampiran SK Pembimbing

KEPUTUSAN DEKAN FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN) RADEN FATAH PALEMBANG
NOMOR : 123 TAHUN 2018

TENTANG

PENUNJUKAN PEMBIMBING SKRIPSI STRATA SATU (S.1)
BAGI MAHASISWA TINGKAT AKHIR FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN) RADEN FATAH PALEMBANG

DEKAN FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN) RADEN FATAH PALEMBANG

Menimbang :
1. Bahwa untuk mengakhiri Program sarjana (S1) bagi Mahasiswa, maka perlu ditunjuk Tenaga ahli sebagai Pembimbing Utama dan Pembimbing kedua yang bertanggung jawab dalam rangka penyelesaian Skripsi Mahasiswa;
2. Bahwa untuk lancarnya tugas pokok itu, maka perlu dikeluarkan Surat Keputusan Dekan (SKD) tersendiri. Dosen yang ditunjuk dan tercantum dalam SKD ini memenuhi syarat untuk melaksanakan tugas tersebut.

Mengingat :
1. Undang-Undang No. 20 Tahun 2003 tentang Sistem Pendidikan Nasional;
2. Undang-Undang No. 14 Tahun 2005 tentang Guru dan Dosen;
3. Undang-Undang No.12 Tahun 2012 tentang Pendidikan Tinggi;
4. Peraturan Pemerintah Nomor 9 Tahun 2003 tentang Wewenang Pengangkatan, Pemindahan dan Pemberhentian Pegawai Negeri Sipil;
5. Peraturan Pemerintah No. 19 Tahun 2005 tentang Standar Nasional Pendidikan;
6. Peraturan Menteri Agama RI No. 53 Tahun 2015 tentang Organisasi dan tata kerja Institut Agama Islam Negeri Raden Fatah Palembang;
7. Peraturan Menteri Keuangan Nomor 53/PMK.02.2014 tentang Standar Biaya Masukan;
8. Peraturan Menteri Pendidikan dan Kebudayaan No.154/2014 tentang Rumpun Ilmu pengetahuan dan Teknologi serta Gelar Lulusan Perguruan Tinggi;
9. Peraturan Menteri Agama No.62 tahun 2015 tentang Statuta Universitas Islam Negeri (UIN) Raden Fatah Palembang;
10. Peraturan Menteri Agama No.33 tahun 2016 tentang Gelar Akademik Perguruan Tinggi Keagamaan;
11. Keputusan Menteri Agama No.394 tahun 2003 tentang Pedoman Pendirian Perguruan Tinggi Agama;
12. DIPA Universitas Islam Negeri Raden Fatah Palembang Tahun 2017;
13. Keputusan Rektor Universitas Islam Negeri Raden Fatah Nomor 669B Tahun 2014 tentang Standar Biaya Honorarium dilingkungan Universitas Islam Negeri Raden Fatah Palembang Tahun 2015;
14. Peraturan Presiden Nomor 129 Tahun 2014 tentang Alih Status IAIN menjadi Universitas Islam Negeri.

M E M U T U S K A N

MENETAPKAN

Pertama : Menunjuk sdr. :
1. Rusmala Santi, M.Kom — NIP : 197911252014032002
2. Muhammad Kadafi — NIDN : 0223108404

Dosen Fakultas Sains dan Teknologi Universitas Islam Negeri (UIN) Raden Fatah Palembang masing-masing sebagai Pembimbing Utama dan Pembimbing Kedua Skripsi Mahasiswa :

Nama : **YENI RAHAYU**
NIM/Jurusan : 14540170/ Sistem Informasi
Semester/Tahun : Genap / 2017 – 2018
Judul Skripsi : Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001: 2005

Kedua : Kepada Pembimbing Utama dan Pembimbing Kedua tersebut diberi hak sepenuhnya untuk merevisi judul/ kerangka dengan sepengetahuan Fakultas.

Ketiga : Masa berlakunya Surat Keputusan Dekan ini Terhitung Mulai Tanggal di tetapkannya sampai dengan Tanggal 11 Juli 2019

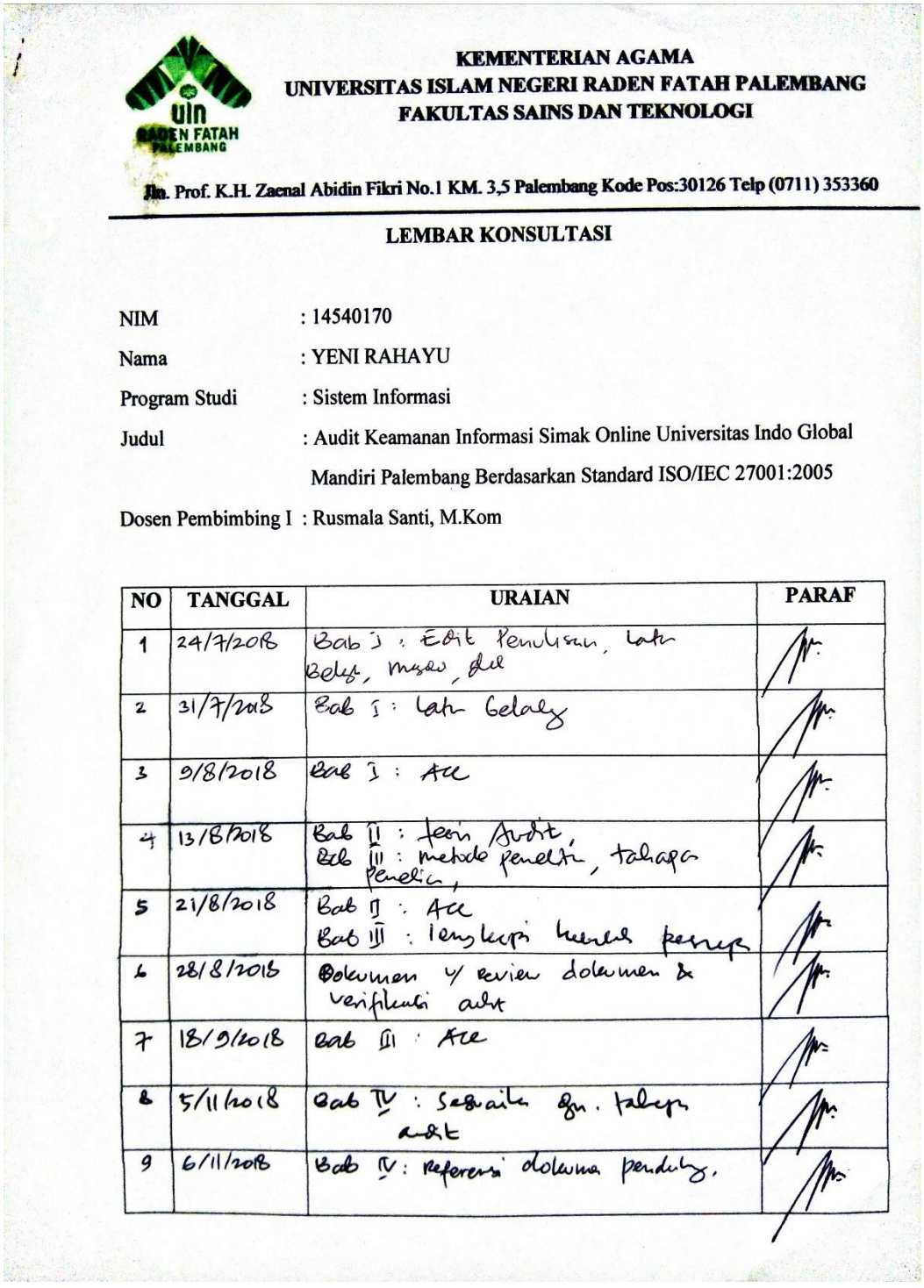
Keempat : Keputusan ini mulai berlaku satu tahun sejak tanggal ditetapkan dan akan ditinjau kembali apabila dikemudian hari ternyata terdapat kekeliruan dalam penetapan ini.

DITETAPKAN DI : PALEMBANG
PADA TANGGAL : 11 – 07 – 2018
REKTOR
DEKAN

DIAN ERLINA

TEMBUSAN :
1. Rektor UIN Raden Fatah Palembang ;
2. Ketua Prodi Sistem Informasi Fakultas Sains dan Teknologi UIN - RF Palembang ;
3. Mahasiswa yang bersangkutan.

Lampiran Lembar Konsultasi Pembimbing I



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI

Jln. Prof. K.H. Zaenal Abidin Fikri No.1 KM. 3,5 Palembang Kode Pos:30126 Telp (0711) 353360

LEMBAR KONSULTASI

NIM : 14540170
Nama : YENI RAHAYU
Program Studi : Sistem Informasi
Judul : Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001:2005
Dosen Pembimbing I : Rusmala Santi, M.Kom

NO	TANGGAL	URAIAN	PARAF
1	24/7/2018	Bab I : Edit Penulisan, Latar Belg, masal, dll	
2	31/7/2018	Bab I : Latar Belakang	
3	9/8/2018	Bab I : Acc	
4	13/8/2018	Bab II : Teori Audit, Bab III : metode penelitian, tahapan penelitian,	
5	21/8/2018	Bab II : Acc Bab III : lengkapi metode penelitian	
6	28/8/2018	Dokumen y/ review dokumen & verifikasi audit	
7	18/9/2018	Bab III : Acc	
8	5/11/2018	Bab IV : Sesuaikan dgn. tahapan audit	
9	6/11/2018	Bab IV : Referensi dokumen pendukung.	

Lampiran Lembar Konsultasi Pembimbing I

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI

Jln. Prof. K.H. Zaenal Abidin Fikri No.1 KM. 3,5 Palembang Kode Pos:30126 Telp (0711) 353360

LEMBAR KONSULTASI

NIM : 14540170
Nama : YENI RAHAYU
Program Studi : Sistem Informasi
Judul : Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001:2005
Dosen Pembimbing I : Rusmala Santi, M.Kom

NO	TANGGAL	URAIAN	PARAF
10	8/11/2018	Bab IV : Acc Bab V : simpulan kalimat jelas,	
		Saran, Dgn. kalimat saran Abstrak : langsung ke masalah	

Lampiran Lembar Konsultasi Pembimbing II

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI

Jln. Prof. K.H. Zaenal Abidin Fikri No.1 KM. 3,5 Palembang Kode Pos:30126 Telp (0711) 353360

LEMBAR KONSULTASI

NIM : 14540170
Nama : YENI RAHAYU
Program Studi : Sistem Informasi
Judul : Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001:2005
Dosen Pembimbing II : Muhamad Kadafi, M.Kom

NO	TANGGAL	URAIAN	PARAF
	10/7-18	Perbaiki latar belakang	
	11/7 18	—11—	
	16/7-18	Perbaiki latar belakang	
	18/7-18	perbaiki latar belakang	
	23/7-18	Acc Bab 2 Lanjut Bab 3	
	25/7-18	Acc Bab 2 Lanjut Bab 3	
	8/8-18	Acc Bab 3 (perbaiki tahapan penelitian)	
		Lanjut Bab IV	

Lampiran Lembar Konsultasi Pembimbing II

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI

Jln. Prof. K.H. Zaenal Abidin Fikri No.1 KM. 3,5 Palembang Kode Pos:30126 Telp (0711) 353360

LEMBAR KONSULTASI

NIM : 14540170

Nama : YENI RAHAYU

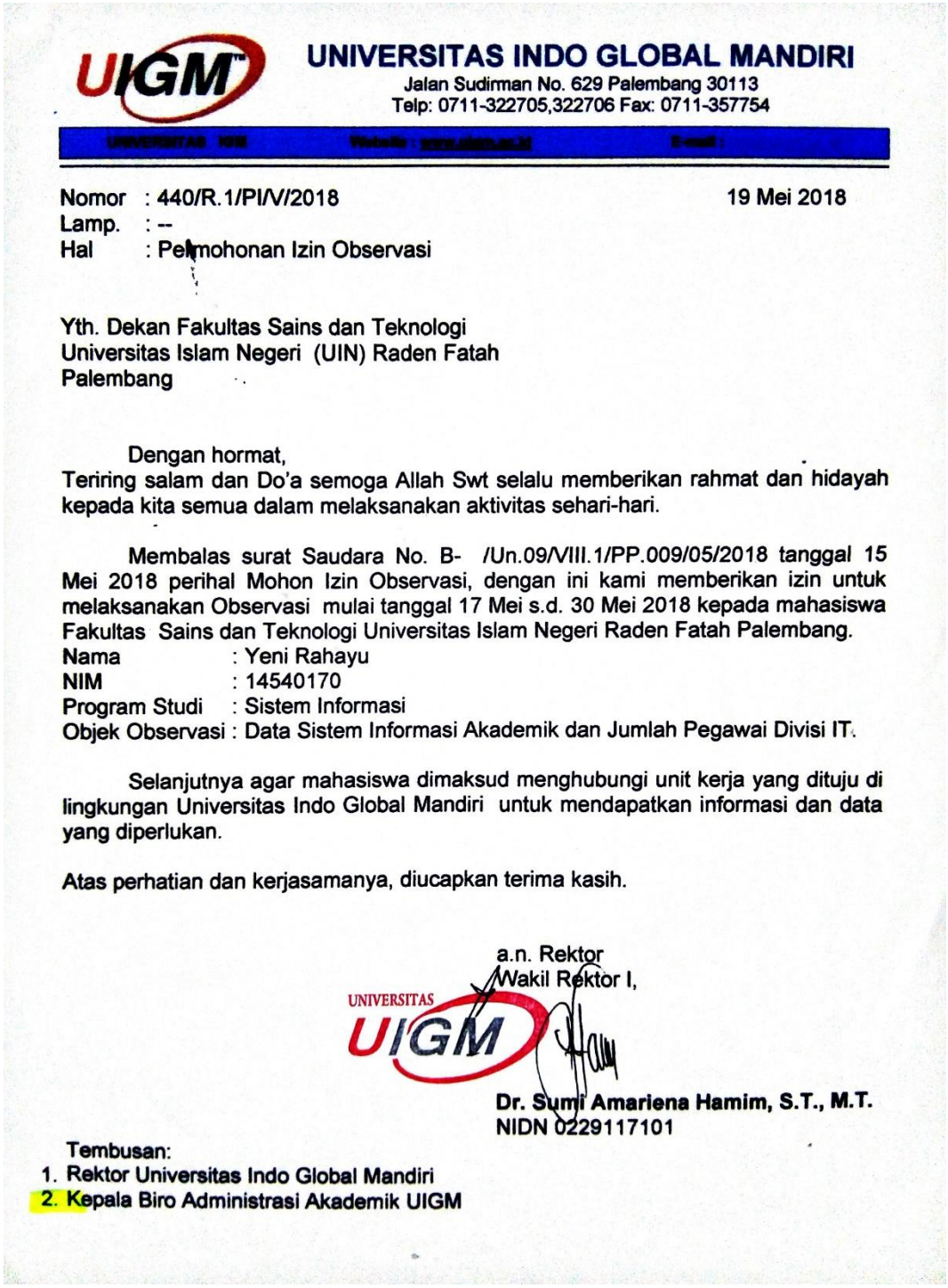
Program Studi : Sistem Informasi

Judul : Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001:2005

Dosen Pembimbing II : Muhamad Kadafi, M.Kom

NO	TANGGAL	URAIAN	PARAF
	26/-18. /10	Pelajari Penelitian yg terkait, Pahami Materi.	
	5/-18. /11	Acc Bab 4 Lanjut Bab 5	
	12/-18 /11	Acc Bab 5 Lap ujian Seminar Hasil	

Lampiran Surat Balasan Surat Izin Observasi



UNIVERSITAS INDO GLOBAL MANDIRI
Jalan Sudirman No. 629 Palembang 30113
Telp: 0711-322705,322706 Fax: 0711-357754

Nomor : 440/R.1/PI/V/2018 19 Mei 2018
Lamp. : --
Hal : Permohonan Izin Observasi

Yth. Dekan Fakultas Sains dan Teknologi
Universitas Islam Negeri (UIN) Raden Fatah
Palembang

Dengan hormat,
Teriring salam dan Do'a semoga Allah Swt selalu memberikan rahmat dan hidayah kepada kita semua dalam melaksanakan aktivitas sehari-hari.

Membalas surat Saudara No. B- /Un.09/VIII.1/PP.009/05/2018 tanggal 15 Mei 2018 perihal Mohon Izin Observasi, dengan ini kami memberikan izin untuk melaksanakan Observasi mulai tanggal 17 Mei s.d. 30 Mei 2018 kepada mahasiswa Fakultas Sains dan Teknologi Universitas Islam Negeri Raden Fatah Palembang.

Nama : Yeni Rahayu
NIM : 14540170
Program Studi : Sistem Informasi
Objek Observasi : Data Sistem Informasi Akademik dan Jumlah Pegawai Divisi IT.

Selanjutnya agar mahasiswa dimaksud menghubungi unit kerja yang dituju di lingkungan Universitas Indo Global Mandiri untuk mendapatkan informasi dan data yang diperlukan.

Atas perhatian dan kerjasamanya, diucapkan terima kasih.

a.n. Rektor
Wakil Rektor I,

Dr. Sumi Amariena Hamim, S.T., M.T.
NIDN 0229117101

Tembusan:
1. Rektor Universitas Indo Global Mandiri
2. Kepala Biro Administrasi Akademik UIGM

Lampiran Surat Izin Penelitian

UNIVERSITAS ISLAM NEGERI (UIN)
RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI

Nomor : B-1302 /Un.09/VIII.1/PP.009/07/2018 16 Juli 2018
Sifat : Penting
Lampiran : -
Hal : **Mohon Izin Penelitian**
An. Yeni Rahayu

Kepada
Yth. Kepala Divisi IT Universitas Indo Global Mandiri
di Palembang

Dalam rangka penyelesaian penulisan Karya Ilmiah berupa skripsi mahasiswa kami :

N a m a	: YENI RAHAYU
NIM / Program Studi	: 14540170 / Sistem Informasi
Alamat	: Gg. Sesy No. 1083 Sekip Jaya Kemuning Palembang
Judul	: Audit Keamanan Informasi SIMAK Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001 : 2005
Waktu Penelitian	: 20 Juli s/d 30 September 2018
Objek Penelitian	: Data sistem informasi (SIMAK Online) dan jumlah pegawai Divisi IT

Sehubungan dengan itu kami mengharapkan bantuan Bapak untuk dapat memberikan izin kepada mahasiswa tersebut untuk melaksanakan penelitian di Instansi/Lembaga yang Bapak pimpin, sehingga memperoleh data yang dibutuhkan.

Demikianlah harapan kami dan atas segala bantuan serta perhatian Bapak, kami haturkan terima kasih.

Dekan,

Dian Erlina

Knowledge, Quality & Integrity

Jl. Prof. K. H. Zainal Abidin Fikry No. 1 Km. 3,5 Palembang 30126
Telp. (0711) 354668 website : www.saintek.radenfatah.ac.id

Lampiran Surat Balasan Surat Izin Penelitian

UNIVERSITAS INDO GLOBAL MANDIRI
Jalan Sudirman No. 629 Palembang 30113
Telp: 0711-322705,322706 Fax: 0711-357754

Nomor : 575/R.1/PI/VII/2018 — 25 Juli 2018
Lamp. : --
Hal : Permohonan Izin Penelitian
a.n. Yeni Rahayu

Yth. Dekan Fakultas Sains dan Teknologi
Universitas Islam Negeri (UIN) Raden Fatah
Palembang

Dengan hormat,

Membalas surat Saudara No. 13-1302/Un.09/VIII.1/PP.009/07/2018 tanggal 16 Juli 2018 prihal seperti pada pokok surat, dengan ini kami memberikan izin untuk melaksanakan Penelitian dari tanggal 20 Juli s.d. 30 September 2018 kepada mahasiswa Fakultas Sains dan Teknologi UIN Raden Fatah Palembang,

Nama	: Yeni Rahayu
NIM	: 14540170
Program Studi	: Sistem Informasi
Judu Penelitian	: Audit Keamanan Informasi SIMAK *Online* Universitas Indo Global Mandiri Palembang Berdasarkan Standad ISO/IEC 27001 : 2005.

Selanjutnya agar mahasiswa yang bersangkutan berkoordinasi dengan Biro Pelaksana Teknis Universitas Indo Global Mandiri untuk mendapatkan informasi dan data yang diperlukan.

Atas perhatian dan kerjasamanya, diucapkan terima kasih.

a.n. Rektor
Wakil Rektor I,

Dr. Sumi Amariena Hamim, S.T., M.T.
NIDN 0229117101

Tembusan:
1. Rektor Universitas Indo Global Mandiri
2. Kepala Biro Pelaksana Teknis Universitas Indo Global Mandiri
3. Mahasiswa ybs.

Lampiran Berita Acara Observasi

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI
Jln. Prof. K.H. Zaenal Abidin Fikri No.1 KM. 3,5 Palembang Kode Pos:30126 Telp (0711) 353360 website: www.radenfatah.ac.id

BERITA ACARA

Pada tanggal 28 Mei 2018 telah dilaksanakan kegiatan observasi yang berkaitan dengan penelitian yang akan dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat : Universitas Indo Global Mandiri Palembang (UIGM Palembang)
Bagian : Biro Pelalaksana Teknis (BPT)

Pihak peneliti melakukan wawancara dengan pihak narasumber yang berkaitan dengan penelitian yang akan dilakukan di Universitas Indo Global Mandiri Palembang, yang kemudian narasumber memberikan jawaban terkait pertanyaan yang diajukan oleh pewawancara. Adapun pertanyaan yang diajukan serta hasil wawancara terlampir.

Palembang, 28 Mei 2018

Peneliti

(Yeni Rahayu)

Kepala Seksi Hardware dan Jaringan

(Reza Maulana, A.Md)

Lampiran :

- Pertanyaan wawancara
- Hasil wawancara

Lampiran Berita Acara Pengambilan Data dan Wawancara

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI
Jln. Prof. K.H. Zaenal Abidin Fikri No.1 KM. 3,5 Palembang Kode Pos:30126 Telp (0711) 353360 website: www.radenfatah.ac.id

BERITA ACARA

Pada tanggal 26 September 2018 telah dilaksanakan kegiatan pengambilan data yang berkaitan dengan penelitian yang akan dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat : Universitas Indo Global Mandiri Palembang (UIGM Palembang)
Bagian : Biro Penunjang Teknis (BPT)

Pihak peneliti melakukan wawancara dengan pihak narasumber yang berkaitan dengan penelitian yang akan dilakukan di Universitas Indo Global Mandiri Palembang, yang kemudian narasumber memberikan jawaban terkait pertanyaan yang diajukan oleh pewawancara. Adapun pertanyaan yang diajukan serta hasil wawancara terlampir.

Palembang, 29 September 2018

Peneliti

(Yeni Rahayu)

Kepala Biro Penunjang Teknis

(Dr. Herri Setiawan, M.Kom)

Lampiran :

- Pertanyaan wawancara
- Hasil wawancara

LAMPIRAN II

Lampiran Audit Charter

Audit Charter

Project ID : ISO/IEC27001:2005-Audit-01

Project Name : Information Security Audit

Auditor : Yeni Rahayu

Project Description :

Penelitian ini berkaitan dengan keamanan informasi terhadap Sistem Informasi Akademik (SIMAK) *Online* Universitas Indo Global Mandiri menggunakan standard ISO/IEC 27001:2005 dengan berfokus pada 11 klausul dan kontrol keamanan informasi.

Project Schedule : September – Oktober

Stakeholder list :

Jabatan	Responden	Klausul pengendalian
Director Information Management	Tasmi, S.Si., M.Kom	ISO/IEC 27001:2005 klausul A.5, A.6 dan A.7
Kepala Biro Pelaksana Teknis (Chief Information Officer)	Dr. Herri Setiawan, M.Kom	ISO/IEC 27001:2005 klausul A.8, A.14 dan A.15
Director Information Management	Tasmi, S.Si., M.Kom	ISO/IEC 27001:2005 klausul A.5, A.6 dan A.7
Kepala Seksi Jaringan dan Hardware (Information Security Officer)	Reza Maulana, A.Md	Manajemen Operasi dan Komunikasi ISO/IEC 27001:2005 klausul A.10 dan A.12
Teknisi Laboratorium (Information Security Officer)	Parhan Oktaria Putra	ISO/IEC 27001:2005 klausul A.9
Teknisi (Information Security Officer)	Jimiria Pratama	ISO/IEC 27001:2005 klausul A.11 dan A.13

Palembang, 2018

Mengetahui Kepala Biro Pelaksana Teknis	Auditor
Universitas Indo Global Mandiri Palembang	
Dr. Herri Setiawan, M.Kom	Yeni Rahayu
NIK : 2003010060	NIM : 14540170

Tabel 4.2 List Pertanyaan Klausul ISO/IEC 27001:2005

Klausul A.5 Kebijakan Keamanan

KLAUSUL	KODE	PERTANYAAN
Klausul A.5.1.1	Q1	Apakah sudah ada keijakan keamanan informasi?
	Q2	Apakah sudah terdokumentasi kebijakan keamanan informasi tersebut?
	Q3	Apakah dokumen kebijakan tersebut sudah dipublikasikan kepada seua pihak terkait?
	Q4	Apakah kebijakan tersebut sudah disosialisasikan dalam bentuk yang relevan, mudah diakses, dan dimengerti?
Klausul A.5.1.2	Q5	Jika terjadi perubahan kebijakan, apakah kebijakan tersebut tetap disesuaikan dengan kefektifan yang berkelanjutan?
	Q6	Apakah perubahan kebijakan tersebut akan dikomunikasikan kepada semua pihak?
	Q7	Apakah ada pernyataan komitmen manajemen serta dukungan terhadap tujuan dan prinsi keamanan informasi?
	Q8	Apakah semua pegawai telah benar-benar memahami keamanan informasi?
	Q9	Apakah kebijakan keamanan informasi sudah dilakukan tinjauan ulang funa mengantisipasi setiap perubahan yang mempengaruhi analisa resiko, seperti kerawanan?
	Q10	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal?

Klalusul A.6 Organisasi Keamanan Informasi

KLAUSUL	KODE	PERTANYAAN
A.6.1.1	Q132	Apakah manajemen terhadap keamanan informasi telah mendukung secara aktif keamanan dalam organisasi dengan arahan yang jelas, komitmen dan penugasan eksplisit?
	Q133	Manajemen tersebut telah bertanggung jawab atas keamanan informasi?
A.6.1.2	Q134	Apakah kegiatan keamanan informasi telah di koordinasi oleh wakil-wakil dari bagian organisasi yang sesuai dengan peran masing-masing?
	Q135	Apakah sudah tedokumentasikan kegiatan kemanan informasi tersebut?

A.6.1.3	Q136	Seluruh tanggung jawab keamanan informasi sudah ditetapkan dengan jelas?
	Q136	Sudah terdokumentasikan kebijakan tersebut?
A.6.1.4	Q137	Apakah telah ditetapkan manajemen fasilitas pengolahan informasi teknik?
	Q138	Apakah sudah terlaksana manajemen pengolahan informasi tersebut?
A.6.1.5	Q139	Apakah sudah diidentifikasi persyaratan dan perjanjian kerahasiaan kebutuhan organisasi untuk melindungi informasi?
	Q140	Apakah kebijakan persyaratan dan perjanjian kerahasiaan organisasi dalam melindungi informasi telah dikaji secara regular?
A.6.1.6	Q141	Kontak dengan pihak berwenang telah terpelihara?
A.6.1.7	Q142	Apakah telah dilaksanakan dan dipelihara kontak dengan kelompok khusu (*special interest*) tau forum ahli keamanan dan asosiasi profesi?
A.6.1.8	Q143	Apakah telah dikaji secara independen pendekatan organisasi untuk mengelola informasi dan penerapannya (sasaran pengendalian, kebijakan, prosedur keamanan infromasi)?
	Q144	Telah dikaji apabila terjadi perubahan signifikan terhadap terhadap penerapan keamanan?
A.6.2.1	Q145	Apakah sudah diidentifikasi resiko terhadap informasi organisasi dan fasilitas pengolahan informasi dari proses bisnis yang melibatkan pihak eksternal?
	Q146	Apakah telah disesuaikan pngendalian terhadap pihak eksternal sebelum pemberian akses?
A.6.2.2	Q147	Sudah diidentifikasi persyaratan keamanan yang harus ditekankan sebelum memberikan hak akses kepada pelanggan informasi atau aset organisasi?
A.6.2.3	Q148	Apakah sudah ada persyaratan keamanan yang relevan terhadap perjanjian pihak ketiga yang meliputi : pengaksesan, pengloahan, komunikasi atau penambahan roduk jasa kedalam aktifitas pengolahan informasi?

Klausul A.7 Pengelolaan Aset

KLAUSUL	KODE	PERTANYAAN
Klausul A.7.1.1	Q11	Apakah semua inventaris aset (aset informasi, aset piranti lunak, aset fisik dan layanan) sudah diidentifikasi dan dicatat?
	Q12	Masing-masing aset apakah sudah disusun dan dipelihara?
	Q13	Apakah sudah ada kebijakan pengelolaan inventaris aset?

	Q14	Apakah klasifikasi lokasi keamanan aset sudah didokumentasikan (sebagai catatan jika terjadi kehilangan dan kerugian)?
Klausul A.7.1.2	Q15	Apakah sudah ditentukan pegawai atau sub bagian yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset?
	Q16	Siapa yanng bertanggung jawab mengontrol dan memelihara terhadap inventaris aset?
	Q17	Berapa jangka waktu pengecekan inventaris aset secara berkala?
	Q18	Apakah sudah diidentifikasi tingkat kepentingan aset?
Kalusus A.7.1.3	Q19	Apakah ada aturan-aturan ketika pihak-pihak tertentu menggunakan informasi aset?
	Q20	Apakah informasi pengelolaan aset sudah terdokumentasi?
	Q21	Seberapa perlunya informasi pengolahan aset didokumentasikan?
Klausul A.7.2.1	Q22	Apakah informasi aset di klasifikasikan dengan tingkat perlindungan yang tepat?
	Q23	Bagaimanakah prosedur pengklasifikasian informasi pengelolaan aset tersebut?
Klausul A.7.2.2	Q24	Apakah ada satu set prosedur untuk menentukan pemberian tanda pelabelan dan penanganan informasi yang bersifat rahasia atau penting?
	Q25	Apakah prosedur tersebut sudah mencakup informasi baik secara fisik maupun dalam format elektronik?
	Q26	Apakah penanganan informasi dikembangkan dan diterapkan?

Klausul A.8 Keamanan Sumber Daya Manusia

KLAUSUL	KODE	PERTANYAAN
Klausul A.8.1.1	Q27	Apakah sudah ditetapkan kebijakan keamanan informasi terkait peran dan tanggung jawab dari pegawai, kontraktor dan pengguna pihak ketiga?
	Q28	Apakah sudah didokumentasikan kebijakan keamanan informasi tersebut?
Klausul A.8.1.2	Q29	Apakah sudah dilaksanakan menurut hukum dan undang-undang yang berlaku untuk verifikasi latar belakang calon pegawai, kontraktor dan pihak ketiga?
	Q30	Apakah sudah ada kebijakan terhadap akses informasi terhadap pegawai, kontraktor dan pihak ketiga?
Klausul A.8.1.3	Q31	Apakah sudah ditetapkan aturan dan syarat kontrak calon pegawai, kontraktor dan pihak ketiga?

	Q32	Apakah ketetapan tersebut sudah terdokumentasikan?
	Q33	Apakah sudah diterapkan persetujuan dan menandatangani kontrak untuk tanggung jawab dan kewajiban sebagai pegawai, kontraktor atau pihak ketiga terhadap keamanan informasi?
Klausul A.8.2.1	Q34	Apakah sudah diterapkan kebijakan dan prosedur keamanan informasi kepada pegawai, kontraktor dan pihak ketiga selama bekerja?
	Q35	Apakah sudah terdokumentasikan kebijakan dan prosedur tersebut?
Klausul A.8.2.2	Q36	Apakah ada prosedur dan kebijakan mengenai pelatihan serta pendidikan terlebih dahulu kepada pegawai, kontraktor dan pihak ketiga secara regular sesuai dengan fungsi kerjanya?
	Q37	Apakah prosedur tersebut sudah terdokumentasikan?
	Q38	Apakah ada kebijakan pendisiplinan ketika pegawai melakukan pelanggaran keamanan?
	Q39	Apakah peraturan kebijakan tersebut sudah terdokumentasikan?
Klausul A.8.2.3	Q40	Apakah sudah ditetapkan kebijakan dalam pengakhiran atau perubahan pekerjaan terhadap pegawai?
Klausul A.8.3.1	Q41	Apakah sudah didokumentasikan kebijakan prosedur tanggung jawab perubahan atau pengakhiran pekerjaan tersebut?
	Q42	Apakah sudah ditetapkan peraturan atau syarat apabila pegawai, kontraktor, dan pihak ketiga dalam mengembalikan semua aset organisasi yang digunakan apabila perjanjian berakhir?
	Q43	Apakah sudah terdokumentasi peraturan tersebut?
Klausul A.8.3.2	Q44	Apakah ada aturan atau persyaratan dalam pengahapusan hak akses apabila pegawai, kontraktor dan pihak ketiga ketika pengakhiran pekerjaan atau perjanjian telah berakhir?
Klausul A.8.3.3	Q45	Apakah fasilitas pengolahan informasi dihapuskan ketika pekerjaan kontrak atau perjanjian berakhir?

Klausul A.9 Keamanan Fisik dan Lingkungan

KLAUSUL	KODE	PERTANYAAN
Klausul A.9.1.1	Q46	Apakah pintu masuk sudah dikendalikan dengan kartu gesek atau PIN guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas?
	Q47	Apakah penting pintu masuk ruang sistem informasi dibatasi dengan sistem pengamanan dan kartu kontrol?
	Q48	Apakah ada kontrol akses fisik atau ruang sebagai tempat menerima tamu?

	Q49	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain didalamnya?
	Q50	Perlukah ruangan khusus atas pembatas seperti dinding untuk seorang pemegang kendali sistem informasi?
Klausul A.9.1.2	Q51	Apakah pengunjung yang datang diawasi dan tanggal datang dan perginya dicatat?
	Q52	Apakah dikontrol dan dibatasi akses ke informasi sensitif dan fasilitas pengolahan informasi?
Klausul A.9.1.3	Q53	Semua pegawai dan karyawan apakah sudah diwajibkan memakai tanda pengenal?
	Q54	Apakah hak akses ke wilayah aman harus dikaji ulang dan diperbarui secara berkala?
Klausul A.9.1.4	Q55	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, kecelakaan dan bencana lainnya?
	Q56	Apakah bahan berbahaya dan mudah meledak sudah disimpan di wilayah yang aman?
Klausul A.9.1.5	Q57	Apakah penempatan ruang sistem informasi sudah termasuk dalam area yang aman?
	Q58	Apakah sudah mempertimbangkan kebijakan tentang makan, minum dam merokok disekitar fasilitas pemrosesan sistem informasi?
	Q59	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan?
Klausul A.9.1.6	Q60	Dari segi wilayah keamanan apakah penempatan posisi ruang sudah membuat nyaman pengelola sistem informasi?
	Q61	Jika ada perbaikan ruangan dan peralatan informasi lainnya apakah pekerja yang berasal dari luar BPT UIGM akan dilakukan pengawasan dan dipantau?
	Q62	Apakah penting mendampingi pekerja yang melakukan perbaikan dan bagaimana prosedur pengawasannya?
Klausul A.9.2.1	Q63	Apakah komputer dan peralatan informasi lainnya seperti server, sudah ditempatkan pada tempat yang cukup aman?
	Q64	Apakah keamanan peralatannya sudah tidak ada peluang akses pihak yang tidak berwenang?
Klausul A.9.2.2	Q65	Apakah peralatannya sudah dilindungi dari kegagalan catu daya listrik?
	Q66	Apakah sudah tersedia peralatan pendukung seperti UPS dan pembangkit listrik cadangan?
Klausul A.9.2.3	Q67	Apakah kabel daya dan telekomunikasi yang membawa data atau jasa sudah dilindungi dari penyadapan dan kerusakan, seperti menggunakan pipa pengaman?

	Q68	Apakah sudah dihindari melakukan routing melalui tempat umum?

Klausul A.10 Manajemen Komunikasi dan Operasi

KLAUSUL	KODE	PERTANYAAN
Klausul A.10.1.1	Q69	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara aman?
	Q70	Jika ada kesalhan operasi atau kesulitan teknis, apakah akan meminta bantuan pengelola/ pegawai lainnya?
	Q71	Apakah (back-up data) sudah dipelihara serta sudah dilakukakan sesuai prosedur?
Klausul A.10.1.2	Q72	Jika ada perubahan terhadap fasilitas dan sistem pengolahan sistem informasi apakah sudah dikontrol dan kendalikan?
	Q73	Apakah sudah dilakukan pencataan perubahan dan apakah perubahan tersebut sudah disosialisasikan ke semua pihak?
Klausul A.10.1.3	Q74	Apakah pegawai di ruang BPT sudah dipisahkan menurut tugas dan tanggung jawab masing-masing?
	Q75	Apakah ada pemantauan dan pengawasan untuk mengurangi resiko insiden memodifikasi tanpa ijin atau penyalahgunaan sistem?
Klausul A.10.2.1	Q76	Apakah tingkat layanan yang dicakup dalam perjanjian pelayananan jasa pihak ketiga sudah diterapkan, dioperasikan dan dipelihara oleh pihak ketiga?
		Apakah salinan back-up dan piranti lunak yang penting sudah dilakukan secara berkala?
Klausul A.10.2.2	Q77	Apakah jasa, laporan dan rekaman yang diberikan oleh pihak ketiga sudah dipantau, dikaji dan diaudit secara regular?
Klausul A.10.3.1	Q78	Apakah peggunaan sumberdaya sudah dipantau dan disesuaikan untuk pemenuhan kapasitas mendatang?
Klausul A.10.3.2	79	Apakah sudah selalu dilakukan pengujian terhadap sistem informasi yang baru, upgrade atau versi terbaru sebelum diterima?
Klausul A.10.5.1	Q80	Apakah fasilitas back-up sudah memadai guna memulihkan seluruh sistem informasi jika terjadi bencana atau kegagalan?
	Q81	Catatan yang akurat dari salinan back-up dan prosedur pemulihan yang terdokumentasi apakah sudah disimpan di lokasi yang terpisah?
	Q82	Apakah media back-up sudah diuji secara berkala untuk memastikan bisa digunakan di situasi darurat?

Klausul A.10.6.1	Q83	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan data dalam jaringan?
	Q84	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan?
Klausul A.10.6.2	Q85	Apakah sudah menerapkan mekanisme pengamanan jaringan yang rawan terhadap serangan?
	Q86	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan?
	Q87	Apabila serangan terjadi, adakah mekanisme recovery jaringan yang diterapkan?
	Q88	Seberapa sering fitur keamanan dan tingkat layanan jaringan di identifikasi?
Klausul A.10.7.1	Q89	Apakah ada prosedur untuk manajemen pemindahan media?
	Q90	Apakah sudah terdokumentasi prosedur tersebut?
Klausul A.10.7.2	Q91	Apakah ada tindakan pemusnahan media apabila tidak lagi diperlukan?
	Q92	Apakah ada prosedur pemusnahan media?
	Q93	Apakah sudah terdokumentasi prosedur tersebut?
Klausul A.10.7.3	Q94	Apakah sudah ada prosedur penanganan dan penyimpanan informasi untuk melindungi informasi dari penyalahgunaan?
	Q95	Apakah sudah terdokumentasi prosedur tersebut?
Klausul A.10.7.4	Q96	Apakah sudah ada dokumentasi sistem untuk melindungi terhadap akses yang tidak sah?
Klausul A.10.8.1	Q97	Apakah sudah ada kebijakan prosedur dan pengendalian untuk melindungi pertukaran informasi dengan menggunakan semua jenis fasilitas komunikasi?
	Q98	Apakah sudah terdokumentasikan prosedur tersebut?
Klausul A.10.8.2	Q99	Apakah ada perjanjian terhadap pertukaran infromasi dan perangkat lunak antara organisasi dan pihak eksternal?
Klausul A.10.8.3	Q100	Apakah sudah disediakan media untuk memuat informasi terhadap hak akses yang tidak sah, penyalahgunaan atau kerusakan selama transportasi diluar batas fisik organisasi?
Klausul A.10.8.4	Q101	Apakah ada perlindungan informasi yang disajikan dalam bentuk pesan elektronik?
Klausul A.10.10.1	Q102	Apakah sudah tersedia log untuk merekam kegiatan pengguna dan kejadian keamanan informasi dalam membantu investigasi dan pemantauan akses?

Klausul A.10.10.2	Q103	Apakah ada prosedur pemantauan penggunaan fasilitas pengolahan informasi dan hasil kegiatan pemantauan ditinjau secara regular?
Klausul A.10.10.3	Q104	Apakah sudah tersedia fasilitas log dan informasi yang harus dilindungi terhadap gangguan dan akses tidak sah?
Klausul A.10.10.4	Q105	Apakah sudah tercacat dalam log kegiatan administrator sistem dan operator sistem?
Klausul A.10.10.5	Q106	Apabila terjadi kesalahan, apakah sudah tercatat dalam log, dianalisis dan diambil tindakan yang sesuai?

Klausul A.11 Pengendalian Akses

KLAUSUL	KODE	PERTANYAAN
Klausul A.11.1.1	Q107	Apakah sudah ditetapkan kebijakan pengendalian akses?
	Q108	Apakah kebijakan tersebut sudah terdokumentasikan berdasarkan persyaratan bisnis dan keamanan untuk akses?
Klausul A.11.2.1	Q109	Apakah ada prosedur pendaftaran dan pembatalan pendaftaran pengguna untuk memberi dan mencabut hak akses terhadap sistem informasi?
	Q110	Apakah sudah terdokumentasikan prosedur tersebut?
Klausul A.11.2.2	Q111	Apakah ada alokasi hak khusus yang harus dibatasi dan dikendalikan?
Klausul A.11.2.3	Q112	Apakah ada alokasi password untuk mengendalikan proses manajemen formal?
Klasusul A.11.2.4	Q113	Apakah sudah ada peninjauan terhadap hak akses pengguna secara regular menggunakan proses formal?
Klausul A.11.3.1	Q114	Apakah ada pedoman yang disyaratkan untuk pengamanan yang baik dalam pemilihan dan penggunaan password?
Klausul A.11.3.2	Q115	Apakah sudah ada kebijakan clear desk terhadap kertas dan media penyimpanan yang dapat di pindahkan untuk fasilitas pengolahan informasi?
	Q116	Apakah sudah ada kebijakan clear screen untuk fasilitas pengolahan informasi?
Klausul A.11.4.1	Q117	Apakah pengguna telah hanya diberikan akses terhadap layanan yang telah diberikan kewenangan penggunaanya secara spesifiik?
A.11.4.3	Q118	Apakah sudah diidentifikasi peralatan secara otomatis untuk mengotentifikasi koneksi lokasi dan peralatan spesifik?

Klausul A.11.4.4	Q119	Apakah sudah ada pelindungan pengendalian secara fisik dan logical terhadap diacnotic dan configuraiton port
Klausul A.11.4.6	Q120	Apakah sudah disegresikan terhadap layanan informasi pengguna dan sistem informasi di dalam jaringan?
Klausul A.11.4.7	Q121	Apakah sudah ada pengendalian routing yang telah diterapkan ke dalam jaringan untuk memastikan bahwa koneksi komputer dan aliran informasi tidak melanggar kebijakan pengendalian akses?
Klausul A.11.5.1	Q122	Apakah sudah ada prosedur log-on yang aman?
Klausul A.11.5.2	Q123	Apakah setiap pengguna mempunyai user id untuk penggunaan personal masing-masing user?
	Q124	Apakah sudah ada teknik validasi dalam setiap user id yang terdaftar?
Klausul A.11.5.3	Q125	Apakah sudah ada sistem manajemen password?
	Q126	Apakah sistem manajemen password yang ada suda interaktif?
Klausul A.11.5.5	Q127	Apakah dalam sistem informasi sudah diterapkan sesi time out?
	Q128	Bagaimana prosedurnya?
Klausul A.11.6.1	Q129	Apakah ada pembatasan terhadap akses informasi?
	Q130	Kepada siapa pembatasan itu dilakukan?
Klausul A.11.6.2	Q131	Apakah sistem yang sensitif sudah memiliki lingkungan komputasi yang diisolasi?

Klausul A.12 Akuisi, Pengembangan dan Pemeliharaan Sistem Informasi

KLAUSUL	KODE	PERTANYAAN
A.12.1.1	Q149	Apakah telah ditetapkan persyaratan bisnis untuk sistem infromasi yang baru?
	Q150	Apakah telah terdokumentasi persyaratan tersebut?
A.12.2.1	Q151	Apakah sudah ada prosedur validasi data ketika memasukkan data ke simak online UIGM?
	Q152	Apakah sudah ada prosedur untuk merespon kesalahan validasi?
A.12.2.2	Q153	Apakah digabungkan ke dalam aplikasi dalam pengecekan validasi untuk mendeteksi kerusakan informasi karena kesalahan?

	Q154	Ketika ada kerusakan informasi karena ada kesalahan pengolahan apakah bisa dideteksi oleh sistem?
A.12.2.3	Q155	Apakah sudah ada perlindungan integritas pesan dalam aplikasi?
	Q156	Sudah ada pengendalian yang tepat dalam persyaratan untuk memastikan keaslian dan perlindungan intgritas pesan dalam aplikasi?
	Q157	Apakah sudah diterapkan persyaratan tersebut?
A.12.2.4	Q158	Apakah sudah divalidasi dan diidentifikasi keluaran data dari aplikasi?
	Q159	Apakah sudah diterapkan validasi dan identifikasi keluaran tersebut?
A.12.3.1	Q160	Apakah sudah ada kebijakan pengendalian kriptografi untuk melindungi informasi?
	Q161	Apakah sudah dikembangkan dan diterapkan pengendalian kriptografi tersebut?
A.12.3.2	Q162	Apakah sudah ada manajemen kunci yang tersedia untuk mendukung penggunaan teknik kriptografi oleh organisasi?
A.12.4.1	Q163	Apakah ada prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional?
A.12.4.2	Q164	Apakah data sudah dipilih secara hati-hati dan dlindungi serta dikendalikan?
A.12.4.3	Q165	Apkah sudah dibatasi akses ke kode sumber program?
A.12.5.1	Q166	Apakah ada prosedur pengendalian yang formal jika terjadi perubahan dalam sistem aplikasi atau informasi?
	Q167	Apakah sudah diterapkan prosedur pengendalian tersebut?
	Q168	Apakah sudah terdokumentasi pengendalian tersebut?
A.12.5.2	Q169	Apakah sudah ditinjau dan diuji apaila ada perubahan sistem operasi atau aplikasi untuk memastikan tidak ada dampak yang merugikan terhadap organisasi?
	Q170	Apakah penting menjaga keamanan sistem informasi ketika dilakkukan perubahan sistem operasi?
A.12.5.3	Q171	Apakah sering melakukan modifikasi perangkat lunak?
	Q172	Apakah sudah dibatasi hanya pada perubahan yang perlu saja daam modifikasi perangkat lunak?
	Q173	Apa sudah dikendalikan dengan ketat seluruh perubahan tersebut?
A.12.5.4	Q174	Apakah sudah dicegah dalam peluang adanya kebocoran informasi?
A.12.5.5	Q178	Apakah sudah dipantau oleh organisasi pengembangan perangkat lunak yang dialihdayakan?

A.12.5.6	Q179	Apakah sudah dievaluasi informasi tepat waktu tentang kerawanan teknis dari sistem infromasi yang digunakan?
	Q180	Apakah sudah diambil tindakan untuk menangani resiko terkait?

Klausul A.13 Manajemen Insiden Keamanan Informasi

KLAUSUL	KODE	PERTANYAAN
A.13.1.1	Q175	Apakah sudah diambil tindakan dan dilaporkan melalui saluran manajemen yang tepat dan cepat apabila terjadi insiden keamanan informasi?
A.13.1.2	Q176	Apa sudah disyaratkan untuk mencatat dan melaporkan setiap kelemahan keamanan yang diamati dan dicurigai?
	Q177	Apakah sudah dilaporkan ke semua pegawai, kontraktor dan pengguna pihak ketiga ketika insiden terbut terjadi?
A.13.2.1	Q178	Apa sudah ditetapkan tanggung jawab manajemen apabila terjadi insiden keamanan informasi?
	Q179	Apakah sudah terdokumentasi ketetapan tersebut?
A.13.2.2	Q180	Apakah sudah tersedia mekanisme yang memungkinkan jenis, volume, dan biaya insiden keamanan informasi?
	Q181	Apakah sudah diukur dan dipantau mekanisme tersebut?
A.13.2.3	Q182	Apakah sudah diambil tindakan pengumpulan bukti terhadap orang atau organisasi selelah insiden keamanan informasi yang melibatkan tindakan hukum (baik perdata atau pidana)?
	Q183	Apakah sudah disimpan bukti terhadap insiden kemanan informasi tersebut?
	Q184	Apa sudah disajikan sesuai aturan berkenaan dengan bukti yang ditetapkan dalam wilayah hukum?

Klausul A.14 Manajemen Keberlanjutan Bisnis (*Business Coninuity Management*)

KLAUSUL	KODE	PERTANYAAN
A.14.1.1	Q185	Sudah dikembangkan dan diplihara untuk keberlanjutan bisnis organisasi secara menyeluruh?
	Q186	Apakah sudah dikembangkan dan dipelihara terkait penggunaan persyaratan keamanan informasi yang dibutuhkan uuntuk keberanjutan bisnis organisasi?
A.14.1.2	Q187	Apakah sudah diidentifikasi kejadian yang dapat menyebabkan gangguan terhadap proses bisnis?
	Q188	Apa sudah diidentifikasi terhadap kemungkinan dan dampak dari gangguan tersebut serta konsekuennya terhadap keamanan informasi?

A.14.1.3	Q189	Apakah sudah diterapkan rencana untuk memelihara atau mengembalikan operasi setelah terjadinya gangguan proses bisnis?
	Q190	Apakah sudah dikembangkan rencana untuk memastikan ketersediaan informasi pada tingkat dan dalam jangka waktu yang diisyaratkan setelah terjadi gangguan atau kegagalan proses bisnis?
A.14.1.4	Q191	Apakah sudah dipelihara kerangka kerja tunggal dari rencana keberlanjutan bisnis untuk memastikan rencana konsisten dan menekankan persyaratan keamanan informasi?
	Q192	Apakah sudah diidentifikasi prioritas untuk pengujian dan pemeliharan kerangka kerja tersebut?
A.14.1.5	\Q193	Apa sudah diuji dan dimutakhirkan secara regular tentang rencana keberlanjutan bisnis untuk memastikan rencana tersebut mutakhir dan efektif?

Klausul A.15 Kesesuaian

KLAUSUL	KODE	PERTANYAAN
A.15.1.1	Q196	Apakah sudah ditetapkan statuta, peraturan perundangan-undangan, dan persyaratan kontrak serta pendekatan organisasi untuk memenuhi persyaratan hukum yang berlaku mengenai keamanan informasi?
	Q197	Apakah sudah didokumentasikan pertaturan tersebut?
	Q198	Apakah sudah dijaga pemutakhirannya untuk masing-masing sistem informasi dan organisasi?
A.15.1.2	Q199	Apakah sudah ada prosedur untuk memastikan kesesuaian dengan peraturan perundang-undangan dan persyaratan kontrak tentang penggunaan materi yang berkenaan produk perangkat lunak yang memiliki hak paten?
	Q200	Apakah sudah diterapkan dan didokumentasikan prosedur tersebut?
A.15.1.3	Q201	Apa sudah dilindungi rekaman penting dari kehilangan, penghancuran, dan pemalsuan sesuai dengan statuta, peraturan perundang-undangan, persyaratan kontrak dan persyaratan bisnis?
A.15.1.4	Q202	Apakah sudah dijamin perlindungan data dan kerahasiaan seperti yang disyaratkan dalam legislasi, regulasi yang relavan dan kontrak jika diperlukan?
A.15.1.5	Q203	Apakah pengguna sudah dicegah dari penggunaan fasilitas pengolahan informasi untuk tujuan yang tidak sah?
A.15.1.6	Q204	Apakah sudah disesuaikan dalam pengendalian kriptografi dengan seluruh perjanjian, undang-undang dan regulasi yang relevan?
A.15.2.1	Q205	Apakah manajer sudah memastikan bahwa seluruh prosedur dalam lingkup tanggungjawabnya dilakukan secara benar untuk mencapai pemenuhan terhadap kebijakan keamanan dan standar?
A.15.2.1	Q206	Apakah sudah di cek secara regular pemenuhan teknis sistem informasi terhadap standar penerapan keamanan?
A.15.3.1	Q207	Apakah sudah direncanakan secara hati-hati dan disetujui dalam persyaratan audit dan kegiatan yang melibatkan pengecekan pada sistem operasional?
	Q208	Apakah sudah diterapkan rencana tersebut guna untuk meminimalisir resiko dari gangguan terhadap proses bisnis?

A.15.3.2	Q209	Apakah sudah ada perlindungan terhadap akses alat audit sistem informasi untuk mencegah setiap kemungkinan penyalahgunaan atau gangguna?

Tabel 4.3 *Statement Of Applicability* (SOA)

A.5 Kebijakan Keamanan		
ISO/IEC 27001:2005	**Applicable**	**Exclusion Statement**
A.5.1.1 Dokumen Kebijakan Keamanan Informasi	D	Kebijakan keamanan informasi tetap menggunakan kebijakan keamanan informasi yang masih berlaku
A.5.1.2 Kajian Kebijakan Keamanan Informasi	D	Tetap disesuaikan, dikomunikasikan dan ditinjau ulang kebijakan keamanan inofrmasi apabila terjadi perubahan kebijakan
A.6 Organisasi Keamanan Informasi		
ISO/IEC 27001:2005	**Applicable**	**Exclusion Statement**
A.6.1.1 Komitmen manajemen keamanan informasi dalam organisasi	D	Manajemen harus mendukung secara aktif keamanan dalam organisasi dengan arahan yang jelas, komitmen nyata, penugasan eksplisit dan tanggung jawab atas keamanan informasi
A.6.1.2 Koordinasi keamanan informasi	D	Kegiatan keamanan informasi harus dikoordinaksikan oleh wakil-wakil dari bagian organisasi yang sesuai dengan peran dan fungsi kerjanya masing-masing
A.6.1.3 Alokasi tanggung jawab keamanan informasi	D	Seluruh tanggung jawab keamanan informasi harus ditetapkan dengan jelas
A.6.1.4 Proses otorisasi unttuk fasilitas pengolahan infromasi	D	Proses otorisasi manajemen untuk fasilitas pengolahan informasi terkini harus ditetapkan dengan jelas
A.6.1.5 Perjanjian kerahasiaan	D	Persyaratan perjanjian kerahasiaan atau *non-disclosure* yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi dan dikaji secara regular
A.6.1.6 kontak dengan pihak berwenang	MD	Kontak dengan pihak berwenang yang relevan belum dipelihara
A.6.1.7 Kontak denan kelompok khusus	D	Kontak dengan kelompok khusus atau forum ahli keamanan dan asosiasi profesi harus dipelihara
A.6.1.8 kajian independen terhadap keamanan informasi	D	Pendekatan organisasi keamanan infromasi dan penerapannya (yaitu sasaran pengendalian, proses dan prosedur untuk keamanan informasi) harus dikaji secara interval terencana, atau ketika terjadi perubahan signifikan terhadap penerapan keamanan.

A.6.2.1Identifikasi resiko terkait pihak eksternal	D	Resiko terhadap informasi organisasi dan fasilitas pengolahan informasi dari proses bisnis yang melibatkan pihak-pihak eksternal harus diidentifikasi dan pengendalian yang sesuai dilaksanakan sebelum pemberian akses
A.6.2.2 penekanan keamanan ketika berhubungan dengan pelanggan	D	Seluruh persyaratan keamanan yang diidentifikasi harus ditekankan sebelum memberikan akses keapada pelanggan terhadap informasi atau aset infromasi
A.6.2.3 penekanan keamanan perjanjian dengan pihak ketiga	D	Perjanjian pihak ketiga yang meliputi pengaksesan, pengolahan ingormasi organisasi atau fasilitass pengolahan informasi, atau penambahan produk atau jasa ke dalam fasilitas pengolahan informasi harus mencakup seluruh persyaratan
A.7 Pengelolaan Aset		
ISO/IEC 27001:2005	**Applicable**	**Exclusion Statement**
A.7.1.1 Inventaris Aset	MD	Semua aset inventaris belum sepenuhnya diidentifikasi dengan jelas dan inventaris dari semua aset penting belum dicatat dan dipelihara
A.7.1.2 Kepemilikan Aset	D	Semua informasi dan aset yang terkait dengan fasilitas pengolahan informasi harus “dimiliki” oleh bagian dari organisasi
A.7.1.3 Penggunaan Aset yang dapat diterima	D	Aturan untuk penggunaan informasi dan aset yang dapat diterima terkait dengan fasilitas pengolahan infromasi harus diidentifikasi didokumentasikan dan diterapkan
A.7.2.1 Pedoman Klasifikasi	D	Informasi haris diklasifikasikan sesuai dengan nilai, persyaratan hukum, sensitivitas dan tingkat kritisnya terhadap organisasi
A.7.2.2 Pelabelan dan Penanganan Informasi	NA	Sekumpulan prosedur yang memadai untuk pelabelan dan penanganan informasi belum dikembangkan dan diterapkan menurut skema klasifikasi yang diadopsi oleh organisasi
A.8 Keamanan Sumber Daya Manusia		
SO/IEC 27001:2005	**Applicable**	**Exclusion Statement**

A.8.1.1 peran dan tanggung jawab	D	Peran dan tanggung jawab dari pegawai, kontraktor dan pengguna pihak ketiga terhadap keamanan harus ditetapkan dan didokumentasikan sesuai dengan kebijakan keamanan informasi organisai
A.8.1.2 penyaringan	D	Verfikasi latar belakang terhadap semua calon pegawai, kontraktor dan pengguna pihak ketiga harus dilaksanakan menurut hukum da undang-undang serta etika yang berlaku dan proporsional terhadap persyaratan bisnis, klasifikasi informasi yang diakseses dan resiko dipersepsikan
A.8.1.3 syarat dan aturan kepegawaian	D	Sebagai bagian dari kewajiban kontrak, pegawai, kontaktor dan pengguna pihak ketiga harus meny syarat dan aturan kontak kepegawaian yang harus menyatakan tanggung jawab
A.8.2.1 tanggung jawab manajemen	D	Manajemen harus mensyaratkan pegawai, kontraktor dan pengguna pihak ketiga untuk menerapkan keamanan menurut kebijakan dan prosedur organisasi yang ditetapkan
A.8.2.2 keedulian, endidikan dan elatihan keamanan informasi	D	Semua pegawaiorgnisasi, kontraktor dan pengguna piak ketiga harus menerima pelatihan kepedulian dan kebijakan Serta prosedur organisasi yang mutakhir secara regular yang sesuai
A.8.2.3 proses pendisiplinan	D	Harus ada proses pendisiplinan yang resmi untuk pegawai yang melakukan pelanggaran keamanan
A.8.3.1 tanggung jawab pengakhiran pekerjaan	D	Tanggung jawab untuk melaksanakan pengakhiran pekerjaan atau perubahan pekerjaan harus ditetapkan dan diberikan dengan jelas
A.8.3.2 pengembalian aset	D	Sesuai pegawai, ontraktor dan pengguna pihak ketiga harus mengembalikan aset organisasi yang digunakannya ketika pekerjaan, kontrak atau perjanjian berakhir
A.8.3.3 penghapusan hak akses	D	Hak akses semua pegawai, kontraktor dan pengguna pihak ketiga terhadap informasi dan fasilitas pengolahan nformasi harus dihapuskan ketika pekerjaan, kontrak atau perjanjian berakhir
A.9 Keamanan Fisik dan Lingkungan		
ISO/IEC 27001:2005	**Applicable**	**Exlusion Statement**

A.9.1.1 Parimeter Keamanan Fisik	RD	Parameter keamanan (batasan seperti dinding, pintu masuk yang dikendalikan dengan kartu atau meja resepsionis yang dijaga) perlu di implementasikan guna untuk melindungi area yang berisi informasi dan fasilitas pengolahan informasi
A.9.1.2 Pengendalian Entri yang Bersifat Fisik	D	Pengawasan terhadap orang-orang dari pihak luar dan membatasi akses terhadap fasilitas informasi
A.9.1.3 Mengamankan Kantor, Ruangan dan Fasilitas	D	Keamanan fisik untuk kantor, ruangan dan fasilitas sudah dirancang dan diterapkan
A.9.1.4 Perlindungan terhadap Ancaman Eksternal dan Lingkungan	D	Perlindungan fisik terhadap kerusakan akibat dari kebakaran, banjir, gempa bumi, ledakan, kerusuhan dan bentuk lain bencana alam atau buatan manusia sudah diterapkan.
A.9.1.5 Bekerja di Area yang Aman	D	Perlindungan fisik dan pedoman kerja dalam area yang aman sudah dirancang dan diterapkan
A.9.1.6 Area Akses Publik, dan Bongkar Muat	D	Titik akses seperti area bongkar muat dan titik lainnya dimana orang yang tidak berwenang dapat masuk kedalam lokasi sudah dikendalikan dan dipisahkan dari fasilitas pengolahan informasi untuk mencegah akses yang tidak sah
A.9.2.1 Penempatan dan Perlindungan Peralatan	D	Peralatan telah ditempatkan dan dilindungi untuk mengurangi resiko dari ancaman dan bahaya dukungan da peluang untuk akses oleh pihak yang tidak berwenang
A.9.2.2 Sarana Pendukung	D	Peralatan telah dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan oleh kegagalan sarana pendukung
A.9.2.3 Keamanan Kabel	D	Kabel daya dan telekomunikasi yang membawa data atau jasa informasi pendukung telah dilindungi dari intersepsi atau kerusakan.
A.10 Manajemen Komunikasi dan Operasi		
ISO/IEC 27001:2005	**Applicable**	**Exclusion Statement**
A.10.1.1 Prosedur Operasi Terdokumentasi	D	Prosedur pengoperasian telah didokumentasikan, dipelihara d an tersedia untuk semua pengguna yang memerlukannya.
A.10.1.2 Manajemen Perubahan	D	Perubahan terhadap fasilitas dan sistem pengolahan informasi telah dikendalikan

A.10.1.3 Pemisahan Tugas	D	Tugas dan lingkup tanggung jawab telah dipisahkan untuk mengurangi pleuang bagi modifikasi yang tidak sengaja atau tidak sah atau penyalahgunaan terhadap aset organisasi.
A.10.2.1 Pelayanan Jasa	D	Telah dikendalikan keamanan, definisi jasa dan tingkat layanan yang dicakup dalam perjanjian pelayanan jasa pihak ketiga diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga.
A.10.2.2 Pemantauan dan Pengkajian Jasa Pihak Ketiga	MD	Jasa, laporan dan rekaman yang diberikan oleh pihak ketiga belum sepenuhnya dipntau, dikaji dan diaudit secara regular
A.10.3.1 Manajemen Kapasitas	D	Penggunaan sumber daya belum dipantau dan disesuaikan untuk pemenuhan kapasitas mendatang.
A.10.3.2 Keberterimaan Sistem	D	Kriteria keberterimaan sistem informasi yang baru, *upgrade*, dan versi baru telah ditetapkan dan dilakukan pengujian sistem yang sesuai selama pengembangan dan sebelum diterima.
A.10.5.1 *Back-up* Informasi	MD	Fasilitas *back-up* dan salinan *back-up* harus memadai untuk memullihkan seluruh sistem informasi jika terjadi bencana atau kegagalan serta harus terdokumentasikan
A.10.6.1 Pengendalian Jaringan	D	Jaringan telah dikendalikan dan dikelola secara memadai, guna melindungi dari ancaman dan untuk meelihara keamanan dari sistem dan aplikasi yang menggunakan jaringan, termasuk informasi dalam transit.
A.10.6.2 Keamanan Layanan Jaringan	D	Fitur keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan telah diidentifikasi dan dicakup dalam setiap perjanjian layanan jaringan, baik diberikan secara *in-house* atau dialihdayakan.
A.10.7.1 Manajaemen Media yang dapat dipindahkan	NA	Prosedur manajemen pemindahan media tidak diterapkan dan terdokumentasikan
A.10.7.2 Pemusnahan Media	NA	Media tidak dimusnakan secara aman dan terjain apabila tidak lagi diperlukan dengan menggunakan prosedur formal
A.10.7.3 Prosedur Penanganan Informasi	D	Prosedur penanganan dan penyimpanan informasi telah ditetapkan untuk melindungi informasi dari pengungkapan yang tidak sah atau penyalahgunaan.

A.10.7.4 Keamanan Dokumentasi Sistem	D	Dokumentasi sistem telah dilindungi terhadap akses yang tidak sah
A.10.8.1 Kebijakan dan Prosedur Pertukaran Informasi	RD	prosedur dan dokumentasi dari kebijakan dan pengendalian untuk melindungi pertukaran informasi dengan menggunakan semua jenis fasilitas komunikasi perlu di terapkan
A.10.8.2 Perjanjian Pertukaran	D	Perjanjian telah ditetapkan untuk meningkatkan pertukaran informasi dan perangkat lunak antara organisasi dan pihak eksternal
A.10.8.3 Media Fisik dan Transit	D	Media yang memuat informasi telah dilindungi terhadap akses yang tidak sah, penyalahgunaan atau kerusakan selama transportasi diluar batas fisik
A.10.8.4 Pesan Elektronik	D	Informasi dalam bentuk pesan elektronik telah dilindungi dengan tepat
A.10.10.1 *Log* Audit	D	*Log* Audit yang merekam kegiatan pengguna, pengecualian dan kejadian keamanan informasi telah dihasilkan dan dijaga pada periode yang disetujui untuk membantu investigasi di masa yang akan datang dan pemantauan pengendalian akses
A.10.10.2 Pemantauan Penggunaan Sistem	D	Prosedur untuk pemantauan penggunaan fasilitas pengolahan informasi t elah ditetapkan dan hasil kegiatan pemantauan ditinjau secara regular
A.10.10.3 Perlindungan Informasi *Log*	D	Fasilitas *log* dan informasi *log* telah dilindungi terhadap gangguan dan akses yang tidak sah
A.10.10.4 *Log* Administrator dan Operator	D	Kegiatan administrator sistem dan operator sistem telah dicatat dalam *log*
A.10.10.5 *Log* atas Kesalahan yang terjadi	D	Kesalahan telah dicatat dalam *log* dan dianalisis dan diambil tindakan yang sesuai
A.11 Pengendalian Akses		
ISO/IEC 27001:2005	**Applicable**	**Exclusion Statement**
A.11.1.1 Kebijakan Pengendalian Akses	D	Kebijakan pengendalian akses telah ditetapkan, didokumentasikan dan dikaji berdasarkan persyaratan bisnis dan keamanan untuk akses

A.11.2.1 Pendaftar Pengguna	D	adanya prosedur pendaftaran dan pembatalan pendaftaran pengguna secara formal untuk pemberian dan pencabutan akses terhadap akses terhadap seluruh layanan dan sistem informasi
A.11.2.2 Manajemen Hak Khusus	D	Alokasi penggunaan hak khusus telah dibatasi dan dikendalikan
A.11.2.3 Manajemen *Password* Pengguna	MD	Belum adanya alokasi *password* untuk mengendalikan proses manajemen formal
A.11.2.4 Tinjauan Terhadap Hak Akses Pengguna	D	Manajemen telah meninjau hak akses secara regular dengan menggunakan proses formal
A.11.3.1 Penggunaan *Password*	D	Penggunaan telah disyaratkan untuk mengikuti pedoman pengamanan yang baik dalam pemilihan dan penggunaan *password*
A.11.3.3 Kebijakan *clear desk* dan *clear screen*	MD	Belum adanya kebijakan *clear desk* terhadap kertas dan media penyimpanan yang dapat dipindahkan untuk fasilitas pengolahan informasi
A.11.4.1 kebijakan Penggunaan Layanan Jaringan	D	Pengguna hanya diberikan akses terhadap layanan yang telah diberikan kewenangan penggunaanya secara spesifik
A.11.4.3 Identifikasi Peralatan dalam Jaringan	PNP	Identifikasi peralatan secara otomatis harus dipertimbangkan sebagai cara untuk mengotentikasi koneksi lokasi dan peralatan spsesifik
A.11.4.4 Peralatan terhadap *Remote Diagnotic* dan *Configuration Port*	D	Akses secara fisik dan *logical* terhadap *diagnotic* dan *configuration port* telah dikendalian
A.11.4.5 Segresi dalam Jaringan	D	Pengelompokan terhadap kayanan informasi di dalam jaringan telah disegresikan
A.11.4.7 Pengendalian *Routing* Jaringan	MD	Pengendalian *routing* belum diterapkan ke dalam jaringan untuk memastikan bahwa koneksi komputer dan aliran informasi tidak melanggar kebijakan pengendalian akses dari aplikasi bisnis
A.11.5.1 Prosedur *Log-on* yang Aman	MD	Akses kedalam sistem informasi perlu dikendalikan dengan prosedur *log-on* yang aman

A.11.5.2 Identifikasi dan Otentikasi Pengguna	D	Semua pengguna memiliki identifikasi unik (*user id*) ang hanya digunakan secara personal dan teknik otentikasi yang sesuai telah dipilih untuk membuktikan identitas pengguna
A.11.5.3 Sistem Manajemen *Password*	D	Sistem mengelola *password* telah interaktif dan memastikan kualitas *password*
A.11.5.5 Sesi *Time-Out*	D	Sesi yang aktif dalam jangka waktu tertentu harus ada mode mati
A.11.6.1 Pembatasan Akses Informasi	D	Akses terhadap informasi dan fungsi sistem aplikasi oleh pengguna dan personel pendukung telah dibatasi sesuai dengan kebijakan pengendalian akses yang ditetapkan
A.11.6.2 Isolasi Sistem yang Sensitif	D	Sistem yang sensitif telah memiliki lingkungan koputasi yang diisolasi
A.12 Akuisi, Pengembangan dan Pemeliharaan Sistem Informasi		
ISO/IEC 27001:2005	**Applicable**	**Exclusion Statement**
A.12.1.1 analisis dan spesifikasi persyaratan keamanan	D	Persyaratan bisnis untuk sistem informasi yang baru
A.12.2.1 validasi dan masukan	D	Masukan data ke dalam aplikasi harus divalidasi untuk memastikan bahwa data tersebut benar dan tepat
A.12.2.2 pengendalian pengolahan internal	D	Pengecekan validasi harus digabungkan ke dalam aplikasi untuk mendeteksi setiap kerusakan infromasi karena kesalahan pengolahan atau tindakan yang disengaja
A.12.2.3 integritas pesan	D	Persyaratan untuk memastikan keaslian dan perlindungan integritas pesan dalam aplikasi harus diidentifikasi dan pengendalian yang tepat harus diidentifikasi dan diterapkan
A.12.2.4	D	Keluaran dari data aplikasi harus divalidasi untuk memastikan bahwa pengolahan informasi yang disimpan adalah benar dan tepat
A.12.3.1 kebijakan tentang penggunaan pengendalian kriptografi	D	Kebijakan tentang penggunaan pengendalian kriptografi untuk melindungi informasi harus dikembangkan dan diterapkan

A.12.3.2 manajemen kunci	D	Manajemen kunci harus tersedia untuk mendukung penggunaan teknik kriptografi oleh organisasi
A.12.4.1 pengendalian perangkat lunak yang operasional	D	Harus tersedia prosedur untuk mengendalikan instalasi perangkat lunak pada sistem yang operasional
A.12.4.2 perlindungan data uji sistem	D	Data uji harus dipilih secara hati-hati dan dilindungi serta dikendalikan
A.12.4.3 pengendalian akses terhadap kode sumber program	D	Akses ke kode sumber program harus dibtasi
A.12.5.1 prosedur pengendalian perubahan	D	Penerapan perubahan harus dikendalikan dengan menggunakan prosedur pengendalian perubahan
A.12.5.2 tinjauan teknis dari aplikasi setelah perubahan sistem operasi	D	Bila sistem operasi diubah aplikasi kritis bisnis harus ditinjau dan diuji untuk memastikan tidak ada dampak yang merugikan terhadap organisasi
A.12.5.3 pembatasan atas perubahan terhadap paket prangkat luak	D	Modifikasi pada paket perangkat lunak harus dihindari, dibatasi hanya pada peubahan yang perlu dan seluruh perubahan harus dikendalikan dengan ketat
A.12.5.4 kebocoran infromasi	D	Peluang untuk kebocoran informasi harus dicegah
A.12.5 pengembangan perangkat lunak yang dialihdayakan	D	Pengembagngan perangkat lunak yang dialihdayakan harus disupervisi dan dipantau oleh organisasi
A.12.5.6 pengendalian kerawanan teknis	MD	Informasi tepat waktu tentang kerawanan teknis dari sistem informasi belum digunakan, eksposur organisasi terhadap kerawanan tersebut dievaluasi dan diambil tindakan yang tepat untuk menangani resiko
A.13 Manajemen Insiden Keamanan Informasi		
ISO/IEC 27001:2005	**Applicable**	**Exclusion Statement**
A.13.1.1 pelaporan kejaian keamanan infromasi	D	Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin
A.13.1.2 pelaporan kelemahan keamanan	D	Semua pegawai, kontraktor dan pengguna pihak ketiga dari sistem informasi dan layanan harus disyaratkan untuk mencatat dan melaporkan setiap kelemahan keamanan yang diamati

A.13.2.1 tanggung jawab dan prosedur	D	Tanggung jawab dan prosedur harus dtetapkan utnuk memastikan tanggpan yang cepat dan sesuai terhadap insiden keamanan
A.13.2.2 pembelajran dari insiden keamanan infromasi	D	Harus tersedia mekanisme yang memunginkan jenis, volume dan biaya insiden keamanan informasi diukur dan diantau
A.13.2.3 pengumpulan bukti	D	Apabila tindka lanjut terhadap orang atau organisasi setelah insiden keamanan infromasi melibatkan tindakan hukum, bukti harus dikumpulkan, disimpan dan disajikan dengan bukti yang telah ditetapkan dalam wilayah hukum yang relevan
A.14 Manajemen Keberlanjutan Bisnis (Business Continuity Management)		
ISO/IEC 27001:2005	**Applicable**	**Exclusion Statement**
A.14.1.1 memasukkan keamanan informasi dalam proses manajemen keberlanjutan bisnis	D	Proses yang dikelola harus dikembangkan dan diekihara untuk kebrlanjutan bisnis organisasi secara menyeluruh yang menkankan penggunaan persyaratan keamanan informasi yang dibutuhkan utnuk keberlanjutan bisnis
A.14.1.2 keberlanjutan bisnis dan asessmen resiko	D	Kejadian yang dapat menyebabkan gangguan terhadap proses bisnis harus diidentifikasi, bersamaan dengan kemungkinan dan dampak dari gangguan tersebut konsekuensinya terhadap keamanan
A.14.1.3 pengembangan dan penerapan rencana keberlanjutan termasuk keamanan informasi	D	Rencana harus dikembangkan dan diterapkan untuk peeliharaan atau mengembalkan operasi dan memastikan ketersediaan informasi pada tingkat dan dalam janga waktu yang disyaratkan
A.14.1.4 kerangka kerja perencanaan keberlanjutan bisni	MD	Kerangka kerja tunggal dari rencana keberlanjutan bisnis perlu dipelihara kembali untuk memastikan rencana konsistem dan menekankan persyaratan keamanan informasi dan untuk identifikasi prioritas untuk pengujian dan pemeliharaan
A.14.1.5 pengujian, pemeliharaan dan asesman ulang rencana keberlanjutan bisnis	MD	Rencana keberlanjutan bisnis harus diuji dan dimutakhirkan secara regular untuk memastikan bahwa rencana tersebut telah mutakhir dari efektif

A.15 Kesesuaian		
ISO/IEC 27001:2005	**Applicable**	**Exclusion Statement**
A.15.1.1 identifikasi peraturan hukum yang berlaku	NA	Seluruh statuta peraturan perundang-undangan dan persyaratan kontrak serta pendekatan organisasi untuk memenuhi persyaratan harus ditetapkan secara eksplisit didokumentasikan, dan dijaga pemutakhirannya
A.15.1.2 hak kekayaan intelektual	NA	Prosedur yang harus sesuai diterapkan untuk memastikan denganperaturan hukum, perundang-undangan dan persyaratan kontrak tentang penggunaan materi berkenaan dimana kemungkinan terdapat hak keakayaan intelektual dan penggunaan produk perangkat lunak yang memiliki hak paten
A.15.1.3 perlindungan rekaman organisasi	NA	Rekaman penting tidak dilindungi dari kehilangan, penghancuran dan pemalsuan sesuai dengan statuta praturan perundang-undangan, persyaratan kontrak dan persyaratan bisnis
A.15.1.4 perlindungan data dan rahasia informasi pribadi	D	Perlindungan data dan kerahasiaan harus dijamin seperti yang disyaratkan dalam legislasi, regulasi yang relevan dan klausul kontrak ika diperlukan
A.15.1.5 pencegahan penyalahgunaan fasilitas pengolahan informasi	D	Pengguna harus dicegah dari pengunaan fasilitas pengolahan informasi untuk tujuan yang tidak sah
A.15.1.6 regulasi pengendalian kriptografi	MD	Pengendalian kriptografi perlu digunakan sesuai dengan seluruh perjanjian, undang-undang dan regulasi yang relevan
A.15.2.1 pemenuhan terhadap kebijakan keamanan dan standar	D	Manajer harus memastikan bahwa seluruh prosedur dalam lingkup tanggung jawab dilakukan secara benar untuk mencapai pemenuhan terhadap kebijakan keamanan dan standar
A.15.2.2 pengecekan pemenuhan teknis	D	Sistem informasi harus secara regular di cek pemenuhan teknis terhadap standar penerapan keamanan
A.15.3.1 pegendalian audit sistem informasi	D	Persyaratan audit dan kegiatan yang melibatkan pngecekan pada sistem operasional harus direncanakan secara berhati-hati dan disetujui untuk meminimalisir resiko dari gangguan terhadap proses bisnis

A.15.3.2 perlindungan terhadap alat audit informasi	D	Akses terhadap alat audit sistem infromasi harus dilindungi untuk mencegah setiap kemungkinan penyalahgunaan atau gangguan

Tabel 4.4 *Gap Analysis : Status of ISO 27001 Implementation*

A.5 Kebijakan Keamanan				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**
A.5.1.1 Dokumen Kebijakan Keamanan Informasi	D	Adanya dokumen kebijakan yang telah terdokumentasikan	Kebijakan keamanan informasi tetap menggunakan kebijakan keamanan informasi yang masih berlaku	Meningkatan pemeliharaan dokumen kebijakan yang telah ada dan tetap diberlakukannya kebijakan tersebut
A.5.1.2 Kajian Kebijakan Keamanan Informasi	D	Adanya dokumen yang telah terdokumentasikan	Tetap disesuaikan, dikomunikasikan dan ditinjau ulang kebijakan keamanan inofrmasi apabila terjadi perubahan kebijakan	melakukan peninjauan ulang yang lebih baik ketika terjadi perubahan kebijakan yang berlaku
A.6 Organisasi Keamanan Informasi				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**
A.6.1.1 Komitmen manajemen keamanan informasi dalam organisasi	D	Terdapat dokumen peran dan tanggung jawab sesuai dengan bagian pada uraian tugasnya	Manajemen mendukung secara aktif keamanan dalam organisasi dengan arahan yang jelas, komitmen nyata, penugasan eksplisit dan tanggung jawab atas keamanan informasi	Menerapkan peran dan tanggung jawab sesuai perannya dalam organisasi
A.6.1.2 Koordinasi keamanan informasi	D	Sesuai dengan uraian tugas masing-masing bagian	Kegiatan keamanan informasi dikoordinaksikan oleh wakil-wakil dari bagian organisasi yang sesuai dengan peran dan fungsi kerjanya masing-masing	Mengkoordinasikan wakil-wakil bagian organisasi yang sesui dengan perannya
A.6.1.3 Alokasi tanggung jawab keamanan informasi	D	Sesuai dengan tugas uraian masing-masing bagian	Seluruh tanggung jawab keamanan informasi ditetapkan dengan jelas	Menjaga tanggung jawab terhada keamanan infomasi
A.6.1.4 Proses otorisasi untuk fasilitas pengolahan infromasi	D	Adanya fasilitas yang lengkap untuk pengolahan informasi	Proses otorisasi manajemen untuk fasilitas pengolahan informasi terkini harus ditetapkan dengan jelas	Memanajemen fasilitas pengolahan informasi

A.6.1.5 Perjanjian kerahasiaan	D	Persyaratan perjanjian terdokumentasi	Persyaratan perjanjian kerahasiaan atau *non-disclosure* yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi dan dikaji secara regular	Menetapkan persyaratan perjanjian untuk perlindungan informasi
A.6.1.6 kontak dengan pihak berwenang	MD	Tidak ditemukan dokumentasi atau perjanjian secara tertulis dengan pihak berwenang	Kontak dengan pihak berwenang yang relevan harus dipelihara	Perlu adanya kontak termasuk komunikasi kepada pihak yang berwenang lainnya
A.6.1.7 Kontak denan kelompok khusus	D	Perjanjian dengan pihak ketiga	Kontak dengan kelompok khusus atau forum ahli keamanan dan asosiasi profesi harus dipelihara	Pemeliharaan dengan kelompok khusus atau pihak ketiga
A.6.1.8 kajian independen terhadap keamanan informasi	D	Adanya dokumen prosedur untuk keamanan informasi	Pendekatan organisasi keamanan infromasi dan penerapannya (yaitu sasaran pengendalian, proses dan prosedur untuk keamanan informasi) harus dikaji secara interval terencana, atau ketika terjadi perubahan signifikan terhadap penerapan keamanan.	Mengkaji pendekatan keamanan informasi dan menerapkanya jika terjadi perubahan
A.6.2.1 Identifikasi resiko terkait pihak eksternal	D	Pemeliharaan fasillitas	Resiko terhadap informasi organisasi dan fasilitas pengolahan informasi dari proses bisnis yang melibatkan pihak-pihak eksternal harus diidentifikasi dan pengendalian yang sesuai dilaksanakan sebelum pemberian akses	Mengidentifikasi resiko terhadap informasi dan fasilitas pengolahan
A.6.2.2 penekanan keamanan ketika berhubungan	D	Adanya perjanjian terhadap aset organisasi	Seluruh persyaratan keamanan yang diidentifikasi harus ditekankan sebelum memberikan akses kepada pelanggan	Pemberian hak akses kepada pihak yang berwenang mengakses sistem informasi

dengan pelanggan			terhadap informasi atau aset infromasi	
A.6.2.3 penekanan keamanan perjanjian dengan pihak ketiga	D	Adanya pembatasan hak akses dan pengolahan. Seperti pada mahasiswa, harus menjadi mahasiswa universitas tersebut dulu	Perjanjian pihak ketiga yang meliputi pengaksesan, pengolahan ingormasi organisasi atau fasilitass pengolahan informasi, atau penambahan produk atau jasa ke dalam fasilitas pengolahan informasi harus mencakup seluruh persyaratan	Pembatasan hak akses kepada pihak yang berwenang, agar tidak adanya hak akses yang tidak sah
A.7 Pengelolaan Aset				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**
A.7.1.1 Inventaris Aset	MD	Belum adanya prosedur dan pencatatan inventraris aset	Semua aset harus diidentifikasi dengan jelas dan inventaris dari semua aset penting dicatat dan dipelihara	Perlu adanya prosedur pemeliharan terhadap inventaris aset terkait piranti lunak, aset informasi, aset fisik dan layanan
A.7.1.2 Kepemilikan Aset	D	Menetapkan kepemilikan aset dan penanggung jawab	Semua informasi dan aset yang terkait dengan fasilitas pengolahan informasi harus “dimiliki” oleh bagian dari organisasi	Menetapkan kepemilikan aset informasi terkait fasilitas pengolahan informasi
A.7.1.3 Penggunaan Aset yang dapat diterima	D	Dokumentasi penggunaan aset	Aturan untuk penggunaan informasi dan aset yang dapat diterima terkait dengan fasilitas pengolahan infromasi harus diidentifikasi didokumentasikan dan diterapkan	Mengidentifikasi dan menerapkan penggunaan aset informasi terkait pengolahan informasi
A.7.2.1 Pedoman Klasifikasi	D		Informasi diklasifikasikan sesuai dengan nilai, persyaratan hukum, sensitivitas dan tingkat kritisnya terhadap organisasi	Mengklasifikasikan informasi sesuai dengan persyaratan hukum
A.7.2.2 Pelabelan dan Penanganan Informasi	NA	Tidak diterapkan prosedur pelabelan dan penanganan informasi yang bersifat rahasia	Sekumpulan prosedur yang memadai untuk pelabelan dan penanganan informasi harus dikembangkan dan diterapkan menurut	Perlu diterapkannya prosedur pelabelan terhadap informasi yang bersifat rahasia, guna agar tidak tertukar atau hilang data

			skema klasifikasi yang diadopsi oleh organisasi	
A.8 Keamanan Sumber Daya Manusia				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**
A.8.1.1 peran dan tanggung jawab	D	Terdapat dokumentasi	Peran dan tanggung jawab dari pegawai, kontraktor dan pengguna pihak ketiga terhadap keamanan harus ditetapkan dan didokumentasikan sesuai dengan kebijakan keamanan informasi organisai	Peran dan tanggung jawab pegawai terhadap keamanan informasi perlu di tetapkan dan dokumentasikan
A.8.1.2 penyaringan	D	Persyaratan pegawai sebelum bekerja	Verfikasi latar belakang terhadap semua calon pegawai, kontraktor dan pengguna pihak ketiga harus dilaksanakan menurut hukum da undang-undang serta etika yang berlaku dan proporsional terhadap persyaratan bisnis, klasifikasi informasi yang diakseses dan resiko dipersepsikan	Perlunya verfikasi latar belakang calon pegawai sebelum dipekerjakan sesuai dengan hukum dan undang-undang
A.8.1.3 syarat dan aturan kepegawaian	D	Terdapat dokumen yang telah terdokumentasikan	Sebagai bagian dari kewajiban kontrak, pegawai, kontaktor dan pengguna pihak ketiga harus meny syarat dan aturan kontak kepegawaian yang harus menyatakan tanggung jawab	Menetapkan syarat dan aturan kepegawaian yang menyatakan tanggung jawab
A.8.2.1 tanggung jawab manajemen	D	Persyaratan pegawai	Manajemen harus mensyaratkan pegawai, kontraktor dan pengguna pihak ketiga untuk menerapkan keamanan menurut kebijakan dan prosedur organisasi yang ditetapkan	Menetapkan persyaratan kepada pegawai untuk menerapkan keaanan menurut kebijakan organisasi yang telah ditetapkan
A.8.2.2	D	Adanya dokumen prosedur	Semua pegawai organisasi, kontraktor dan pengguna piak ketiga	Melakukan pelatihan dan sosialisasi terkait kepedulia dan kebijaan organisasi

		kebijakan oganisasi	harus menerima pelatihan kepedulian dan kebijakan Serta prosedur organisasi yang mutakhir secara regular yang sesuai	
A.8.2.3 proses pendisiplinan	D	Pelanggaran terhadap pegawai	Harus ada proses pendisiplinan yang resmi untuk pegawai yang melakukan pelanggaran keamanan	Mendisiplinkan khusus pegawai yag melanggar aturan keamanan informasi
A.8.3.1 tanggung jawab pengakhiran pekerjaan	D	Terdapat dokumentasi kebijakan pengakhiran pekerjaan	Tanggung jawab untuk melaksanakan pengakhiran pekerjaan atau perubahan pekerjaan harus ditetapkan dan diberikan dengan jelas	Tanggung jawab terhadap keputusan pekerjaan yang ditetapkan dengan jelas
A.8.3.2 pengembalian aset	D	Persyaratan pengembalian aset	Sesmua pegawai, kontraktor dan pengguna pihak ketiga harus mengembalikan aset organisasi yang digunakannya ketika pekerjaan, kontrak atau perjanjian berakhir	Menetapkan persyaratan pengembalian aset informasi ketika pekerjaan atau kontrak berakhir
A.8.3.3 penghapusan hak akses	D	Terdapat dokumen, seperti pada simak online pada mahasiswa alumni, meraka tidak bisa melakukan login sebagai mahasiswa	Hak akses semua pegawai, kontraktor dan pengguna pihak ketiga terhadap informasi dan fasilitas pengolahan nformasi harus dihapuskan ketika pekerjaan, kontrak atau perjanjian berakhir	Menghapus hak akses terhadap pihak yang telah berhenti atau perjanjian kontrak berakhir
A.9 Keamanan Fisik dan Lingkungan				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**

A.9.1.1 Parimeter Keamanan Fisik	RD	Pada pintu masuk belum dilengkapi dengan pengamanan menggunakan kartu gesek atau PIN guna untuk meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas.	Parameter keamanan (batasan seperti dinding, pintu masuk yang dikendalikan dengan kartu atau meja resepsionis yang dijaga) harus digunakan untuk melindungi area yang berisi informasi dan fasilitas pengolahan informasi	Perlu pengamanan terhadap pintu masuk agar meminimalisir terjadinya pencurian, keamanan dan kehilangan informasi atau fasilitas lainnya
A.9.1.2 Pengendalian Entri yang Bersifat Fisik	D	Pembatasan hak akses	Pengawasan terhadap orang-orang dari pihak luar dan membatasi akses terhadap fasilitas informasi	Membatasi hak akses terhadap pihak luar terkait fasilitas informasi
A.9.1.3 Mengamankan Kantor, Ruangan dan Fasilitas	D	Terlihat pada kondisi ruangan kantor saat ini	Keamanan fisik untuk kantor, ruangan dan fasilitas sudah dirancang dan diterapkan	Mengamankan dan enjaga ruangan serta fasilitas yang terdapat di ruangan kerja
A.9.1.4 Perlindungan terhadap Ancaman Eksternal dan Lingkungan	D	Telah diterapkan	Perlindungan fisik terhadap kerusakan akibat dari kebakaran, banjir, gempa bumi, ledakan, kerusuhan dan bentuk lain bencana alam atau buatan manusia sudah diterapkan.	Melindungi ancaman dari kerusakan terhadap fasilitas informasi
A.9.1.5 Bekerja di Area yang Aman	D	Telah diterapkan	Perlindungan fisik dan pedoman kerja dalam area yang aman sudah dirancang dan diterapkan	Melindungi area kerja yang aman
A.9.1.6 Area Akses Publik, dan Bongkar Muat	D	Terlihat dari ruangan kerja	Titik akses seperti area bongkar muat dan titik lainnya dimana orang yang tidak berwenang dapat masuk kedalam lokasi sudah dikendalikan dan dipisahkan dari fasilitas pengolahan informasi untuk mencegah akses yang tidak sah	Melindungi titik akses terhadap pihak luar yang tidak sah terkait ruangan dan lokasi pengolahan informasi

A.9.2.1 Penempatan dan Perlindungan Peralatan	D	Tata letak penyimpanan fasilitas dalam ruangan	Peralatan telah ditempatkan dan dilindungi untuk mengurangi resiko dari ancaman dan bahaya dukungan da peluang untuk akses oleh pihak yang tidak berwenang	Melindungi peralatan untuk mengurangi resiko dari ancaman akses pihak yang tidak sah
A.9.2.2 Sarana Pendukung	D	Perlindungan seperti pada kabel-kabel	Peralatan telah dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan oleh kegagalan sarana pendukung	Melindungi peralatan dari kegagalan catu daya
A.9.2.3 Keamanan Kabel	D	Perlindungan kabel dari kerusakan	Kabel daya dan telekomunikasi yang membawa data atau jasa informasi pendukung telah dilindungi dari intersepsi atau kerusakan.	Melindungi kabel komunikasi dengan bahan yang kuat dan tidak mudah rusak
A. 10 Manajemen Komunikasi dan Operasi				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**
A.10.1.1 Prosedur Operasi Terdokumentasi	D	Sop pengoperasian sistem informasi	Prosedur pengoperasian telah didokumentasikan, dipelihara dan tersedia untuk semua pengguna yang memerlukannya.	Menerapkan SOP guna memudahkan pengoperasian sistem informasi
A.10.1.2 Manajemen Perubahan	D	Pengendalian perubahan fasilitas dan olah sistem	Perubahan terhadap fasilitas dan sistem pengolahan informasi telah dikendalikan	Mengendalikan failitas pengolahan sistem informasi jika terjadi perubahan
A.10.1.3 Pemisahan Tugas	D	Terdapat dokumen untuk pemisahan tugas sesuai dengan fungsi masing-masing	Tugas dan lingkup tanggung jawab telah dipisahkan untuk mengurangi peluang bagi modifikasi yang tidak sengaja atau tidak sah atau penyalahgunaan terhadap aset organisasi.	Memanajemen tugas dan tanggung jawab yang sesuai agar terhindar dari penyalahgunaan aset organisasi
A.10.2.1 Pelayanan Jasa	D	Perjanjian terhadap pihak ketiga	Telah dikendalikan keamanan, definisi jasa dan tingkat layanan yang dicakup dalam perjanjian pelayanan	Mengendalikan dan memelihara perjanjian terhadap pihak ketiga dalam hal pelayanan

			jasa pihak ketiga diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga.	
A.10.2.2 Pemantauan dan Pengkajian Jasa Pihak Ketiga	MD	Laporan dan rekaman yang diberian oleh pihak ketiga belum dipantau, dikaji dan diaudit secara regular	Jasa, laporan dan rekaman yang diberikan oleh pihak ketiga harus dipntau, dikaji dan diaudit secara regular	Perlu adanya laporan dan rekaman dari phak ketiga atau vendor agar bisa melihat apa-apa saja yang telah dipantau
A.10.3.1 Manajemen Kapasitas	MD	Masih dalam proses perencanaan	Penggunaan sumber daya belum dipantau dan disesuaikan untuk pemenuhan kapasitas mendatang. Untuk saat ini masih belum ditargetkan penyesuaiannya fleksibel	Memantau dan menyesuaikan pemenuhan kapasitas mendatang terhadap sistem informasi
A.10.3.2 Keberterima an Sistem	D	Pengujian sistem yang baru	Kriteria keberterimaan sistem informasi yang baru, *upgrade*, dan versi baru telah ditetapkan dan dilakukan pengujian sistem yang sesuai selama pengembangan dan sebelum diterima.	Melakukan pengujian terhadap sistem yang baru atau pengembangan sistem sebelum diterima
A.10.5.1 *Back-up* Informasi	MD	Masih dalam proses	Fasilitas *back-up* dan salinan *back-up* harus memadai untuk memullihkan seluruh sistem informasi jika terjadi bencana atau kegagalan serta harus terdokumentasikan	Perlu menyediakan fasilitas untuk salinan back up untuk meminimalisir terjadinya kehilangan data secara permanen jika ada salinan data ditempat lain
A.10.6.1 Pengendalia n Jaringa	D	Pengendalian jaringan dalam	Jaringan telah dikendalikan dan dikelola secara memadai, guna melindungi dari ancaman dan untuk memelihara keamanan dari sistem dan aplikasi yang menggunakan jaringan, termasuk informasi dalam transit.	Melindungi jaringan dari ancaman dan memelihara keamanan dari sistem dan aplikasi jaringan

A.10.6.2 Keamanan Layanan Jaringan	D	Terhubung dengan vendor	Fitur keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan telah diidentifikasi dan dicakup dalam setiap perjanjian layanan jaringan, baik diberikan secara *in-house* atau dialihdayakan.	Menetapkan persyaratan layanan jaringan dan perjanjian layanan jaringan
A.10.7.1 Manajaemen Media yang dapat dipindahkan	NA	Tidak ada prosedur pemindahan media	Prosedur manajemen pemindahan media harus diterapkan dan terdokumentasikan	Harus diterapkannya pemindahan media
A.10.7.2 Pemusnahan Media	NA	Tindakan pemusnahan media belum diterapkan dan terdokumentasikan	Media harus dimusnakan secara aman dan terjain apabila tidak lagi diperlukan dengan menggunakan prosedur formal	Pemusnahan media perlu diterapkan guna untuk meminimalisir media yang tidak digunakan
A.10.7.3 Prosedur Penanganan Informasi	D	Penanganan informasi dari pengungkapan yang tidak sah	Prosedur penanganan dan penyimpanan informasi telah ditetapkan untuk melindungi informasi dari pengungkapan yang tidak sah atau penyalahgunaan.	Menangani dan melindungi informasi dari pengungkapan yang ridak sah
A.10.7.4 Keamanan Dokumentasi Sistem	D		Dokumentasi sistem telah dilindungi terhadap akses yang tidak sah	Melindungi sistem dari akses yang tidak sah
A.10.8.1 Kebijakan dan Prosedur Pertukaran Informasi	RD	Belum adanya dokumentasi kebijakan pengendalian pertukaran informasi	prosedur dan dokumentasi dari kebijakan dan pengendalian untuk melindungi pertukaran informasi dengan menggunakan semua jenis fasilitas komunikasi	Perlu diterapkan prosedur kebijakan dalam penggunaan fasilitas agar tidak sembarangan pihak dapat menggunakan fasilits tersebut
A.10.8.2 Perjanjian Pertukaran	D	Perjanjian pertukaran informasi dan perangkat lunak	Perjanjian telah ditetapkan untuk meningkatkan pertukaran informasi dan perangkat lunak antara organisasi dan pihak eksternal	Menetapkan perjanjian guna meningkatkan pertukaran informasi daan perangkat lunak

A.10.8.3 Media Fisik dan Transit	D	Penanganan media yang memuat informasi dilindungi dari akses yang tidak sah	Media yang memuat informasi telah dilindungi terhadap akses yang tidak sah, penyalahgunaan atau kerusakan selama transportasi diluar batas fisik	Menangani media yang memuat informasi terhadap akses yang tidak sah atau kerusakan selama transportasi
A.10.8.4 Pesan Elektronik	D	Informasi dalam bentuk pesan elektronik seperti sms	Informasi dalam bentuk pesan elektronik telah dilindungi dengan tepat	Menangani informasi dalam bentuk pesan elektronik haru dilindungi dengan tepat
A.10.10.1 *Log* Audit	D	Perekaman kegiatan pengguna pada log audit	*Log* Audit yang merekam kegiatan pengguna, pengecualian dan kejadian keamanan informasi telah dihasilkan dan dijaga pada periode yang disetujui untuk membantu investigasi di masa yang akan datang dan pemantauan pengendalian akses	Melindungi semua aktifitas pengguna yang dijaga untuk membantu investigasi di masa datang
A.10.10.2 Pemantauan Penggunaan Sistem	D	Adanya prosedur pemantauan dan penggunaan infromasi	Prosedur untuk pemantauan penggunaan fasilitas pengolahan informasi t elah ditetapkan dan hasil kegiatan pemantauan ditinjau secara regular	Memantau penggunaan fasilitas seperti adanya CCTV yng mmantau aktifitas pengguna dalam ruangan
A.10.10.3 Perlindungan Informasi *Log*	D		Fasilitas *log* dan informasi *log* telah dilindungi terhadap gangguan dan akses yang tidak sah	Melindungi hak akses yang tidak sah dengan fasilitas log dan infromasi log
A.10.10.4 *Log* Administrator dan Operator	D	Pencatatan dalam log admin dan operator	Kegiatan administrator sistem dan operator sistem telah dicatat dalam *log*	Mencatat kegiatan admin dan operator dalam log
A.10.10.5 *Log* atas Kesalahan yang terjadi	D		Kesalahan telah dicatat dalam *log* dan dianalisis dan diambil tindakan yang sesuai	Mengambil tindakan ketika terjadi kesalahan pencatatan dalam log
A.11 Pengendalian Akses				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**
A.11.1.1 Kebijakan	D	Adanya kebijakan yang	Kebijakan pengendalian akses	Mendokumentasikan dan mengkaji

Pengendalian Akses		telah terdokumentsikan	telah ditetapkan, didokumentasikan dan dikaji berdasarkan persyaratan bisnis dan keamanan untuk akses	persyaratan kebijakanpengendalian akses
A.11.2.1 Pendaftar Pengguna	D	Terdapat prosedur pendaftaran	adanya prosedur pendaftaran dan pembatalan pendaftaran pengguna secara formal untuk pemberian dan pencabutan akses terhadap akses terhadap seluruh layanan dan sistem informasi	Perlu adanya Sop pendaftaran dan pembatalan hak akses
A.11.2.2 Manajemen Hak Khusus	D	Manajamenen hak khusus	Alokasi penggunaan hak khusus telah dibatasi dan dikendalikan	Mengendalikan alokasi hak khusus
A.11.2.3 Manajemen *Password* Pengguna	MD	Masih dalam perencanaan	Harus adanya alokasi *password* untuk mengendalikan proses manajemen formal	Perlu adanya alokasi khusus password
A.11.2.4 Tinjauan Terhadap Hak Akses Pengguna	D	Meninjau hak akses	Manajemen telah meninjau hak akses secara regular dengan menggunakan proses formal	Memanajemen hak akses
A.11.3.1 Penggunaan *Password*	D	Ada pedoman dalam sistem informasi itu sendiri	Penggunaan telah disyaratkan untuk mengikuti pedoman pengamanan yang baik dalam pemilihan dan penggunaan *password*	Menetapkan persaratan dalam pemilihan password
A.11.3.3 Kebijakan *clear desk* dan *clear screen*	MD	Masih dalam proses	Harus adanya kebijakan *clear desk* terhadap kertas dan media penyimpanan yang dapat dipindahkan untuk fasilitas pengolahan informasi	Perlu adanya kebijakan clear desk dan media penyimpanan untuk pemindahan fasilitas pengolahan informasi
A.11.4.1 kebijakan Penggunaan Layanan Jaringan	D	Terdapat pada sistem informasi	Pengguna hanya diberikan akses terhadap layanan yang telah diberikan kewenangan penggunaanya secara spesifik	Memberikan layanan terhadap pihak yang berwenang sescara spesifik

A.11.4.3 Identifikasi Peralatan dalam Jaringan	PNP		Identifikasi peralatan secara otomatis harus dipertimbangkan sebagai cara untuk mengotentikasi koneksi lokasi dan peralatan spsesifik	Perlu identifikasi peralatan secara otomatis dalam mendeteksi koneksi lokasi dan peralatan
A.11.4.4 Peralatan terhadap *Remote Diagnotic* dan *Configuration Port*	D	Pengendalian terhadap configuration port	Akses secara fisik dan *logical* terhadap *diagnotic* dan *configuration port* telah dikendalian	Mengendalikan akses fisik dan ogical terhadap diagnotic dan konfigurasi port
A.11.4.5 Segresi dalam Jaringan	D	Pengelompokan layanan informasi	Pengelompokan terhadap kayanan informasi di dalam jaringan telah disegresikan	Mengelompokkan layanan informasi dalam jaringa
A.11.4.7 Pengendalian *Routing* Jaringan	MD	Belum adanya pengendalian	Pengendalian *routing t*elah diterapkan ke dalam jaringan untuk memastikan bahwa koneksi komputer dan aliran informasi tidak melanggar kebijakan pengendalian akses dari aplikasi bisnis	Perlu disediadakannya pengendalian terhadap routing terhadap jaringan agar tidak melanggar kebijakan akses dari aplikasi bisnis
A.11.5.1 Prosedur *Log-on* yang Aman	MD	Belum adanya prosedur	Akses kedalam sistem informasi harus dikendalikan dengan prosedur *log-on* yang aman	Perlu adanya prosedur log on yang aman
A.11.5.2 Identifikasi dan Otentikasi Pengguna	D	Pengguna memiliki user id	Semua pengguna memiliki identifikasi unik (*user id*) yang hanya digunakan secara personal dan teknik otentikasi yang sesuai telah dipilih untuk membuktikan identitas pengguna	Pengguna harus memiliki user id yang hanya bisa digunakan secara personal untuk identitas pengguna
A.11.5.3 Sistem Manajemen *Password*	D	Telah terdeteksi di sistem infromasi terkait	Sistem mengelola *password* telah interaktif dan memastikan kualitas *password*	Memilih password yang berkualitas guna meminimalisir terjadinya pengguna lain mudah mengenali password kita
A.11.5.5 Sesi *Time-Out*	D	Terlihat pada sistem informasi	Sesi yang aktif dalam jangka waktu tertentu harus ada mode mati	Menerapkan sesi time out pada sistem informasi

A.11.6.1 Pembatasan Akses Informasi	D	Pembatasan kebijakan pengendalian akses pada sistem informasi	Akses terhadap informasi dan fungsi sistem aplikasi oleh pengguna dan personel pendukung telah dibatasi sesuai dengan kebijakan pengendalian akses yang ditetapkan	Membatasi pengguna yang memiliki hak akses
A.11.6.2 Isolasi Sistem yang Sensitif	D	Terlihat pada lingkungan ruangan	Sistem yang sensitif telah memiliki lingkungan koputasi yang diisolasi	Memiliki ruangan lingkungan koputasi yang diisolasi
A. 12 Akuisi, pengembangan dan pemeliharaan sistem informasi				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**
A.12.1.1 analisis dan spesifikasi persyaratan keamanan	D	Adanya persyaratan terhadap bisni untuk SI	Persyaratan bisnis untuk sistem informasi yang baru	Menetapkan persyaratan bisnis terhadap sistem infromasi yang baru
A.12.2.1 validasi dan masukan	D	Terdapat SOP merespon keslahan masukan validasi data	Masukan data ke dalam aplikasi harus divalidasi untuk memastikan bahwa data tersebut benar dan tepat	Memvalidasi masukan data pada aplikasi dengan benar dan tepat
A.12.2.2 pengendalian pengolahan internal	D	Terlihat pada sistem infromasi	Pengecekan validasi harus digabungkan ke dalam aplikasi untuk mendeteksi setiap kerusakan infromasi karena kesalahan pengolahan atau tindakan yang disengaja	Mengecek validasi yang digabungkan ke dalam aplikasi
A.12.2.3 integritas pesan	D	Adanya persyaratan perlindungan integritas pesan	Persyaratan untuk memastikan keaslian dan perlindungan integritas pesan dalam aplikasi harus diidentifikasi dan pengendalian yang tepat harus diidentifikasi dan diterapkan	Mensyaratkan dan memastikan perlindungan integritas pesan dalam aplikasi
A.12.2.4	D	Terdapat pada sistem informasi	Keluaran dari data aplikasi harus divalidasi untuk memastikan bahwa pengolahan informasi yang disimpan adalah benar dan tepat	Validasi keluaran data untuk memastikan pengolahan informasi yang benar dan tepat

A.12.3.1 kebijakan tentang penggunaan pengendalian kriptografi	D	Terdapat pada sistem informasi	Kebijakan tentang penggunaan pengendalian kriptografi untuk melindungi informasi harus dikembangkan dan diterapkan	Menrapkan kriptografi pada sistem informasi
A.12.3.2 manajemen kunci	D		Manajemen kunci harus tersedia untuk mendukung penggunaan teknik kriptografi oleh organisasi	Memanajemen kunci untuk mendukung penggunaan teknik kriptografi
A.12.4.1 pengendalian perangkat lunak yang operasional	D	Terdapat prosedur instalasi sistem operasi	Harus tersedia prosedur untuk mengendalikan instalasi perangkat lunak pada sistem yang operasional	Menyediakan prosedur instalasi perangkat lunak
A.12.4.2 perlindungan data uji sistem	D	Dilakukan dengan hati-hati dalam melndungi data	Data uji harus dipilih secara hati-hati dan dilindungi serta dikendalikan	Memilih data uji secara hati-hati
A.12.4.3 pengendalian akses terhadap kode sumber program	D	Pembatasan akses ke kode sumber program	Akses ke kode sumber program harus dibtasi	Membatasi akses ke kode sumber program
A.12.5.1 prosedur pengendalian perubahan	D	Prosedur peruban dalam sistem	Penerapan perubahan harus dikendalikan dengan menggunakan prosedur pengendalian perubahan	Sudah ada prosedur namun belum terdokumentasi, perlu didokumentasikan prosedur tersebut, guna untuk pengendalian
A.12.5.2 tinjauan teknis dari aplikasi setelah perubahan sistem operasi	D	Peninjauan dan pengujian sistem operasi yang diubah	Bila sistem operasi diubah aplikasi kritis bisnis harus ditinjau dan diuji untuk memastikan tidak ada dampak yang merugikan terhadap organisasi	Meninjau dan menguji sistem infromasi yang diubah aplikasi kritis dan memastikan tidak ada dampak yang merugikan
A.12.5.3 pembatasan atas perubahan terhadap paket prangkat luak	D		Modifikasi pada paket perangkat lunak harus dihindari, dibatasi hanya pada peubahan yang perlu dan seluruh perubahan harus dikendalikan dengan ketat	Mengendalikan modifiasi perangkat lunak dan membatasi pada perubahan yang perlu saja
A.12.5.4 kebocoran infromasi	D	Pencegahan terhadap kebocoran	Peluang untuk kebocoran informasi harus dicegah	Mencegah peluangan adanya kebocoran data

		telah diterapkan		
A.12.5 pengembangan perangkat lunak yang dialihdayakan	D	Pemantauan pengembangan perangkat lunak	Pengembagngan perangkat lunak yang dialihdayakan harus disupervisi dan dipantau oleh organisasi	Memantau pengembangan perangkatt lunak yang dialihdayakan
A.12.5.6 pengendalian kerawanan teknis	MD	Belum adanya informasi tepat waktu terhada terjadinya kerawanan teknis	Informasi tepat waktu tentang kerawanan teknis dari sistem infromasi harus digunakan haru diperoleh, eksposur organisasi terhadap kerawanan tersebut dievaluasi dan diambil tindakan yang tepat untuk menangani resiko	Perlu dievaluasi kerawanan terhadap teknis guna meminimalisir resiko yang akan datang
A.13 Manajemen Insiden Keamanan Informasi				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**
A.13.1.1 pelaporan kejaian keamanan infromasi	D	Adanya pelaporan	Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin	Mealporkan jika terjadi kejadian keamanan informai yan tidak tepat
A.13.1.2 pelaporan kelemahan keamanan	D	Terlihat pada uraian tugas BPT	Semua pegawai, kontraktor dan pengguna pihak ketiga dari sistem informasi dan layanan harus disyaratkan untuk mencatat dan melaporkan setiap kelemahan keamanan yang diamati	Mencatat dan meaporkan kelemahan keamanan yang diamati
A.13.2.1 tanggung jawab dan prosedur	D	Adanya dokumen prosedur	Tanggung jawab dan prosedur harus dtetapkan utnuk memastikan tanggpan yang cepat dan sesuai terhadap insiden keamanan	Menetapkan tanggung jawab terhadap insisden keamanan
A.13.2.2 pembelajran dari insiden keamanan infromasi	D		Harus tersedia mekanisme yang memungkinkan jenis, volume dan biaya insiden keamanan informasi diukur dan dipantau	Mekanisme, volume dan biaya insiden harus diukur dan di pantau

A.13.2.3 pengumpula n bukti	D	Menyimpan data bukti tindakan terhadap insiden keamanan	Apabila tindka lanjut terhadap orang atau organisasi setelah insiden keamanan informasi melibatkan tindakan hukum, bukti harus dikumpulkan, disimpan dan disajikan dengan bukti yang telah ditetapkan dalam wilayah hukum yang relevan	Menyimpan data bukti terhadap yang melanggar atau terjadinya insiden keamanan yang melibatkan hukum
A.14 Manajemen Keberlanjutan Bisnis				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**
A.14.1.1 memasukkan keamanan informasi dalam proses manajemen keberlanjuta n bisnis	D	Dalam proses wawancara	Proses yang dikelola harus dikembangkan dan dipelihara untuk keberlanjutan bisnis organisasi secara menyeluruh yang menkankan penggunaan persyaratan keamanan informasi yang dibutuhkan untuk keberlanjutan bisnis	Mengembangkan dan memelihara keberlanjutan bisnis secara menyeluruh
A.14.1.2 keberlanjuta n bisnis dan asessmen resiko	D		Kejadian yang dapat menyebabkan gangguan terhadap proses bisnis harus diidentifikasi, bersamaan dengan kemungkinan dan dampak dari gangguan tersebut konsekuensinya terhadap keamanan	Mengidentifikasi proses bisnis sebelum melanjutkan keberlanjutan bisnis
A.14.1.3 pengembang an dan penerapan rencana keberlanjuta n termasuk keamanan informasi	D	Ketersediaan informasi dalam rencana pengembanga n dan pemeliharaan operasi	Rencana harus dikembangkan dan diterapkan untuk pemeliharaan atau mengembalkan operasi dan memastikan ketersediaan informasi pada tingkat dan dalam janga waktu yang disyaratkan	Mengenbangkan rencana dan menerapkan pemeliharaan operasi dan ketersediaan informasi
A.14.1.4 kerangka kerja	MD	Masih dalam proses	Kerangka kerja tunggal dari rencana	Perlu disediakan kerangka kerja tunggal

perencanaan keberlanjutan bisni			keberlanjutan bisnis harus dipelihara untuk memastikan rencana konsistem dan menekankan persyaratan keamanan informasi dan untuk identifikasi prioritas untuk pengujian dan pemeliharaan	dalam keberlanjutan rencana bisnis
A.14.1.5 pengujian, pemeliharaan dan asesman ulang rencana keberlanjutan bisnis	MD	Masih dalam proses	Rencana keberlanjutan bisnis harus diuji dan dimutakhirkan secara regular untuk memastikan bahwa rencana tersebut telah mutakhir dari efektif	Perlu adanya pengujian dan pemutakhiran terhadap keberlanjutan bisnis sebelum dilanjutkan proses bisnis tersebut
A.5 Kesesuaian				
ISO/IEC 27001:2005	**Status**	***Look For***	***Findings***	**Rekomendasi**
A.15.1.1 identifikasi peraturan hukum yang berlaku	NA	Tidak ada statuta, peraturan perundanga-undangan dan persyaratan kontrak	Seluruh statuta peraturan perundang-undangan dan persyaratan kontrak serta pendekatan organisasi untuk memenuhi persyaratan harus ditetapkan secara eksplisit didokumentasikan, dan dijaga pemutakhirannya	Perlu adanya persyaratan prundang-undangan kontrak secara resmi, diterapkan dan dikendalikan
A.15.1.2 hak kekayaan intelektual	NA	Tidak ada prosedur untuk peraturan hukum tentang penggunaan materi berkenaan penggunaan produk	Prosedur yang harus sesuai diterapkan untuk memastikan denganperaturan hukum, perundang-undangan dan persyaratan kontrak tentang penggunaan materi berkenaan dimana kemungkinan terdapat hak keakayaan intelektual dan penggunaan produk perangkat lunak yang memiliki hak paten	Perlu adanya prosedur yang harus diterapkan dalam persyaratan kontrak dalam penggunaan materi, produk perangkat lunak
A.15.1.3 perlindungan	NA	Tidak ada rekaman	Rekaman penting harus dilindungi dari	Harus tersedia rekaman untuk merekan data

rekaman organisasi			kehilangan, penghancuran dan pemalsuan sesuai dengan statuta praturan perundang-undangan, persyaratan kontrak dan persyaratan bisnis	yang penting guna untuk meminimalisir resiko dan ancaman dari luar
A.15.1.4 perlindungan data dan rahasia informasi pribadi	D		Perlindungan data dan kerahasiaan harus dijamin seperti yang disyaratkan dalam legislasi, regulasi yang relevan dan klausul kontrak ika diperlukan	Mensyaratkan dan melindungi kerahasiaan dalam legislasi, regulasi yang relevan
A.15.1.5 pencegahan penyalahgunaan fasilitas pengolahan informasi	D	Pembatasan akses dalam hak penggunaan fasilitas	Pengguna harus dicegah dari pengunaan fasilitas pengolahan informasi untuk tujuan yang tidak sah	Mencegah pengguna fasilitas informasi dengan tujuan yang tidak sah
A.15.1.6 regulasi pengendalian kriptografi	MD	Masih dalam proses	Pengendalian kriptografi harus digunakan sesuai dengan seluruh perjanjian, undang-undang dan regulasi yang relevan	Perlu dikendalikan dengan kriptografi yang sesuai dengan perjanjian
A.15.2.1 pemenuhan terhadap kebijakan keamanan dan standar	D	Seluruh prosedur dalam lingkup dan tanggung jawab yang benar	Manajer harus memastikan bahwa seluruh prosedur dalam lingkup tanggung jawab dilakukan secara benar untuk mencapai pemenuhan terhadap kebijakan keamanan dan standar	Memastikan rosedur dalam lingkup tanggung jawab dilakukan secara benar
A.15.2.2 pengecekan pemenuhan teknis	D		Sistem informasi harus secara regular di cek pemenuhan teknis terhadap standar penerapan keamanan	Mengecek pemenuhan teknis terhadap standar keamanan
A.15.3.1 pegendalian audit sistem informasi	D	Adanya surat penerimaan dan persetujuan	Persyaratan audit dan kegiatan yang melibatkan pengecekan pada sistem operasional harus direncanakan secara berhati-hati dan disetujui untuk meminimalisir resiko dari gangguan	Mensyaratkan audit dan kegiatan yang melibatkan pengecekan pada sistem operasional harus direncanakan secara berhati-hati dan disetujui

			terhadap proses bisnis	
A.15.3.2 perlindungan terhadap alat audit informasi	D		Akses terhadap alat audit sistem infromasi harus dilindungi untuk mencegah setiap kemungkinan penyalahgunaan atau gangguan	Mencegah Akses terhadap alat audit sistem infromasi dan harus dilindungi

Tabel 4.5 Rekomendasi Kebijakan dan Prosedur Keamanan Informasi

Klausul ISO/IEC 27001:2005	Permasalahan/kondisi saat ini	Rekomendasi
A.5 Kebijakan Keamanan	Kebijakan keamanan informasi telah diterapkan, akan tetapi keamanan informasi belum disosialisasikan dalam bentuk yang relevan, mudah dimengerti dan mudah diakses	Sebaiknya kebijakan keamanan disosialisasikan dalam bentuk yang relevan, mudah dimengerti, dan mudah diakses
A.6 Organisasi Keamanan Informasi	Koordinasi wakil dari organisasi belum disesuaikan dengan perannya dalam kegiatan keamanan informasi, tidak terpeliharanya kontak dengan pihak berwenang dan kontak kelompok khusus atau forum ahli keamanan	a. Koordinasi wakil-wakil dari organisasi yang sesuai dengan perannya dalam kegiatan keamanan informasi b. Perlu dipelihara dengan kontak pihak yang berwenang c. Pemeliharaan kontak dengan kelompok khusus (*special interest*) atau forum ahli keamanan dan asosiasi profesi
A.7 Pengendalian Akses	Pada dokumen inventaris aset belum adanya identifikasi dan pencatatan yang diterapkan, aset informasi dan prosedur pemberian tanda pelabelan serta penanganan informasi yang bersifat rahasia juga belum0020terpelihara dan diterapkan.	a. Identifikasi dan pencatatan untuk dokumentasi inventaris aset (aset informasi, aset piranti lunak, aset fisik dan layanan) b. Pemeliharaan terhadap aset informasi c. Prosedur dan tindakan pemberian tanda pelabelan serta penanganan informasi yang bersifat rahasia atau penting d. Dokumentasi prosedur pelabelan
A.8 Keamanan Sumber Daya Manusia	Calon pegawai belum diverifikasi latar belakangnya yang disesuaikan menurut hukum dan undang-undang yang berlaku dan	a. Verifikasi latar belakang calon pegawai sebelum di pekerjakan dilaksanakan dan disesuaikan menurut

	belum di tetapkan aturan, syarat kontrak calon pegawai, kontraktor dan pihak ketiga	hukum dan undang-undang yang berlaku b. Perlu penetapan aturan dan syarat kontrak calon pegawai, kontraktor dan pihak ketiga sebelum dipekerjakan
A.9 Keamanan Fisik dan Linkungan	Dalam keamanan fisik dan lingkungan terdapat parimeter keamanan yang belum diterapkan pada pintu masuk yang blum dikendalikan dengan PIN atau kartu gesek guna untuk meminimalisir terjadinya pencurian atau kesalahan dalam penggunaan fasilitas pengolahan informasi yang ada	Pintu masuk perlu dikendalikan dengan PIN atau kartu gesek guna untuk meminimalisir terjadinya pencurian atau kesalahan dalam penggunaan fasilitas pengolahan informasi yang ada
A.10 Manajemen Komunikasi dan Operasi	Belum adanya pengkajian ulang dan audit secara regular mengenai jasa, laporan dan rekamanan dari piak ketiga. Sumber daya belum sepenuhnya di pantau untuk pemenuhan kapasitas mendatang. Fasilitas dan prosedur media dan pencatatan belum sepenuhnya diterapkan dan didokumentasikan serta kebijakan dan pengendalian pertukaran informasi belum diadakannya prosedur perlindungan pertukaran informasi	a.Pengkajian ulang dan audit secara regular mengenai jasa, laporan dan rekaman pemantauan dari pihak ketiga b.Pemantauan sumber daya disesuaikan untuk pemenuhan kapasitas mendatang c. Fasilitas media dan pencatatan untuk *back-up* data yang memadai untuk memulihkan sistem jika terjadi kegagalan atau bencana d. Perlu diterapkannya prosedur pemindahan media e. Tindakan untuk pemusnahan media apabila media tersebut tidak lagi digunakan f. Perlu adanya prosedur dalam pemusnahan media g.Dokumen prosedur pemusnahan media h. Prosedur kebijakan dan pengendalian untuk melindungi pertukaran

		informasi dengan semua jenis fasilitas komunikasi i. Dokumentasi prosedur perlindungan pertukaran informasi
A.11 Pengendalian Akses	Alokasi untuk password belum dikendalikan. Kebijakan clear desk, log on belum diterapkan prosedur dan dokumentasinya. Pengendalian routing belum diterapkan ke alam jaringan untuk memastikan koneksi komputer dan aliran informasi tidak melanggar kebijakan pengendalian akses.	a. Alokasi untuk *password* untuk mengendalikan manajemen formal b. Perlu adanya kebijakan *clear desk* terhadap media penyimpanan yang dapat dipindahkan untuk fasilitas pengolahan informasi c. Pengendalian terhadap *routing* yang diterapkan ke dalam jaringan untuk memastikan bahwa koneksi komputer dan aliran infromasi tidak melanggar kebijakan pengendalian akses d. Perlunya prosedur *Log-on* yang aman e. Dokumentasi prosedur *log-on*
A.12 Akuisi, Pengembangan dan Pemeliharaan Sistem Informasi	Belum sepenuhnya diterapkan prosedur pengendalian yang formal terkait perubahan dalam sistem aplikasi, belum dievaluasi informasi yang tepat waktu terkait kerawanan teknis dari SI dan belum adanya tindakan pengambilan dalam menangani resiko terkait kerawanan teknis	a. Perlunya dokumentasi prosedur pengendalian yang formal terkait perubahan dalam sistem aplikasi atau informasi b. Evaluasi informasi tepat waktu terkait kerawanan teknis dari sistem informasi yang digunakan c. Perlu pengambilan tindakan segera dalam menangani resiko terkait kerawanan teknis dari sistem informasi
A.13 Manajemen Kerawanan Teknis	Pada klausul manajemen insiden keamanan informasi kondisi keamanan saat ini dan kondisi ideal berdasarkan ISO/IEC 27001:2005 telah sesuai dengan standar keamanan ISO/IEC 27001:2005	Lebih ditingkatkan kembali dalam tingkatan optmal dalam menangani insiden keamanan informasi
A.14 Manajemen Keberlanjutan Bisnis	tidak adanya kerangka kerja tunggal untuk	Pelu adanya perencanaan pembuatan kerangka kerja

(*Business Continuity Managemen*)	rencana bisnis kedepan, belum adanya pengujian terlebih dahulu terhadap pemutakhiran proses bisnis lebih lanjut	tunggal untuk rencana bisnis IT kedepannya agar keberlanjutan bisnis terencana dan tidak menimbulkan kesalahan serta perlu dilakukan pengujian terlebih dahulu sebelum pemutakhiran proses bisnis lebih lanjut
A.15 Kesesuaian	belum adanya persyaratan perundang-undangan kontrak secara resmi,belum diterapkan persyaratan kontrak dalam penggunaan materi dan produk perangkat lunak, tidak adanya rekaman untuk merekam data penting terkait penghancuran dan pemalsuan kontrak, dan tidak adanya perjanjian pengendalian kriptografi.	a. Perlunya penetapan statuta, peraturan perundang-undangan dan persyaratan kontrak untuk memenuhi persyaratan hukum yang berlaku mengenai keamanan informasi b. Perlu prosedur untuk memastikan kesesuaian denga peraturan perundang-undangan dan persyaratan kontrak terkait penggunaan materi berkenaan produk perangkat lunak yang memiliki hak paten c. Perlu perlindungan rekaman penting dari kehilangan, penghancuran, dan pemalsuan yang sesuai statuta, peraturan perundang-undangan dan persyaratan kontrak dan bisnis d. Perlunya penyesuaian kriptografi sesuai dengan perjanjian, undang-undang dan regulasi yang relevan.

LAMPIRAN III

LAMPIRAN JAWABAN WAWANCARA

Lembar Kertas Kerja Audit

Audit Keamanan Simak Online Universitas Indo Global Mandiri Paembang

Berdasarkan Standard ISO/IEC 27001:2005

Document ID	: INTV- DIM
Project Name	: Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001:2005
Auditor	: Yeni Rahayu
Auditee	: Tasmi, S.Si., M.Kom
Description	: Lembar kertas audit ini merupakan bagian dari penelitian tugas akhir mahasiswa Program Studi Sistem Informasi, Universitas Islam Negeri Raden Fatah Palembang Lembar kertas kerja audit ini digunakan untuk mengetahui tingkat keamanan informasi simak online Universitas Indo Global Mandiri Palembang.
Date	: 01 OKTOBER 2018
Responsible	: Information Security Officer (ISO)

Approved by

(Tasmi, S.Si., M.Kom)

Auditor

(Yeni Rahayu)

PERTANYAAN WAWANCARA

Document ID : INTV-DIM

Klausul A.5 Kebijakan Keamanan

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	Klausul A.5.1.1	Q1	Apakah sudah ada kejakan keamanan informasi?	Ya	
		Q2	Apakah sudah terdokumentasi kebijakan keamanan informasi tersebut?	ya	
		Q3	Apakah dokumen kebijakan tersebut sudah dipublikasikan kepada seua pihak terkait?	ya	
		Q4	Apakah kebijakan tersebut sudah disosialisasikan dalam bentuk yang relevan, mudah diakses, dan dimengerti?	tidak	Belum Sepenuhnya
	Klausul A.5.1.2	Q5	Jika terjadi perubahan kebijakan, apakah kebijakan tersebut tetap disesuaikan dengan kefektifan yang berkelanjutan?	ya	
		Q6	Apakah perubahan kebijakan tersebut akan dikomunikasikan kepada semua pihak?	ya	Sosialisasi terhadap pegawai
		Q7	Apakah ada pernyataan komitmen manajemen serta dukungan terhadap tujuan dan prinsi keamanan informasi?	ya	
		Q8	Apakah semua pegawai telah benar-benar memahami keamanan informasi?	tidak	Belum Seluruhnya mengetahui keamanan informasi

		Q9	Apakah kebijakan keamanan informasi sudah dilakukan tinjauan ulang funa mengantisipasi setiap perubahan yang mempengaruhi analisa resiko, seperti kerawanan?	ya	
		Q10	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal?	tidak	

Klausul A.7 Pengelolaan Aset

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	Klausul A.7.1.1	Q11	Apakah semua inventaris aset (aset informasi, aset piranti lunak, aset fisik dan layanan) sudah diidentifikasi dan dicatat?	tidak	Belum di identifikasi
		Q12	Masing-masing aset apakah sudah disusun dan dipelihara?	tidak	Ada, hanya' saja belum seluruhnya disusun
		Q13	Apakah sudah ada kebijakan pengelolaan inventaris aset?	ya	
		Q14	Apakah klasifikasi lokasi keamanan aset sudah didokumentasikan (sebagai catatan jika terjadi kehilangan dan kerugian)?	ya	
	Klausul A.7.1.2	Q15	Apakah sudah ditentukan pegawai atau sub bagian yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset?	ya	
		Q16	Siapa yanng bertanggung jawab mengontrol dan memelihara terhadap inventaris aset?	ya	Isi Inyan
		Q17	Berapa jangka waktu pengecekan inventaris aset secara berkala?	ya	per bulan.

		Q18	Apakah sudah diidentifikasi tingkat kepentingan aset?	Ya	
	Kalusus A.7.1.3	Q19	Apakah ada aturan-aturan ketika pihak-pihak tertentu menggunakan informasi aset?	Ya	Perakuran tersendiri, hanya pada pihak tertentu Saja
		Q20	Apakah informasi pengelolaan aset sudah terdokumentasi?	tidak	
		Q21	Seberapa perlunya informasi pengolahan aset didokumentasikan?	Ya	
	Klausul A.7.2.1	Q22	Apakah informasi aset di klasifikasikan dengan tingkat perlindungan yang tepat?	Ya	
		Q23	Bagaimanakah prosedur pengklasifikasian informasi pengelolaan aset tersebut?	Ya	Ada prosedur yang ada dalam arsip -
	Klausul A.7.2.2	Q24	Apakah ada satu set prosedur untuk menentukan pemberian tanda pelabelan dan penanganan informasi yang bersifat rahasia atau penting?	tidak	tidak ada label atau tanda
		Q25	Apakah prosedur tersebut sudah mencakup informasi baik secara fisik maupun dalam format elektronik?	tidak	
		Q26	Apakah penanganan informasi dikembangkan dan diterapkan?	Ya	karena sangat perlu dikembangkan guna penanganan keamanan informasi kedepan

PERTANYAAN WAWANCARA

Document ID : INTV-

Klalusul A.6 Organisasi Keamanan Informasi

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	A.6.1.1	Q132	Apakah manajemen terhadap keamanan informasi telah mendukung secara aktif keamanan dalam organisasi dengan arahan yang jelas, komitmen dan penugasan eksplisit?	YA	
		Q133	Manajemen tersebut telah bertanggung jawab atas keamanan informasi?	YA	
	A.6.1.2	Q134	Apakah kegiatan keamanan informasi telah di koordinasi oleh wakil-wakil dari bagian organisasi yang sesuai dengan peran masing-masing?	tidak	terkadang ada yang menangani tidak pada peran tersebut
		Q135	Apakah sudah tedokumentasikan kegiatan kemanan informasi tersebut?	YA	
	A.6.1.3	Q136	Seluruh tanggung jawab keamanan informasi sudah ditetapkan dengan jelas?	YA	
		Q136	Sudah terdokumentasikan kebijakan tersebut?	YA	
	A.6.1.4	Q137	Apakah telah ditetapkan manajemen fasilitas pengolahan informasi teknik?	YA	
		Q138	Apakah sudah terlaksana manajemen pengolahan informasi tersebut?	YA	
	A.6.1.5	Q139	Apakah sudah diidentifikasi persyaratan dan perjanjian kerahasiaan kebutuhan organisasi untuk melindungi informasi?	YA	Ada peraturan tersendiri untuk organisasi dalam melindungi informasi / ASet

		Q140	Apakah kebijakan persyaratan dan perjanjian kerahasiaan organisasi dalam melindungi informasi telah dikaji secara regular?	YA	
	A.6.1.6	Q141	Kontak dengan pihak berwenang telah terpelihara?	tidak	Belum sepenuhnya
	A.6.1.7	Q142	Apakah telah dilaksanakan dan dipelihara kontak dengan kelompok khusu (*special interest*) tau forum ahli keamanan dan asosiasi profesi?	tidak	Karena terkait / ada kontak dengan Vendor / pihak ketiga belum sepenuhnya terlakna dalam hal keamanan, tetapi terus ditanyan: jika ada kesalahan
	A.6.1.8	Q143	Apakah telah dikaji secara independen pendekatan organisasi untuk mengelola informasi dan penerapannya (sasaran pengendalian, kebijakan, prosedur keamanan infromasi)?	YA	
		Q144	Telah dikaji apabila terjadi perubahan signifikan terhadap terhadap penerapan keamanan?	Y/A	
	A.6.2.1	Q145	Apakah sudah diidentifikasi resiko terhadap informasi organisasi dan fasilitas pengolahan informasi dari proses bisnis yang melibatkan pihak eksternal?	YA	
		Q146	Apakah telah disesuaikan pngendalian terhadap pihak eksternal sebelum pemberian akses?	YA	
	A.6.2.2	Q147	Sudah diidentifikasi persyaratan keamanan yang harus ditekankan sebelum memberikan hak akses kepada pelanggan informasi atau aset organisasi?	YA	
	A.6.2.3	Q148	Apakah sudah ada persyaratan keamanan yang relevan terhadap perjanjian pihak ketiga yang meliputi : pengaksesan, pengloahan, komunikasi atau penambahan roduk jasa kedalam aktifitas pengolahan informasi?	YA	Ada perjanjian pada pihak ketiga atau vendor

Lembar Kertas Kerja Audit

Audit Keamanan Simak Online Universitas Indo Global Mandiri Paembang

Berdasarkan Standard ISO/IEC 27001:2005

Document ID	: INTV-CIO
Project Name	: Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001:2005
Auditor	: Yeni Rahayu
Auditee	: Dr. Herri Setiawan, M.Kom
Description	: Lembar kertas audit ini merupakan bagian dari penelitian tugas akhir mahasiswa Program Studi Sistem Informasi, Universitas Islam Negeri Raden Fatah Palembang Lembar kertas kerja audit ini digunakan untuk mengetahui tingkat keamanan informasi simak online Universitas Indo Global Mandiri Palembang.
Date	: 01 OKTOBER 2018
Responsible	: Director Information Management (DIM)

Approved by

Biro Pelaksana Teknis UGM

(Dr. Herri Setiawan, M.Kom)

Auditor

(Yeni Rahayu)

Document ID : INTV-

Klalusul A.14 Manajemen Keberlanjutan Bisnis (*Business Coninuity Management*)

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	A.14.1.1	Q185	Sudah dikembangkan dan diplihara untuk keberlanjutan bisnis organisasi secara menyeluruh?	ya	
		Q186	Apakah sudah dikembangkan dan dipelihara terkait penggunaan persyaratan keamanan informasi yang dibutuhkan uuntuk keberanjutan bisnis organisasi?	ya	pasti diidentifikasi terlebih dahulu untuk keberlanjutan bisnis kedepannya
	A.14.1.2	Q187	Apakah sudah diidentifikasi kejadian yang dapat menyebabkan gangguan terhadap proses bisnis?	ya	
		Q188	Apa sudah diidentifikasi terhadap kemungkinan dan dampak dari gangguan tersebut serta konsekuennya terhadap keamanan informasi?	ya	
	A.14.1.3	Q189	Apakah sudah diterapkan rencana untuk memelihara atau mengembalikan operasi setelah terjadinya gangguan proses bisnis?	ya	Sangat perlu
		Q190	Apakah sudah dikembangkan rencana untuk memastikan ketersediaan informasi pada tingkat dan dalam jangka waktu yang diisyaratkan setelah terjadi gangguan atau kegagalan proses bisnis?	ya	perangaran setelah terjadi gangguan direncanakan kembali ketersediannya
	A.14.1.4	Q191	Apakah sudah dipelihara kerangka kerja tunggal dari rencana keberlanjutan bisnis untuk memastikan rencana konsisten dan menekankan persyaratan keamanan informasi?	tidak	Belum, karena ada kerjasama dengan Vendor. jadi terima dari vendor
		Q192	Apakah sudah diidentifikasi prioritas untuk pengujian dan pemeliharan kerangka kerja tersebut?	tidak	
	A.14.1.5	Q193	Apa sudah diuji dan dimutakhirkan secara regular tentang rencana keberlanjutan bisnis untuk memastikan rencana tersebut mutakhir dan efektif?	tidak	

Document ID : INTV-

Klalusul A.15 Kesesuaian

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	A.15.1.1	Q196	Apakah sudah ditetapkan statuta, peraturan perundangan-undangan, dan persyaratan kontrak serta pendekatan organisasi untuk memenuhi persyaratan hukum yang berlaku mengenai keamanan informasi?	tidak.	Adanya peraturan, akan tetapi belum sepenuhnya telah sesuai
		Q197	Apakah sudah didokumentasikan pertaturan tersebut?	tidak.	
		Q198	Apakah sudah dijaga pemutakhirannya untuk masing-masing sistem informasi dan organisasi?	ya	
	A.15.1.2	Q199	Apakah sudah ada prosedur untuk memastikan kesesuaian dengan peraturan perundang-undangan dan persyaratan kontrak tentang penggunaan materi yang berkenaan produk perangkat lunak yang memiliki hak paten?	tidak	
		Q200	Apakah sudah diterapkan dan didokumentasikan prosedur tersebut?	ya	
	A.15.1.3	Q201	Apa sudah dilindungi rekaman penting dari kehilangan, penghancuran, dan pemalsuan sesuai dengan statuta, peraturan perundang-undangan, persyaratan kontrak dan persyaratan bisnis?	tidak	Masih dalam proses perencanaan
	A.15.1.4	Q202	Apakah sudah dijamin perlindungan data dan kerahasiaan seperti yang disyaratkan dalam legislasi, regulasi yang relavan dan kontrak jika diperlukan?	ya	
	A.15.1.5	Q203	Apakah pengguna sudah dicegah dari penggunaan fasilitas pengolahan informasi untuk tujuan yang tidak sah?	ya	
	A.15.1.6	Q204	Apakah sudah disesuaikan dalam pengendalian kriptografi dengan seluruh perjanjian, undang-undang dan regulasi yang relevan?	tidak.	

	A.15.2.1	Q205	Apakah manajer sudah memastikan bahwa seluruh prosedur dalam lingkup tanggungjawabnya dilakukan secara benar untuk mencapai pemenuhan terhadap kebijakan keamanan dan standar?	ya	
	A.15.2.1	Q206	Apakah sudah di cek secara regular pemenuhan teknis sistem informasi terhadap standar penerapan keamanan?	ya	Pengecekannya secara berkala
	A.15.3.1	Q207	Apakah sudah direncanakan secara hati-hati dan disetujui dalam persyaratan audit dan kegiatan yang melibatkan pengecekan pada sistem operasional?	ya	Mempersiapkan rencana untuk persyaratan ketika akan dilakukan audit
		Q208	Apakah sudah diterapkan rencana tersebut guna untuk meminimalisir resiko dari gangguan terhadap proses bisnis?	ya	
	A.15.3.2	Q209	Apakah sudah ada perlindungan terhadap akses alat audit sistem informasi untuk mencegah setiap kemungkinan penyalahgunaan atau gangguna?	ya	

PERTANYAAN WAWANCARA

Document ID : INTV-CIO

Klausul A.8 Keamanan Sumber Daya Manusia

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	Klausul A.8.1.1	Q27	Apakah sudah ditetapkan kebijakan keamanan informasi terkait peran dan tanggung jawab dari pegawai, kontraktor dan pengguna pihak ketiga?	YA	
		Q28	Apakah sudah didokumentasikan kebijakan keamanan informasi tersebut?	YA	Ada kebijakan atau persyaratan ketika sebelum dipekerjakan
	Klausul A.8.1.2	Q29	Apakah sudah dilaksanakan menurut hukum dan undang-undang yang berlaku untuk verifikasi latar belakang calon pegawai, kontraktor dan pihak ketiga?	tidak	Masih dalam rencana terkait persyaratan calon
		Q30	Apakah sudah ada kebijakan terhadap akses informasi terhadap pegawai, kontraktor dan pihak ketiga?	YA	Ada prosedurnya
	Klausul A.8.1.3	Q31	Apakah sudah ditetapkan aturan dan syarat kontrak calon pegawai, kontraktor dan pihak ketiga?	tidak	
		Q32	Apakah ketetapan tersebut sudah terdokumentasikan?	YA	
		Q33	Apakah sudah diterapkan persetujuan dan menandatangani kontrak untuk tanggung jawab dan kewajiban sebagai pegawai, kontraktor atau pihak ketiga terhadap keamanan informasi?	YA	
	Klausul A.8.2.1	Q34	Apakah sudah diterapkan kebijakan dan prosedur keamanan informasi kepada pegawai, kontraktor dan pihak ketiga selama bekerja?	YA	Sudah ada prosedurnya

		Q35	Apakah sudah terdokumentasikan kebijakan dan prosedur tersebut?	YA	
	Klausul A.8.2.2	Q36	Apakah ada prosedur dan kebijakan mengenai pelatihan serta pendidikan terlebih dahulu kepada pegawai, kontraktor dan pihak ketiga secara regular sesuai dengan fungsi kerjanya?	YA	Disosralisasikan terlebih dahulu atau pelatihan
		Q37	Apakah prosedur tersebut sudah terdokumentasikan?	YA	
		Q38	Apakah ada kebijakan pendisiplinan ketika pegawai melakukan pelanggaran keamanan?	YA	Setelah dipekerjakan, ada kebijakan pendisiplinan terlebih dahulu
		Q39	Apakah peraturan kebijakan tersebut sudah terdokumentasikan?	YA	
	Klausul A.8.2.3	Q40	Apakah sudah ditetapkan kebijakan dalam pengakhiran atau perubahan pekerjaan terhadap pegawai?	YA	
	Klausul A.8.3.1	Q41	Apakah sudah didokumentasikan kebijakan prosedur tanggung jawab perubahan atau pengakhiran pekerjaan tersebut?	YA	
		Q42	Apakah sudah ditetapkan peraturan atau syarat apabila pegawai, kontraktor, dan pihak ketiga dalam mengembalikan semua aset organisasi yang digunakan apabila perjanjian berakhir?	YA	Ketika Selesai dipekerjakan, Semua fasilitas yang diberi, dikembalikan semua
		Q43	Apakah sudah terdokumentasi peraturan tersebut?	YA	
	Klausul A.8.3.2	Q44	Apakah ada aturan atau persyaratan dalam pengahapusan hak akses apabila pegawai, kontraktor dan pihak ketiga ketika pengakhiran pekerjaan atau perjanjian telah berakhir?	YA	
	Klausul A.8.3.3	Q45	Apakah fasilitas pengolahan informasi dihapuskan ketika pekerjaan kontrak atau perjanjian berakhir?	YA	

Lembar Kertas Kerja Audit

Audit Keamanan Simak Online Universitas Indo Global Mandiri Paembang Berdasarkan Standard ISO/IEC 27001:2005

Document ID	: INTV-ISO-3
Project Name	: Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001:2005
Auditor	: Yeni Rahayu
Auditee	: Reza Maulana, A.Md
Description	: Lembar kertas audit ini merupakan bagian dari penelitian tugas akhir mahasiswa Program Studi Sistem Informasi, Universitas Islam Negeri Raden Fatah Palembang Lembar kertas kerja audit ini digunakan untuk mengetahui tingkat keamanan informasi simak online Universitas Indo Global Mandiri Palembang.
Date	: 01 OKTOBER 2018
Responsible	: Information Security Officer (ISO)

Approved by

(Reza Maulana, A.Md)

Auditor

(Yeni Rahayu)

PERTANYAAN WAWANCARA

Document ID : INTV-ISO

Klausul A.10 Manajemen Komunikasi dan Operasi

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	Klausul A.10.1.1	Q69	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara aman?	Ya	Semua telah didata dan dipelihara
		Q70	Jika ada kesalhan operasi atau kesulitan teknis, apakah akan meminta bantuan pengelola/ pegawai lainnya?	Ya	
		Q71	Apakah (back-up data) sudah dipelihara serta sudah dilakukakan sesuai prosedur?	Ya	
	Klausul A.10.1.2	Q72	Jika ada perubahan terhadap fasilitas dan sistem pengolahan sistem informasi apakah sudah dikontrol dan kendalikan?	Ya	Ada, dan di kendalikan apabila terjadi Perubahan
		Q73	Apakah sudah dilakukan pencataan perubahan dan apakah perubahan tersebut sudah disosialisasikan ke semua pihak?	Ya	Disosialisasikan kepada pihak atau Pegawai ketika terjadi perubahan
	Klausul A.10.1.3	Q74	Apakah pegawai di ruang BPT sudah dipisahkan menurut tugas dan tanggung jawab masing-masing?	Ya	Ada uraian tugasnya sendiri.
		Q75	Apakah ada pemantauan dan pengawasan untuk mengurangi resiko insiden memodifikasi tanpa ijin atau penyalahgunaan sistem?	Ya	
	Klausul A.10.2.1	Q76	Apakah tingkat layanan yang dicakup dalam perjanjian pelayananan jasa pihak ketiga sudah diterapkan, dioperasikan dan dipelihara oleh pihak ketiga? Apakah salinan back-up dan piranti lunak yang penting sudah dilakukan secara berkala?	Ya	Perjanjian terhadap Vendor. Ada Salinannya juga, kalo

	Klausul A.10.2.2	Q77	Apakah jasa, laporan dan rekaman yang diberikan oleh pihak ketiga sudah dipantau, dikaji dan diaudit secara regular?	tidak	Harga mengacu dari Vendor.
	Klausul A.10.3.1	Q78	Apakah peggunaan sumberdaya sudah dipantau dan disesuaikan untuk pemenuhan kapasitas mendatang?	tidak	fleksibel, tergantung kebutuhan Sign
	Klausul A.10.3.2	Q79	Apakah sudah selalu dilakukan pengujian terhadap sistem informasi yang baru, upgrade atau versi terbaru sebelum diterima?	ya	
	Klausul A.10.5.1	Q80	Apakah fasilitas back-up sudah memadai guna memulihkan seluruh sistem informasi jika terjadi bencana atau kegagalan?	tidak	Ada, tapi belum sepenuhnya
		Q81	Catatan yang akurat dari salinan back-up dan prosedur pemulihan yang terdokumentasi apakah sudah disimpan di lokasi yang terpisah?	tidak	
		Q82	Apakah media back-up sudah diuji secara berkala untuk memastikan bisa digunakan di situasi darurat?	~~tidak~~ ya	

PERTANYAAN WAWANCARA

Document ID : INTV-ISO

Klausul A.10 Manajemen Komunikasi dan Operasi

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	Klausul A.10.6.1	Q83	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan data dalam jaringan?	YA	
		Q84	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan?	YA	Bagian kasi jaringan yang khusus Menangani jaringan
	Klausul A.10.6.2	Q85	Apakah sudah menerapkan mekanisme pengamanan jaringan yang rawan terhadap serangan?	YA	
		Q86	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan?	YA	
		Q87	Apabila serangan terjadi, adakah mekanisme recovery jaringan yang diterapkan?	YA	
		Q88	Seberapa sering fitur keamanan dan tingkat layanan jaringan di identifikasi?	YA	Per Bulan
	Klausul A.10.7.1	Q89	Apakah ada prosedur untuk manajemen pemindahan media?	TIDAK	
		Q90	Apakah sudah terdokumentasi prosedur tersebut?	BELUM	
	Klausul A.10.7.2	Q91	Apakah ada tindakan pemusnahan media apabila tidak lagi diperlukan?	TIDAK	Ditaruh digudang tidak ada prosedur nya
		Q92	Apakah ada prosedur pemusnahan media?	TIDAK	
		Q93	Apakah sudah terdokumentasi prosedur tersebut?	TIDAK	

	Klausul A.10.7.3	Q94	Apakah sudah ada prosedur penanganan dan penyimpanan informasi untuk melindungi informasi dari penyalahgunaan?	YA	Ada prosedur penanganan
		Q95	Apakah sudah terdokumentasi prosedur tersebut?	YA	
	Klausul A.10.7.4	Q96	Apakah sudah ada dokumentasi sistem untuk melindungi terhadap akses yang tidak sah?	YA	
	Klausul A.10.8.1	Q97	Apakah sudah ada kebijakan prosedur dan pengendalian untuk melindungi pertukaran informasi dengan menggunakan semua jenis fasilitas komunikasi?	BELUM	fasilitas selalu diusahakan yang terbaik, tetapi pengendalianya belum ada, tetapi ada perlindungan
		Q98	Apakah sudah terdokumentasikan prosedur tersebut?	BELUM	
	Klausul A.10.8.2	Q99	Apakah ada perjanjian terhadap pertukaran infromasi dan perangkat lunak antara organisasi dan pihak eksternal?	YA	jika dengan pihak luar, ada perjanjian dulu pastinya
	Klausul A.10.8.3	Q100	Apakah sudah disediakan media untuk memuat informasi terhadap hak akses yang tidak sah, penyalahgunaan atau kerusakan selama transportasi diluar batas fisik organisasi?	YA	
	Klausul A.10.8.4	Q101	Apakah ada perlindungan informasi yang disajikan dalam bentuk pesan elektronik?	YA	
	Klausul A.10.10.1	Q102	Apakah sudah tersedia log untuk merekam kegiatan pengguna dan kejadian keamanan informasi dalam membantu investigasi dan pemantauan akses?	YA	Dipantau, Ada CCTV juga
	Klausul A.10.10.2	Q103	Apakah ada prosedur pemantauan penggunaan fasilitas pengolahan informasi dan hasil kegiatan pemantauan ditinjau secara regular?	YA	PER BULAN
	Klausul		Apakah sudah tersedia fasilitas log dan informasi yang harus dilindungi terhadap gangguan dan akses tidak	YA	

	A.10.10.3	Q104	sah?		
	Klausul A.10.10.4	Q105	Apakah sudah tercacat dalam log kegiatan administrator sistem dan operator sistem?	YA	
	Klausul A.10.10.5	Q106	Apabila terjadi kesalahan, apakah sudah tercatat dalam log, dianalisis dan diambil tindakan yang sesuai?	YA.	

Document ID : INTV-

Klalusul A.12 Akuisi, Pengembangan dan Pemeliharaan Sistem Informasi

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	A.12.1.1	Q149	Apakah telah ditetapkan persyaratan bisnis untuk sistem infromasi yang baru?	YA	
		Q150	Apakah telah terdokumentasi persyaratan tersebut?	YA	
	A.12.2.1	Q151	Apakah sudah ada prosedur validasi data ketika memasukkan data ke simak online UIGM?	YA	Ada SOP nya
		Q152	Apakah sudah ada prosedur untuk merespon kesalahan validasi?	YA	Ada dalam SOP SI
	A.12.2.2	Q153	Apakah digabungkan ke dalam aplikasi dalam pengecekan validasi untuk mendeteksi kerusakan informasi karena kesalahan?	YA	
		Q154	Ketika ada kerusakan informasi karena ada kesalahan pengolahan apakah bisa dideteksi oleh sistem?	YA	Ada notif / pemberitahuan kesalahan
	A.12.2.3	Q155	Apakah sudah ada perlindungan integritas pesan dalam aplikasi?	YA	
		Q156	Sudah ada pengendalian yang tepat dalam persyaratan untuk memastikan keaslian dan perlindungan intgritas pesan dalam aplikasi?	YA	Di uji terlebih dahulu
		Q157	Apakah sudah diterapkan persyaratan tersebut?	YA	
	A.12.2.4	Q158	Apakah sudah divalidasi dan diidentifikasi keluaran data dari aplikasi?	YA	
		Q159	Apakah sudah diterapkan validasi dan identifikasi keluaran tersebut?	YA	
	A.12.3.1	Q160	Apakah sudah ada kebijakan pengendalian kriptografi untuk melindungi informasi?	YA	Untuk pengamanan, perlu bahan harus ada kriptografi

		Q161	Apakah sudah dikembangkan dan diterapkan pengendalian kriptografi tersebut?	YA	
	A.12.3.2	Q162	Apakah sudah ada manajemen kunci yang tersedia untuk mendukung penggunaan teknik kriptografi oleh organisasi?	YA	
	A.12.4.1	Q163	Apakah ada prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional?	YA	
	A.12.4.2	Q164	Apakah data sudah dipilih secara hati-hati dan dlindungi serta dikendalikan?	YA	
	A.12.4.3	Q165	Apkah sudah dibatasi akses ke kode sumber program?	YA	
	A.12.5.1	Q166	Apakah ada prosedur pengendalian yang formal jika terjadi perubahan dalam sistem aplikasi atau informasi?	YA	
		Q167	Apakah sudah diterapkan prosedur pengendalian tersebut?	YA	
		Q168	Apakah sudah terdokumentasi pengendalian tersebut?	BELUM	
	A.12.5.2	Q169	Apakah sudah ditinjau dan diuji apaila ada perubahan sistem operasi atau aplikasi untuk memastikan tidak ada dampak yang merugikan terhadap organisasi?	YA	
		Q170	Apakah penting menjaga keamanan sistem informasi ketika dilakkukan perubahan sistem operasi?	YA	
	A.12.5.3	Q171	Apakah sering melakukan modifikasi perangkat lunak?	YA	
		Q172	Apakah sudah dibatasi hanya pada perubahan yang perlu saja daam modifikasi perangkat lunak?	YA	
		Q173	Apa sudah dikendalikan dengan ketat seluruh perubahan tersebut?	YA	

	A.12.5.4	Q174	Apakah sudah dicegah dalam peluang adanya kebocoran informasi?	YA	
	A.12.5.5	Q178	Apakah sudah dipantau oleh organisasi pengembangan perangkat lunak yang dialihdayakan?	YA	
	A.12.5.6	Q179	Apakah sudah dievaluasi informasi tepat waktu tentang kerawanan teknis dari sistem infromasi yang digunakan?	TIDAK	
		Q180	Apakah sudah diambil tindakan untuk menangani resiko terkait?	Belum	

Lembar Kertas Kerja Audit

Audit Keamanan Simak Online Universitas Indo Global Mandiri Paembang

Berdasarkan Standard ISO/IEC 27001:2005

Document ID	: INTV-ISO-1
Project Name	: Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001:2005
Auditor	: Yeni Rahayu
Auditee	: Parhan Oktaria Putra
Description	: Lembar kertas audit ini merupakan bagian dari penelitian tugas akhir mahasiswa Program Studi Sistem Informasi, Universitas Islam Negeri Raden Fatah Palembang Lembar kertas kerja audit ini digunakan untuk mengetahui tingkat keamanan informasi simak online Universitas Indo Global Mandiri Palembang.
Date	: 01 OKTOBER 2018
Responsible	: Information Security Officer (ISO)

Approved by

Biro Pelaksana Teknis UGM

(Parhan Oktaria Putra)

Auditor

(Yeni Rahayu)

PERTANYAAN WAWANCARA

Document ID : INTV-ISO

Klalusul A.9 Keamanan Fisik dan Lingkungan

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	Klausul A.9.1.1	Q46	Apakah pintu masuk sudah dikendalikan dengan kartu gesek atau PIN guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas?	Tidak	Masih dengan kunci biasa
		Q47	Apakah penting pintu masuk ruang sistem informasi dibatasi dengan sistem pengamanan dan kartu kontrol?	ya	
		Q48	Apakah ada kontrol akses fisik atau ruang sebagai tempat menerima tamu?	ya	Ada ruang khusus
		Q49	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain didalamnya?	ya	
		Q50	Perlukah ruangan khusus atas pembatas seperti dinding untuk seorang pemegang kendali sistem informasi?	ya	
	Klausul A.9.1.2	Q51	Apakah pengunjung yang datang diawasi dan tanggal datang dan perginya dicatat?	ya	
		Q52	Apakah dikontrol dan dibatasi akses ke informasi sensitif dan fasilitas pengolahan informasi?	ya	
	Klausul A.9.1.3	Q53	Semua pegawai dan karyawan apakah sudah diwajibkan memakai tanda pengenal?	ya	

	Klausul A.9.1.4	Q55	kerusakan akibat dari ledakan, kecelakaan dan bencana lainnya?	Ya	
		Q56	Apakah bahan berbahaya dan mudah meledak sudah disimpan di wilayah yang aman?	Ya	Ada ruang khusus tersendiri
	Klausul A.9.1.5	Q57	Apakah penempatan ruang sistem informasi sudah termasuk dalam area yang aman?	Ya	
		Q58	Apakah sudah mempertimbangkan kebijakan tentang makan, minum dam merokok disekitar fasilitas pemrosesan sistem informasi?	Ya	Ada peringatannya yang di tempel pada tembok
		Q59	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan?	Ya	
	Klausul A.9.1.6	Q60	Dari segi wilayah keamanan apakah penempatan posisi ruang sudah membuat nyaman pengelola sistem informasi?	Ya	
		Q61	Jika ada perbaikan ruangan dan peralatan informasi lainnya apakah pekerja yang berasal dari luar BPT UIGM akan dilakukan pengawasan dan dipantau?	Ya	
		Q62	Apakah penting mendampingi pekerja yang melakukan perbaikan dan bagaimana prosedur pengawasannya?	Ya	
	Klausul A.9.2.1	Q63	Apakah komputer dan peralatan informasi lainnya seperti server, sudah ditempatkan pada tempat yang cukup aman?	Ya	
		Q64	Apakah keamanan peralatannya sudah tidak ada peluang akses pihak yang tidak berwenang?	Ya	Hanya orang tertentu
	Klausul A.9.2.2	Q65	Apakah peralatannya sudah dilindungi dari kegagalan catu daya listrik?	Ya	
		Q66	Apakah sudah tersedia peralatan pendukung seperti UPS dan pembangkit listrik cadangan?	Ya	

	Klausul A.9.2.3	Q67	Apakah kabel daya dan telekomunikasi yang membawa data atau jasa sudah dilindungi dari penyadapan dan kerusakan, seperti menggunakan pipa pengaman?	Ya	
		Q68	Apakah sudah dihindari melakukan routing melalui tempat umum?	Ya	

Lembar Kertas Kerja Audit

Audit Keamanan Simak Online Universitas Indo Global Mandiri Paembang

Berdasarkan Standard ISO/IEC 27001:2005

Document ID	: INTV-ISO-4
Project Name	: Audit Keamanan Informasi Simak Online Universitas Indo Global Mandiri Palembang Berdasarkan Standard ISO/IEC 27001:2005
Auditor	: Yeni Rahayu
Auditee	: Jimiria Pratama
Description	: Lembar kertas audit ini merupakan bagian dari penelitian tugas akhir mahasiswa Program Studi Sistem Informasi, Universitas Islam Negeri Raden Fatah Palembang Lembar kertas kerja audit ini digunakan untuk mengetahui tingkat keamanan informasi simak online Universitas Indo Global Mandiri Palembang.
Date	: 01 OKTOBER 2018
Responsible	: Information Security Officer (ISO)

Approved by	Auditor
Biro Pelaksana Teknis UIGM	
(Jimiria Pratama)	(Yeni Rahayu)

PERTANYAAN WAWANCARA

Document ID : INTV-ISO

Klausul A.11 Pengendalian Akses

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	Klausul A.11.1.1	Q107	Apakah sudah ditetapkan kebijakan pengendalian akses?	YA	
		Q108	Apakah kebijakan tersebut sudah terdokumentasikan berdasarkan persyaratan bisnis dan keamanan untuk akses?	YA	
	Klausul A.11.2.1	Q109	Apakah ada prosedur pendaftaran dan pembatalan pendaftaran pengguna untuk memberi dan mencabut hak akses terhadap sistem informasi?	YA	Dicabut Hak Akses ketika membatalkan pendaftaran pada SI
		Q110	Apakah sudah terdokumentasikan prosedur tersebut?	YA	
	Klausul A.11.2.2	Q111	Apakah ada alokasi hak khusus yang harus dibatasi dan dikendalikan?	YA	
	Klausul A.11.2.3	Q112	Apakah ada alokasi password untuk mengendalikan proses manajemen formal?	tidak	
	Klasusul A.11.2.4	Q113	Apakah sudah ada peninjauan terhadap hak akses pengguna secara regular menggunakan proses formal?	YA	
	Klausul A.11.3.1	Q114	Apakah ada pedoman yang disyaratkan untuk pengamanan yang baik dalam pemilihan dan penggunaan password?	YA	Ada SOP

	Klausul A.11.3.2	Q115	Apakah sudah ada kebijakan clear desk terhadap kertas dan media penyimpanan yang dapat di pindahkan untuk fasilitas pengolahan informasi?	tidak	tidak ada prosedur / kebijakan saat ini
		Q116	Apakah sudah ada kebijakan clear screen untuk fasilitas pengolahan informasi?	YA	penghapusan pada SI, ada
	Klausul A.11.4.1	Q117	Apakah pengguna telah hanya diberikan akses terhadap layanan yang telah diberikan kewenangan penggunaanya secara spesifiik?	YA	
	A.11.4.3	Q118	Apakah sudah diidentifikasi peralatan secara otomatis untuk mengotentifikasi koneksi lokasi dan peralatan spesifik?	tidak	Belum ada saat ini
	Klausul A.11.4.4	Q119	Apakah sudah ada pelindungan pengendalian secara fisik dan logical terhadap diacnotic dan configuraiton port	YA	
	Klausul A.11.4.6	Q120	Apakah sudah disegresikan terhadap layanan informasi pengguna dan sistem informasi di dalam jaringan?	YA	
	Klausul A.11.4.7	Q121	Apakah sudah ada pengendalian routing yang telah diterapkan ke dalam jaringan untuk memastikan bahwa koneksi komputer dan aliran informasi tidak melanggar kebijakan pengendalian akses?	tidak	Belum sepenuhnya, masih dalam proses, ketika ada kesalah hanya di perbaiki lagi
	Klausul A.11.5.1	Q122	Apakah sudah ada prosedur log-on yang aman?	tidak	
	Klausul A.11.5.2	Q123	Apakah setiap pengguna mempunyai user id untuk penggunaan personal masing-masing user?	YA	Ada pada SI
		Q124	Apakah sudah ada teknik validasi dalam setiap user id yang terdaftar?	YA	
	Klausul A.11.5.3	Q125	Apakah sudah ada sistem manajemen password?	YA	

Document ID : INTV-

Klalusul A.13 Manajemen Insiden Keamanan Informasi

NO	KLAUSUL	KODE	PERTANYAAN	YA/TIDAK	KOMENTAR
1	A.13.1.1	Q175	Apakah sudah diambil tindakan dan dilaporkan melalui saluran manajemen yang tepat dan cepat apabila terjadi insiden keamanan informasi?	Ya	Pasti melapor Ketika terjadi insiden
	A.13.1.2	Q176	Apa sudah disyaratkan untuk mencatat dan melaporkan setiap kelemahan keamanan yang diamati dan dicurigai?	Ya	
		Q177	Apakah sudah dilaporkan ke semua pegawai, kontraktor dan pengguna pihak ketiga ketika insiden terbut terjadi?	Ya	
	A.13.2.1	Q178	Apa sudah ditetapkan tanggung jawab manajemen apabila terjadi insiden keamanan informasi?	ya	telah dibagi tanggung jawab sesuai perannya
		Q179	Apakah sudah terdokumentasi ketetapan tersebut?	ya	
	A.13.2.2	Q180	Apakah sudah tersedia mekanisme yang memungkinkan jenis, volume, dan biaya insiden keamanan informasi?	Ya	Direncanakan dan diperkirakan dulu
		Q181	Apakah sudah diukur dan dipantau mekanisme tersebut?	Ya	
	A.13.2.3	Q182	Apakah sudah diambil tindakan pengumpulan bukti terhadap orang atau organisasi selelah insiden keamanan informasi yang melibatkan tindakan hukum (baik perdata atau pidana)?	Ya	Dikumpulkan dan disimpan bukti-bukti yang melibatkan tindakan hukum ~~seperti terjadi~~
		Q183	Apakah sudah disimpan bukti terhadap insiden kemanan informasi tersebut?	Ya	
		Q184	Apa sudah disajikan sesuai aturan berkenaan dengan bukti yang ditetapkan dalam wilayah hukum?	Ya	

LAMPIRAN IV

URAIAN TUGAS KARYAWAN UNIVERSITAS INDO GLOBAL MANDIRI PALEMBANG

UNIVERSITAS INDO GLOBAL MANDIRI (UIGM)

BIRO PELAKSANA TEKNIS

Jl. Jend. Sudirman No. 629 Km. 4 Palembang
Telp.(0711) 322705 – 322706 Fax. (0711) 357754

FAKULTAS ILMU KOMPUTER Website : www.uigm.ac.id E-mail : info @igm.ac.id

URAIAN TUGAS KARYAWAN UNIVERSITAS INDO GLOBAL MANDIRI

Nama : Ir. Dedy Hermanto, MT
NIK : 2010030022
Jabatan : Kepala Bagian Laboratorium
Unit Kerja : Biro Pelkasana Teknis

No.	Uraia Tugas	Produk	Frekuensi
1	Menyusun rencana dan program kerja Bagian Laboratorium	Proposal	1 per tahun ajaran
2	Menyiapkan data dan bahan Renstra	Laporan dan Inventaris	1 per tahun ajaran
3	Melaksanakan pembagian tugas kepada staf sesuai bidangnya;	Jobdesk, Daftar Piket	Sesuai kebutuhan
4	Menyiapkan data dan bahan RKAT BPT	Laporan dan Proposal	1 per tahun ajaran
5	Melaksanakan administrasi BPT ; Surat masuk/keluar , pengembangan, pengelolaan dan pemeliharaan laboratorium	10-15 Surat, Berita Acara dan Rekomendasi	1 bulan
6	Menyusun konsep laporan-laporan Melaksanakan tugas lain yang diberikan oleh atasan;	Draft Laporan	Sesuai kebutuhan
7	Menyusun laporan sebagai pertanggung jawaban kepada atasan	Laporan Tahunan	1 Tahun Ajaran

Palembang, 11 April 2018

Mengetahui,
Kepala Biro Pelaksana Teknis

Kepala Bagian Labororium

Dr. Herri Setiawan, M.Kom
NIK. 2003010060

Ir. Dedy Hermanto, MT
NIK. 2010030022

UNIVERSITAS INDO GLOBAL MANDIRI (UIGM)
BIRO PELAKSANA TEKNIS
Jl. Jend. Sudirman No. 629 Km. 4 Palembang
Telp.(0711) 322705 – 322706 Fax. (0711) 357754
FAKULTAS ILMU KOMPUTER Website : www.uigm.ac.id E-mail : info @igm.ac.id

URAIAN TUGAS KARYAWAN UNIVERSITAS INDO GLOBAL MANDIRI

Nama : Tasmi, S.Si.,M.Kom
NIK : 2017010230
Jabatan : Kepala Bagian Jaringan dan Hardware
Unit Kerja : Biro Pelakasana Teknis

No.	Uraian Tugas	Produk	Frekuensi
1	Menyusun rencana dan program kerja Bagian Jaringan dan Hardware	Proposal	1 per tahun ajaran
2	Menyiapkan data dan bahan Renstra	Laporan dan Inventaris	1 per tahun ajaran
3	Melaksanakan pembagian tugas kepada staf sesuai bidangnya	Jobdesk, Daftar Piket	Sesuai kebutuhan
4	Menyiapkan data dan bahan RKAT BPT	Laporan dan Proposal	1 per tahun ajaran
5	Melaksanakan administrasi BPT ; Surat Masuk/Keluar , pengembangan, pengelolaan dan pemeliharaan Jaringan dan Hardware	10-15 Surat, Berita Acara dan Rekomendasi	1 bulan
6	Menyusun konsep laporan-laporan Melaksanakan tugas lain yang diberikan oleh atasan	Draft Laporan	Sesuai kebutuhan
7	Menyusun laporan sebagai pertanggung jawaban kepada atasan	Laporan Tahunan	1 Tahun Ajaran

Palembang, 11 April 2018

Mengetahui,
Kepala Biro Pelaksana Teknis

Dr. Herri Setiawan, M.Kom
NIK. 2003010060

Kepala Bagian Jaringan dan Hardware

Tasmi, S.Si.,M.Kom
NIK. 2017010230

UNIVERSITAS INDO GLOBAL MANDIRI (UIGM)
BIRO PELAKSANA TEKNIS
Jl. Jend. Sudirman No. 629 Km. 4 Palembang
Telp.(0711) 322705 – 322706 Fax. (0711) 357754
FAKULTAS ILMU KOMPUTER Website : www.uigm.ac.id E-mail : info @igm.ac.id

URAIAN TUGAS KARYAWAN UNIVERSITAS INDO GLOBAL MANDIRI

Nama : M. Agus Munandar, A.Md
NIK : 2010020051
Jabatan : Kepala Seksi Laboratorium
Unit Kerja : Biro Pelakasana Teknis

No.	Uraian Tugas	Produk	Frekuensi
1	Membantu menyusun rencana dan program kerja seksi laboratorium	Inventaris, draft proposal	1 per tahun ajaran
2	Menyiapkan data dan bahan Renstra	Laporan dan Inventaris	1 per tahun ajaran
3	Melaksanakan pembagian tugas kepada staff teknisi laboratorium	Jobdesk, jadwal pemeliharaan	Sesuai kebutuhan
4	Menyiapkan lab	Install dan ketersedian software	Sesuai kebutuhan
5	Membantu menyiapkan data dan bahan RKAT BPT	Data inventaris	1 per tahun ajaran
6	Melaksanakan administrasi BPT ; pengembangan, pengelolaan dan pemeliharaan laboratorium	Berita Acara, perbaikan peralatan, laporan	1 minggu
7	Membantu menyusun konsep laporan-laporan dan melaksanakan tugas teknis lain yang diberikan oleh atasan;	Draft Laporan	Sesuai kebutuhan
8	Menyusun laporan sebagai pertanggung jawaban kepada atasan	Laporan Tahunan	1 Tahun Ajaran

Palembang, 11 April 2018

Mengetahui,
Kepala Biro Pelaksana Teknis

Dr. Herri Setiawan, M.Kom
NIK. 2003010060

Kepala Seksi Laboratorium

M.Agus Munandar, A.Md
NIK. 2010020051

UNIVERSITAS INDO GLOBAL MANDIRI (UIGM)
BIRO PELAKSANA TEKNIS
Jl. Jend. Sudirman No. 629 Km. 4 Palembang
Telp.(0711) 322705 – 322706 Fax. (0711) 357754
FAKULTAS ILMU KOMPUTER Website : www.uigm.ac.id E-mail : info @igm.ac.id

URAIAN TUGAS KARYAWAN UNIVERSITAS INDO GLOBAL MANDIRI

Nama : Parhan Oktaria Putra
NIK :
Jabatan : Teknisi Laboratorium
Unit Kerja : Biro Pelakasana Teknis

No.	Uraian Tugas	Produk	Frekuensi
1	Membantu menyusun rencana dan program kerja seksi laboratorium	Inventaris, draft proposal	1 per tahun ajaran
2	Menyiapkan data dan bahan Renstra	Laporan dan Inventaris	1 per tahun ajaran
3	Menyiapkan laboratorium	Install, LAN, ketersediaan software dan perbaikan peralatan	Sesuai kebutuhan
4	Membantu menyiapkan data dan bahan RKAT BPT	Data inventaris	1 per tahun ajaran
5	Membantu pelaksanakan administrasi BPT ; pengembangan, pengelolaan dan pemeliharaan laboratorium	Laporan monitoring di lapangan	1 minggu
6	Melaksanakan tugas teknis lain yang diberikan oleh atasan;	Laporan	Sesuai kebutuhan
7	Pemeliharaan laboratorium	Monitoring, perbaikan dan evaluasi peralatan	1 Minggu

Palembang, 11 April 2018

Mengetahui,
Kepala Biro Pelaksana Teknis

Dr. Herri Setiawan, M.Kom
NIK. 2003010060

Teknisi,

Parhan Oktaria Putra

UNIVERSITAS INDO GLOBAL MANDIRI (UIGM)
BIRO PELAKSANA TEKNIS
Jl. Jend. Sudirman No. 629 Km. 4 Palembang
Telp.(0711) 322705 – 322706 Fax. (0711) 357754
FAKULTAS ILMU KOMPUTER Website : www.uigm.ac.id E-mail : info @igm.ac.id

URAIAN TUGAS KARYAWAN UNIVERSITAS INDO GLOBAL MANDIRI

Nama : Dr. Herri Setiawan, M.Kom
NIK : 2003010060
Jabatan : Kepala Biro Pelaksana Teknis
Unit Kerja : Biro Pelaksana Teknis

No.	Uraian Tugas	Produk	Frekuensi
1	Menyusun rencana dan program kerja BPT	Proposal	1 per tahun ajaran
2	Mempelajari dan mengadopsi perkembangan TIK di lingkungan UIGM, dan mengkaji peraturan/perundang undangan yang menaunginya	Kutipan/dokumentasi/publikasi /jurnal/buku buku dan perundang-undangan	1 per tahun ajaran
3	Mengoordinasikan: a. Pelaksanaan dan penyusunan Renstra bidang; b. Mengoordinasikan pelaksanaan dan menyusun RKAT BPT; c. Menetapkan dan Mengkoordinasikan pelaksanaan pembagian tugas kepada Kepala Bagian; d. Mengoordinasikan pelaksanaan pengembangan, pengelolaan dan pemeliharaan laboratorium, jaringan internet/komputer dan peralatan TIK lainnyaMengoordinasikan pelayanan teknologi informasi untuk pendidikan, penelitian, dan pengabdian kepada masyarakat; e. Mengoordinasikan pelaksanaan administrasi BPT;	Proposal, Laporan Proposal Jobdesk, Jadwal Perencanaan	1 per tahun ajaran Sesuai Kebutuhan
4	Melaksanakan Monitoring dan Evaluasi di lingkiungsn BPT	Laporan, Rekomendasi	1 semester
5	Menyusun konsep laporan-laporan	Laporan	Sesuai kebutuhan
6	Menyusun laporan sebagai pertanggung jawaban kepada atasan	Laporan Tahunan	1 Tahun Ajaran

Palembang, 11 April 2018

Mengetahui,
Wakil Rektor II

John Roni Coyanda, M.Si
NIK.1999010007

Kepala Biro Pelaksana Teknis

Dr. Herri Setiawan, M.Kom
NIK. 2003010060

UNIVERSITAS INDO GLOBAL MANDIRI (UIGM)
BIRO PELAKSANA TEKNIS
Jl. Jend. Sudirman No. 629 Km. 4 Palembang
Telp.(0711) 322705 – 322706 Fax. (0711) 357754
FAKULTAS ILMU KOMPUTER Website : www.uigm.ac.id E-mail : info @igm.ac.id

URAIAN TUGAS KARYAWAN UNIVERSITAS INDO GLOBAL MANDIRI

Nama : Jimiria Pratama
NIK :
Jabatan : Teknisi
Unit Kerja : Biro Pelakasana Teknis

No.	Uraia Tugas	Produk	Frekuensi
1	Turut membantu menyusun rencana dan program kerja BPT	Inventaris, laporan	1 per tahun ajaran
2	Menyiapkan Jaringan, Hardware dan Laboratorium	Install, LAN, ketersediaan software dan perbaikan peralatan TIK	Sesuai kebutuhan
3	Memastikan kesiapan jaringan, hardware dan laboratorium	Data inventaris	1 per tahun ajaran
4	Mengumpulkan data dan bahan sebagai masukan penyusunan RKAT	Laporan monitoring di lapangan	1 per tahun ajaran
5	Melakukan Pemeliharaan rutin jaringan, hardware dan laboratorium	Laporan monitoring, perbaikan dan evaluasi peralatan	Sesuai kebutuhan
6	Melaksanakan tugas teknis lain yang diberikan oleh atasan	Laporan	Sesuai kebutuhan

Palembang, 11 April 2018

Mengetahui,
Kepala Biro Pelaksana Teknis

Dr. Herri Setiawan, M.Kom
NIK. 2003010060

Teknisi

Jimiria Pratama

UNIVERSITAS INDO GLOBAL MANDIRI (UIGM)
BIRO PELAKSANA TEKNIS
Jl. Jend. Sudirman No. 629 Km. 4 Palembang
Telp.(0711) 322705 – 322706 Fax. (0711) 357754
FAKULTAS ILMU KOMPUTER Website : www.uigm.ac.id E-mail : info @igm.ac.id

URAIAN TUGAS KARYAWAN UNIVERSITAS INDO GLOBAL MANDIRI

Nama : Adam Jaya Putra
NIK :
Jabatan : Teknisi
Unit Kerja : Biro Pelakasana Teknis

No.	Uraia Tugas	Produk	Frekuensi
1	Turut membantu menyusun rencana dan program kerja BPT	Inventaris, laporan	1 per tahun ajaran
2	Menyiapkan Jaringan, Hardware dan Laboratorium	Install, LAN, ketersediaan software dan perbaikan peralatan TIK	Sesuai kebutuhan
3	Memastikan kesiapan jaringan, hardware dan laboratorium	Data inventaris	1 per tahun ajaran
4	Mengumpulkan data dan bahan sebagai masukan penyusunan RKAT	Laporan monitoring di lapangan	1 per tahun ajaran
5	Melakukan Pemeliharaan rutin jaringan, hardware dan laboratorium	Laporan monitoring, perbaikan dan evaluasi peralatan	Sesuai kebutuhan
6	Melaksanakan tugas teknis lain yang diberikan oleh atasan;	Laporan	Sesuai kebutuhan

Palembang, 11 April 2018

Mengetahui,
Kepala Biro Pelaksana Teknis

Dr. Herri Setiawan, M.Kom
NIK. 2003010060

Teknisi

Adam Putra Jaya

UNIVERSITAS INDO GLOBAL MANDIRI (UIGM)
BIRO PELAKSANA TEKNIS
Jl. Jend. Sudirman No. 629 Km. 4 Palembang
Telp.(0711) 322705 – 322706 Fax. (0711) 357754
FAKULTAS ILMU KOMPUTER Website : www.uigm.ac.id E-mail : info @igm.ac.id

URAIAN TUGAS KARYAWAN UNIVERSITAS INDO GLOBAL MANDIRI

Nama : Reza Maulana, A.Md
NIK : 2017020087
Jabatan : Kepala Seksi Jaringan dan Hardware
Unit Kerja : Biro Pelakasana Teknis

No.	Uraian Tugas	Produk	Frekuensi
1	Membantu menyusun rencana dan program kerja seksi Jaringan dan Hardware	Inventaris, draft proposal	1 per tahun ajaran
2	Membantu menyiapkan data dan bahan Renstra	Laporan dan Inventaris	1 per tahun ajaran
3	Melaksanakan pembagian tugas kepada staff teknisi jaringan dan hardware	Jobdesk, jadwal pemeliharaan	Sesuai kebutuhan
4	Membantu menyiapkan data dan bahan RKAT BPT	Data inventaris	1 per tahun ajaran
5	Melaksanakan administrasi BPT ; pengembangan, pengelolaan dan pemeliharaan jaringan dan hardware	Berita Acara, perbaikan peralatan, laporan	1 minggu
6	Membantu menyusun konsep laporan-laporan dan melaksanakan tugas teknis lain yang diberikan oleh atasan;	Draft Laporan	Sesuai kebutuhan
7	Menyusun laporan sebagai pertanggung jawaban kepada atasan	Laporan Tahunan	.01 Tahun Ajaran

Palembang, 11 April 2018

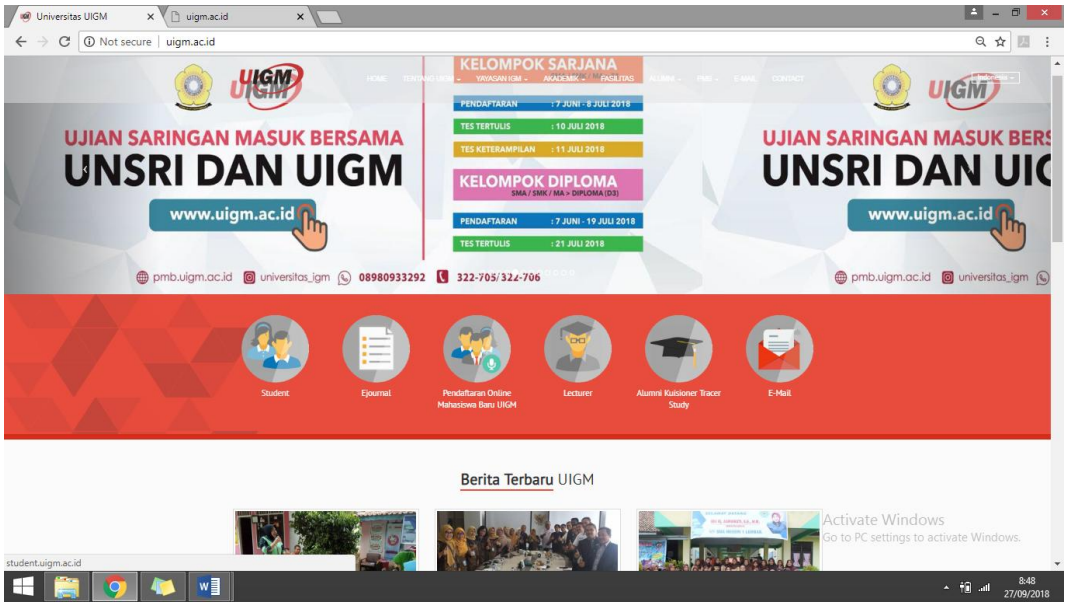
Mengetahui,
Kepala Biro Pelaksana Teknis

Dr. Herri Setiawan, M.Kom
NIK. 2003010060

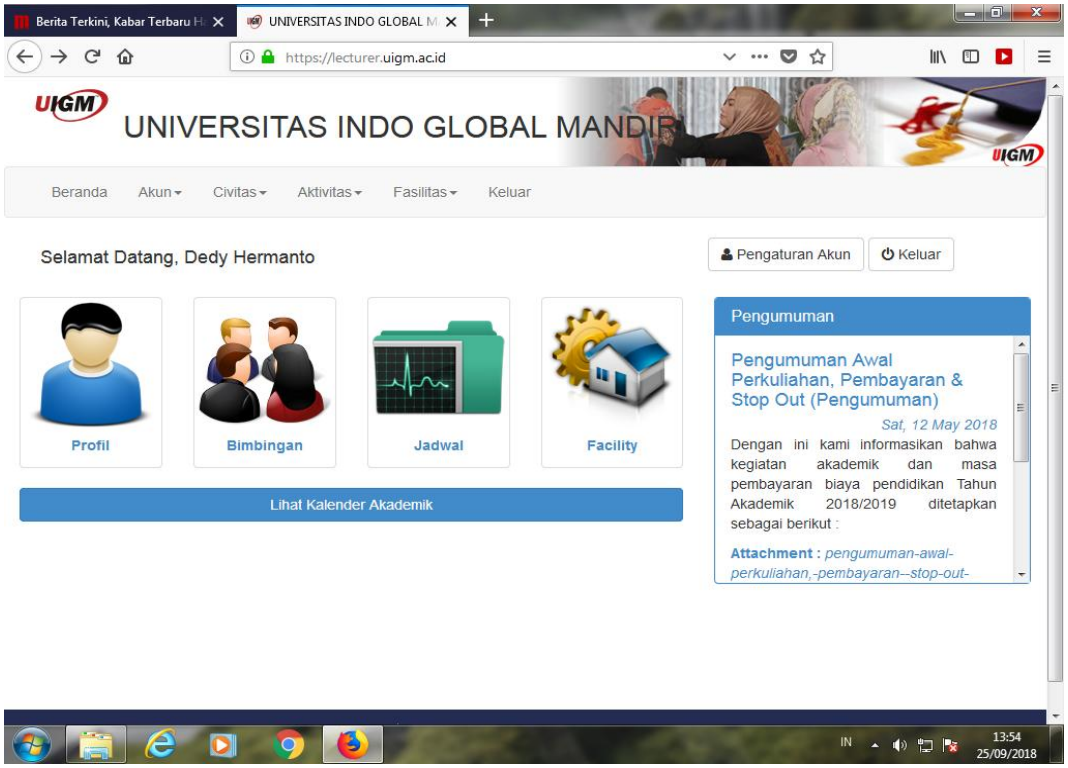
Kepala Seksi Jaringan dan Hardware

Reza Maulana , A.Md
NIK. 2017020087

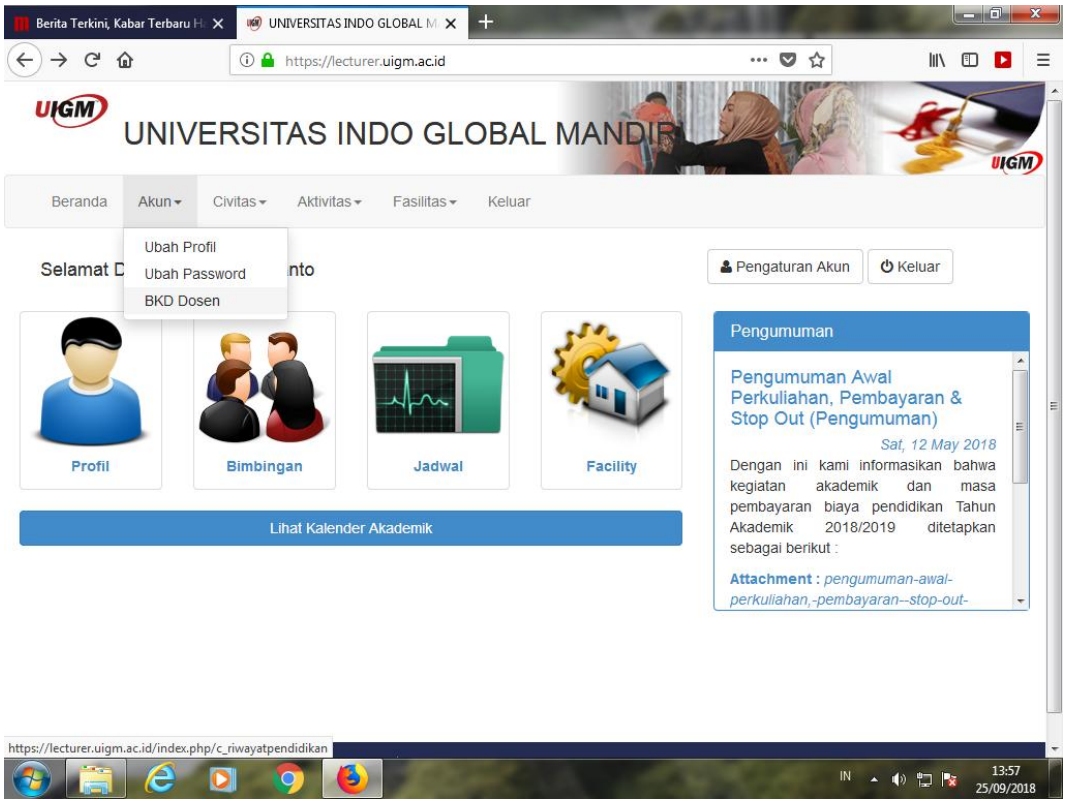
Lampiran Tampilan Sistem Informasi Akademik Universitas Indo Global Mandiri Palembang



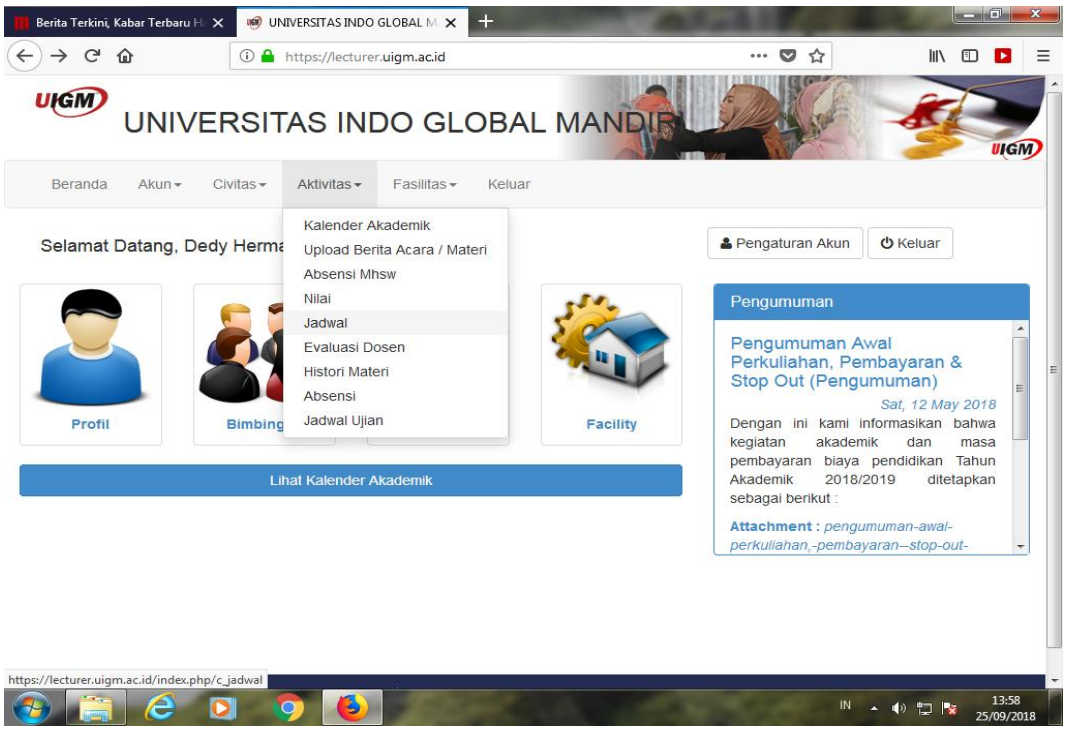
Gambar 4.4 halaman utama simak *online*



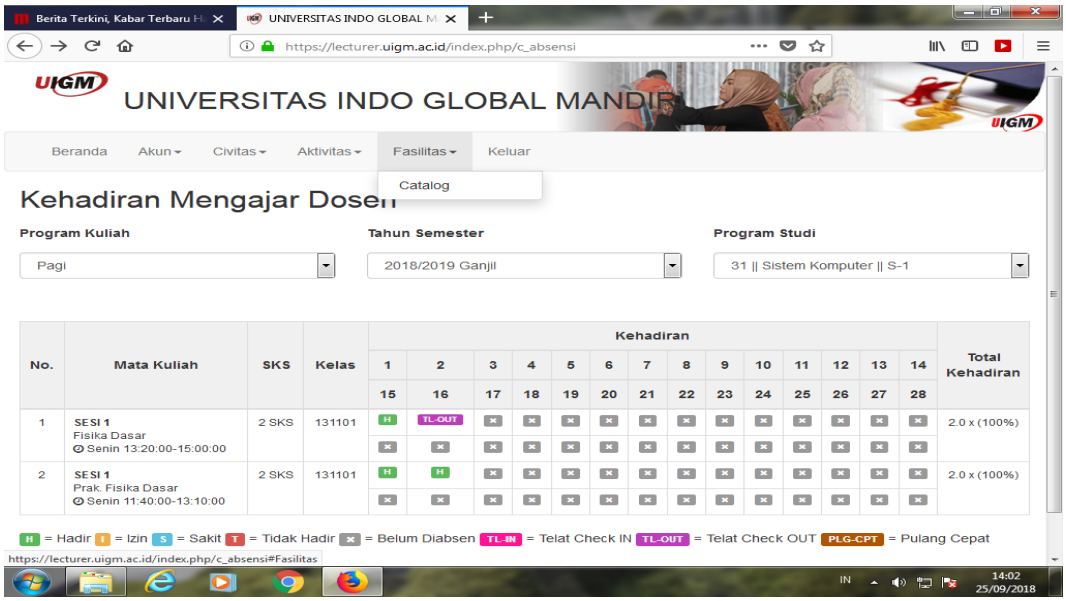
Gambar 4.5 halaman login sebagai dosen



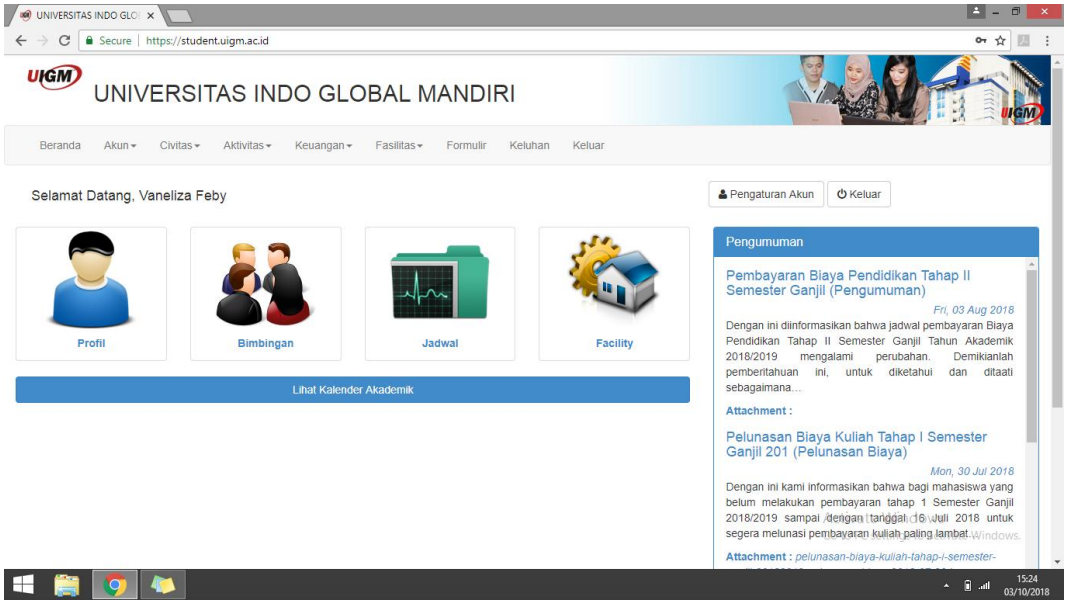
Gambar 4.6 halaman menu akun



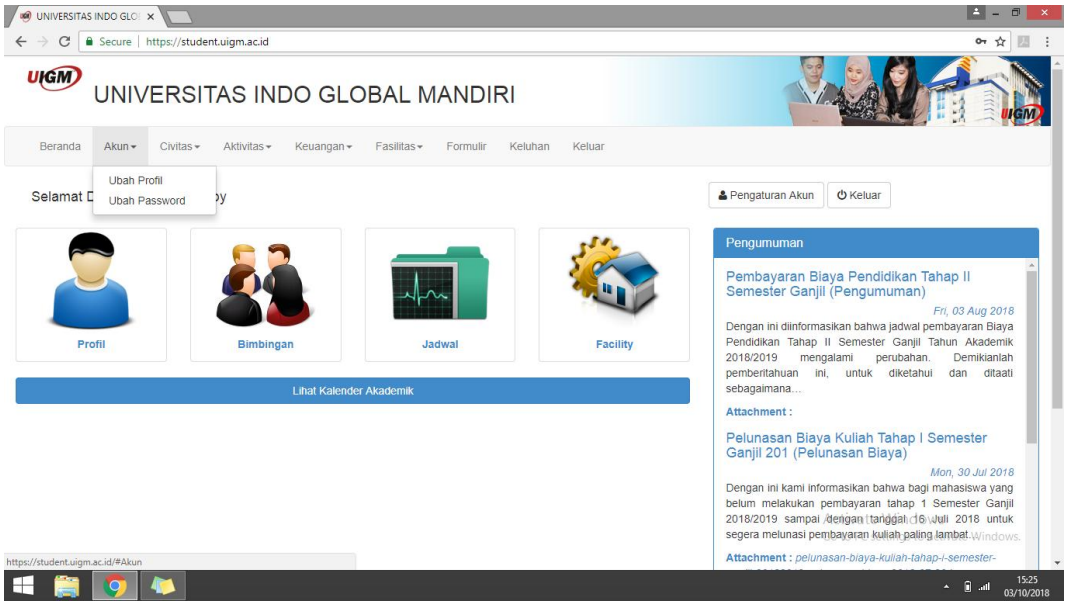
Gambar 4.7 hamanan menu aktivitas



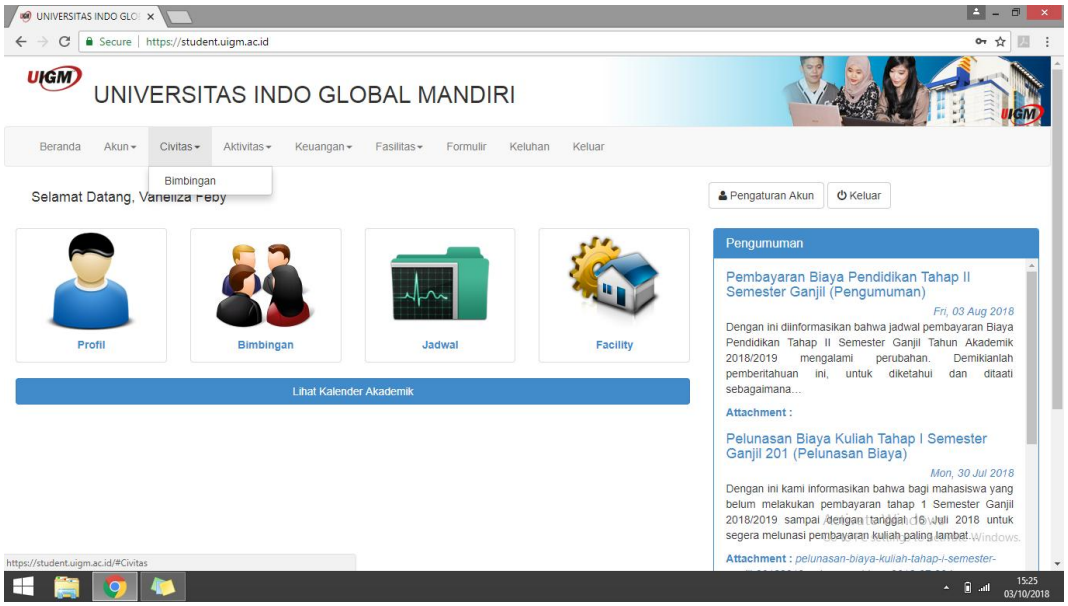
Gambar 4.8 halaman menu fasilitas



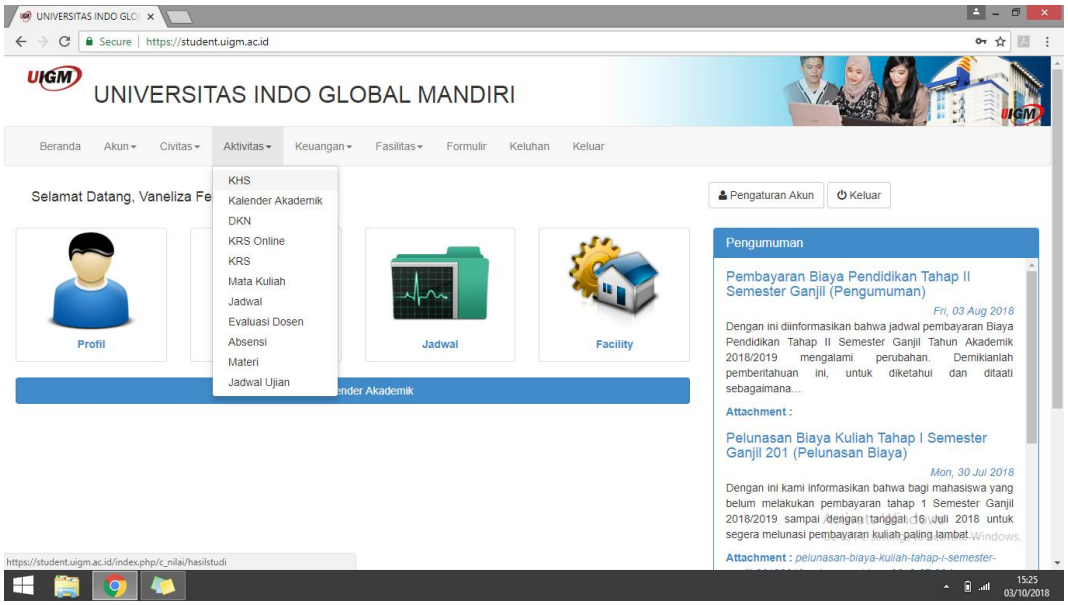
Gambar 4.8 tampilan utama menu login mahasiswa



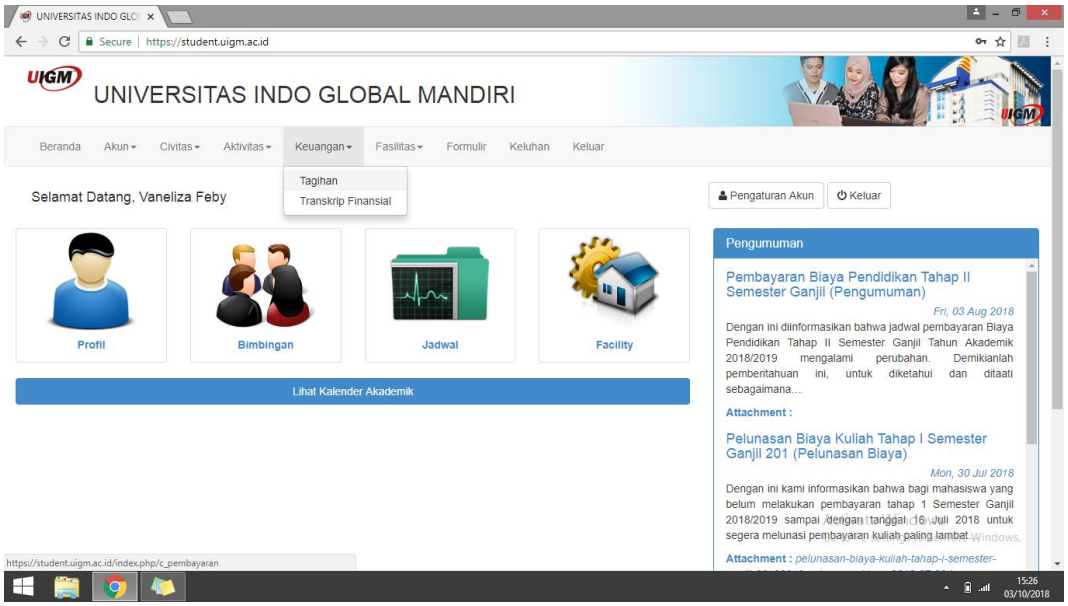
Gambar 4.9 tampilan sub menu akun



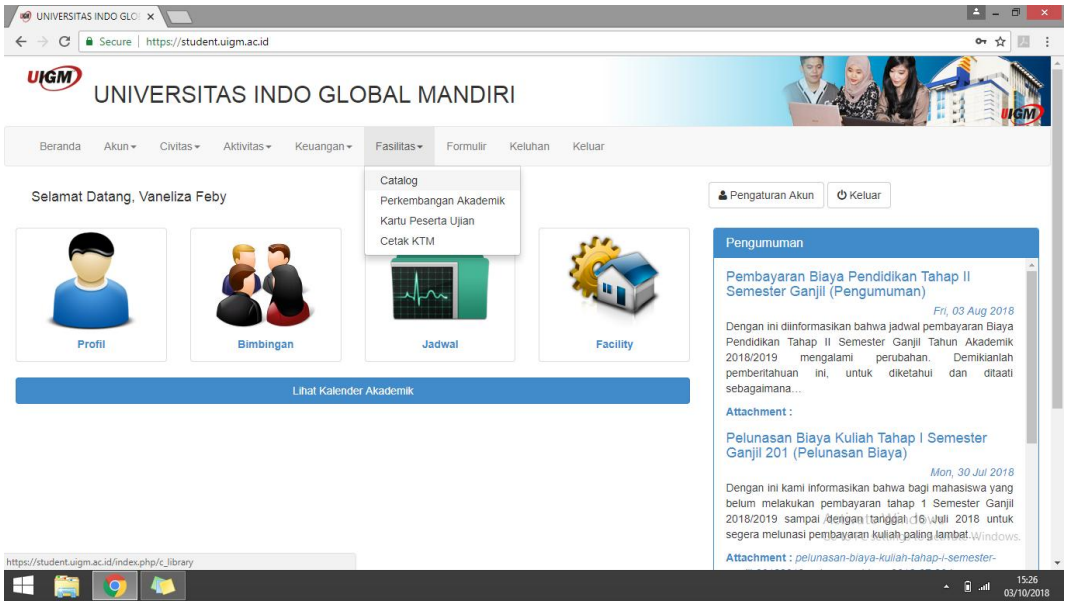
Gambar 4.10 sub menu civitas



Gambar 4.11 sub menu aktivitas mahasiswa

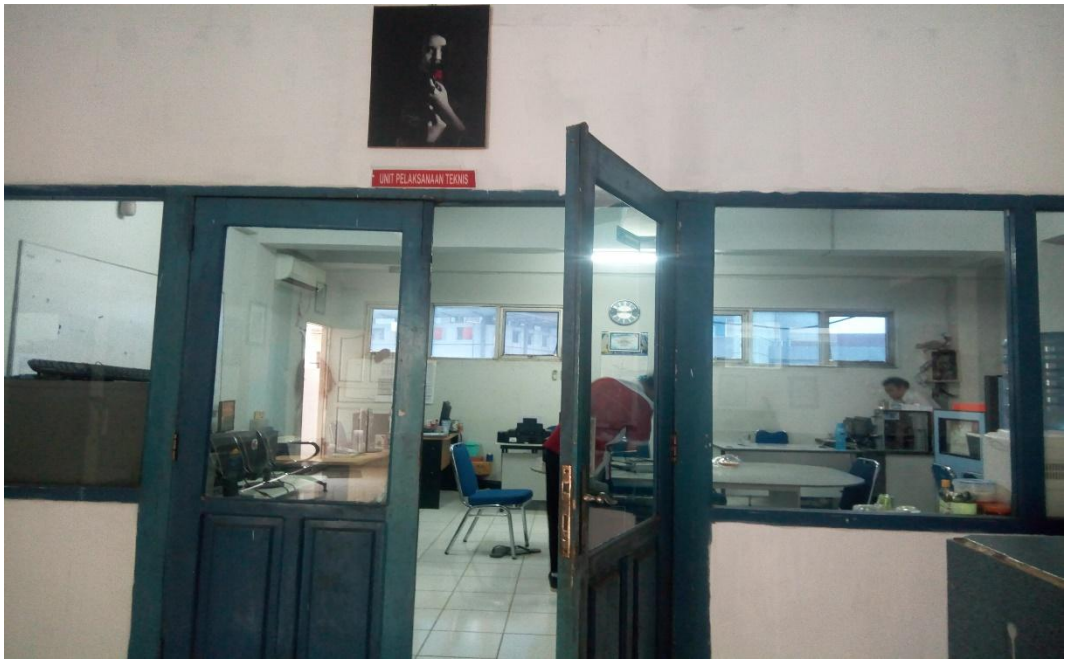


Gambar 4.12 sub menu keuangan



Gambar 4.13 sub menu fasilitas mahasiswa

Lampiran Dokumentasi



Ruangan Bagian Pelaksanaan Teknis. Dengan pintu yang belum difasilitasi dengan pengamanan kartu gesek atau PIN

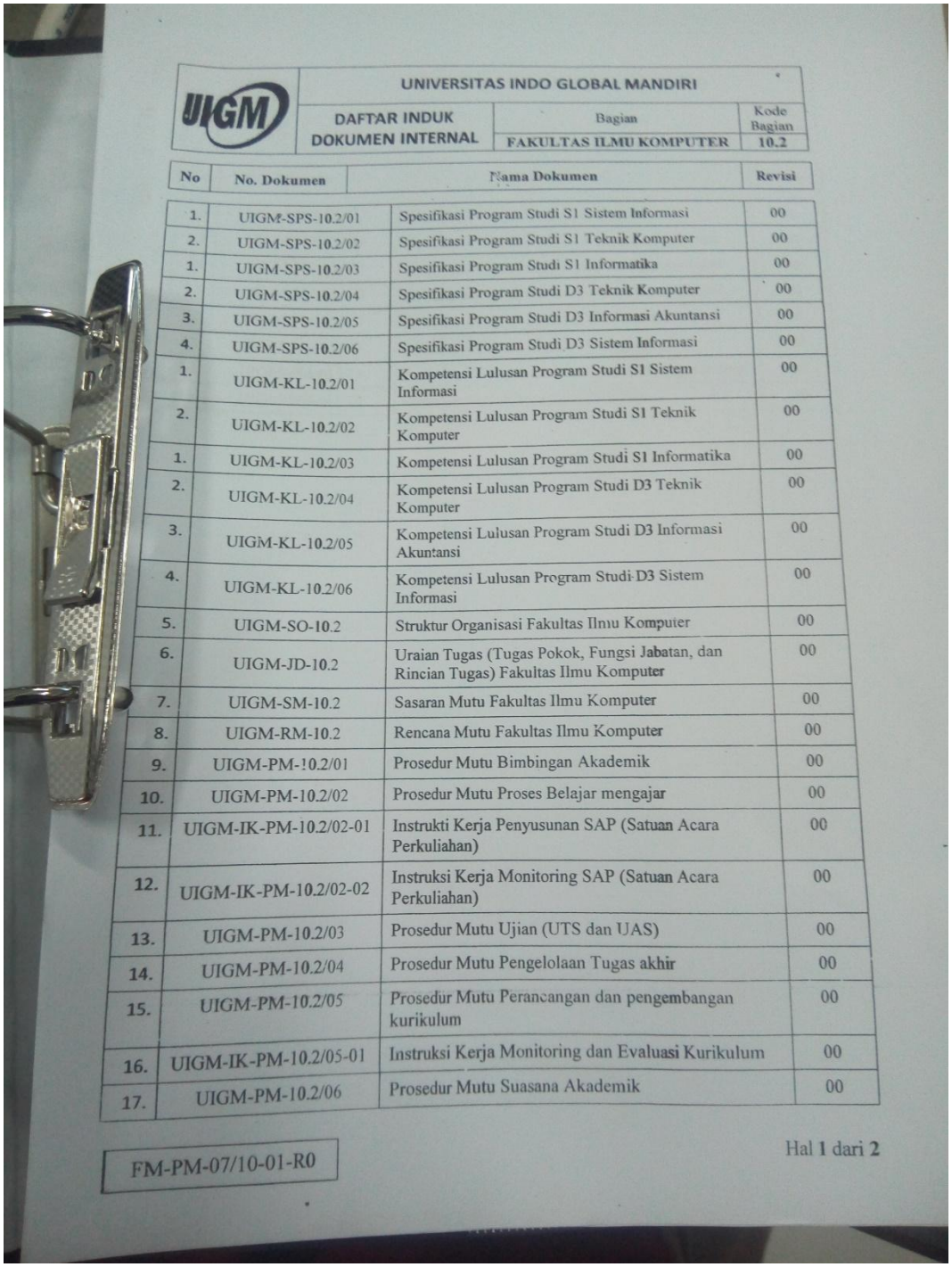
Kondisi ruangan, dengan aset teknologi dengan 8 PC dan kondisi ruangan yang tidak dibatasi dengan dinding atau bilik khusus untuk pengelolaan sistem informasi.

Kondisi ruangan pada bagian teknisi, hardware dan jaringan. Belum adanya pengamanan pada pintu masuk dengan kartu gesek atau PIN serta belum adanya pembatasan bilik khusus komputer untuk pengelolaan informasi.

Pemantauan komputer untuk CCTV tergabung ruangannya dengan penempatan server.

Penempatan server dan kabel yang telah disusun dan dilindungi dari catu daya

Tempat almari pengarsipan, dokumen prosedur dan kebijakan terkait organisasi.



UNIVERSITAS INDO GLOBAL MANDIRI

DAFTAR INDUK DOKUMEN INTERNAL | Bagian: FAKULTAS ILMU KOMPUTER | Kode Bagian: 10.2

No	No. Dokumen	Nama Dokumen	Revisi
1.	UIGM-SPS-10.2/01	Spesifikasi Program Studi S1 Sistem Informasi	00
2.	UIGM-SPS-10.2/02	Spesifikasi Program Studi S1 Teknik Komputer	00
1.	UIGM-SPS-10.2/03	Spesifikasi Program Studi S1 Informatika	00
2.	UIGM-SPS-10.2/04	Spesifikasi Program Studi D3 Teknik Komputer	00
3.	UIGM-SPS-10.2/05	Spesifikasi Program Studi D3 Informasi Akuntansi	00
4.	UIGM-SPS-10.2/06	Spesifikasi Program Studi D3 Sistem Informasi	00
1.	UIGM-KL-10.2/01	Kompetensi Lulusan Program Studi S1 Sistem Informasi	00
2.	UIGM-KL-10.2/02	Kompetensi Lulusan Program Studi S1 Teknik Komputer	00
1.	UIGM-KL-10.2/03	Kompetensi Lulusan Program Studi S1 Informatika	00
2.	UIGM-KL-10.2/04	Kompetensi Lulusan Program Studi D3 Teknik Komputer	00
3.	UIGM-KL-10.2/05	Kompetensi Lulusan Program Studi D3 Informasi Akuntansi	00
4.	UIGM-KL-10.2/06	Kompetensi Lulusan Program Studi D3 Sistem Informasi	00
5.	UIGM-SO-10.2	Struktur Organisasi Fakultas Ilmu Komputer	00
6.	UIGM-JD-10.2	Uraian Tugas (Tugas Pokok, Fungsi Jabatan, dan Rincian Tugas) Fakultas Ilmu Komputer	00
7.	UIGM-SM-10.2	Sasaran Mutu Fakultas Ilmu Komputer	00
8.	UIGM-RM-10.2	Rencana Mutu Fakultas Ilmu Komputer	00
9.	UIGM-PM-10.2/01	Prosedur Mutu Bimbingan Akademik	00
10.	UIGM-PM-10.2/02	Prosedur Mutu Proses Belajar mengajar	00
11.	UIGM-IK-PM-10.2/02-01	Instrukti Kerja Penyusunan SAP (Satuan Acara Perkuliahan)	00
12.	UIGM-IK-PM-10.2/02-02	Instruksi Kerja Monitoring SAP (Satuan Acara Perkuliahan)	00
13.	UIGM-PM-10.2/03	Prosedur Mutu Ujian (UTS dan UAS)	00
14.	UIGM-PM-10.2/04	Prosedur Mutu Pengelolaan Tugas akhir	00
15.	UIGM-PM-10.2/05	Prosedur Mutu Perancangan dan pengembangan kurikulum	00
16.	UIGM-IK-PM-10.2/05-01	Instruksi Kerja Monitoring dan Evaluasi Kurikulum	00
17.	UIGM-PM-10.2/06	Prosedur Mutu Suasana Akademik	00

FM-PM-07/10-01-R0

Hal 1 dari 2

Salah satu dokumentasi list dokumen, prosedur atau kebijakan yang telah di arsipkan

CURRICULUM VITAE

Nama	**: Yeni Rahayu**
Tempat, Tanggal lahir	**: Jember, 08 Desember 1996**
Jenis Kelamin	**: Perempuan**
Nama Ayah / Pekerjaan	**: Ngatiran / Wiraswasta**
Nama Ibu / Pekerjaan	**: Rumiati / Wiraswasta**
Alamat	**: Jl. Raya Kota Baru, Kelurahan Saung Dadi RT 02/RW 01, Martapura, Ogan Komering Ulu Timur Sumatera Selatan 32181**
No. HP	**: +6282179359221**
Email	**: riryrahayu08@gmail.com**
Riwayat Pendidikan	**:**
2002-2005	**: SDN NOGOSARI IX Rambi Puji, Jember, Jawa Timur**
2005-2007	**: SDN 1 Saung Dadi, Martapura, OKU TIMUR**
2007-2010	**: SMP N 3 Buay Pemuka Peliung, OKU TIMUR**
2010-2014	**: MAS AL-IKHLAS Pemetung Basuki, OKU TIMUR**
2014-2018	**: Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Raden Fatah Palembang**