

Dokumen Perencanaan Sistem Manajemen Keamanan Informasi Administrasi Akademik Berdasarkan ISO 27001:2013 Pada Bagian AAK Universitas Dinamika

Rico Kurniawan¹⁾ Erwin Sutomo²⁾ Vivine Nurcahyawati³⁾

Program Studi/Jurusan Sistem Informasi
Universitas Dinamika

Jl. Raya Kedung Baruk 98 Surabaya, 60298

Email : 1)15410100036@Dinamika.ac.id, 2)Sutomo@Dinamika.ac.id, 3)Vivine @Dinamika.ac.id

Abstract: Bagian Administrasi Akademik dan Kemahasiswaan (Bagian AAK) merupakan unit pendukung yang dimiliki oleh Universitas Dinamika. Pada kondisi saat ini, Bagian AAK masih memiliki kendala dari sisi manajemen dan operasional dalam penanganan keamanan informasi, yang dapat menimbulkan permasalahan terkait dengan *confidentiality* (kerahasiaan data yang dimiliki masih rentan untuk dapat diakses oleh pihak yang tidak bertanggung jawab), *Integrity* (keutuhan), dan *Availability* (ketersediaan) yang dapat mempengaruhi *business continuity*. Berdasarkan permasalahan di atas, dampak yang dapat ditimbulkan yaitu menurunnya kepercayaan mahasiswa dan pihak terkait dengan pelayanan yang diberikan oleh Bagian AAK. Untuk mengatasi dampak tersebut, maka dibutuhkan penyusunan dokumen terkait dengan perencanaan SMKI dengan menggunakan metode *Failure and Effect Analysis* (FMEA) yang berfungsi untuk menghitung dan mengidentifikasi efek dari dampak risiko terhadap aset jika terjadi pada instansi, sehingga Bagian AAK mampu menyediakan informasi administrasi akademik yang aman dalam sisi manajemen dan operasional. Hasil dari penelitian ini yaitu dokumen perencanaan SMKI, dokumen penyusunan kontrol objektif dan kontrol keamanan, dan dokumen SOP yang meliputi kebijakan keamanan informasi pada proses bisnis akademik, instruksi kerja dan rekam kerja. Dihasilkan beberapa pengelolaan di antaranya adalah pengelolaan *Human Resource Security*, pengelolaan keamanan fisik, pengelolaan kontrol akses, pengelolaan penanganan keamanan informasi, pengelolaan penggunaan *otentikasi*, pengelolaan keamanan pengguna, dan pengelolaan perangkat jaringan. Dengan tujuan, dapat membantu Bagian AAK dalam melakukan pengamanan terhadap aset-aset penting yang dimiliki oleh Bagian AAK, juga untuk menghindari adanya insiden terkait keamanan informasi yang disebabkan oleh faktor disengaja atau tidak disengaja dalam melakukan pengelolaan aset informasi atau hal-hal lain terkait dengan tata kelola informasi yang berada di lingkungan Bagian AAK.

Keyword : Bagian AAK, Keamanan Informasi, ISO 27001:2013

Universitas Dinamika adalah lembaga pendidikan yang bergerak di bidang teknologi informasi. Salah satu misi dari Universitas Dinamika yaitu membentuk Sumber daya manusia yang profesional, unggul, dan berkompetensi. Untuk mendukung misi tersebut, Universitas Dinamika memiliki unit kerja pendukung dalam bidang administrasi akademik yaitu Bagian Administrasi Akademik dan Kemahasiswaan (Bagian AAK).

Untuk meningkatkan kompetensi, terdapat dua layanan sesuai dengan analisis rantai nilai yaitu layanan utama dan pendukung. Layanan utama terdiri atas registrasi mahasiswa baru, perencanaan kuliah, perkuliahan, ujian dan penilaian, serta yudisium. Layanan pendukung

terdiri atas pengelolaan keuangan dan pengelolaan administrasi umum.

Untuk menunjang layanan tersebut, Bagian AAK berkoordinasi dengan beberapa unit kerja yaitu Bagian *Marketing*, Bagian Keuangan, Unit kerja Kemahasiswaan, Unit kerja Perpustakaan, Program Studi, Unit kerja Laboratorium, Unit kerja Administrasi Umum, dan unit kerja Pengembangan dan Penerapan Teknologi Informasi (PPTI). Keterkaitan Bagian AAK dengan unit kerja dan bagian lain tentunya memiliki aliran informasi yang penting, proses bisnis antara Bagian AAK dengan Bagian *Marketing* memiliki aliran informasi yang terdiri atas informasi biodata mahasiswa, dan informasi pendaftaran. Proses bisnis antara bagian AAK dengan bagian keuangan memiliki aliran

informasi yang terdiri dari informasi biaya pengembangan, informasi biaya operasional pengembangan, dan informasi biaya uang gedung. Proses bisnis antara Bagian AAK dengan unit kerja kemahasiswaan memiliki aliran informasi yang terdiri atas informasi kegiatan orientasi kehidupan dan kampus (OKK) serta beasiswa. Proses bisnis antara Bagian AAK dengan unit kerja perpustakaan memiliki aliran informasi yang terdiri atas informasi jadwal pengumpulan hasil kerja praktik dan tugas akhir. Proses bisnis antara Bagian AAK dengan program studi (*Prodi*) memiliki aliran informasi yang terdiri atas informasi yang berhubungan rencana perkuliahan. Pada unit studi meliputi dosen yang memiliki aliran informasi berupa rencana pembelajaran. Proses bisnis antara Bagian AAK dengan fakultas, memiliki aliran informasi yang terdiri atas informasi yang berhubungan dengan tugas akhir dan yudisium. Proses bisnis antara Bagian AAK dengan unit kerja laboratorium, memiliki aliran yang terdiri atas informasi rencana pelaksanaan praktikum. Proses bisnis antara Bagian AAK dengan unit kerja administrasi umum, memiliki aliran informasi yang terdiri atas informasi ketersediaan peralatan yang akan digunakan pada ruangan perkuliahan. Proses bisnis antara Bagian AAK dengan unit kerja PPTI, memiliki aliran informasi yang terdiri atas informasi penggunaan dan bantuan yang berkaitan dengan teknologi informasi. Selain aset informasi dan keterkaitan antara Bagian AAK dengan unit kerja lain, ada aset lain yang perlu dilindungi yaitu meliputi aset perangkat lunak yang terdiri dari *Sicyca*, Perwalian *online*, Presensi *online*, Penilaian *Online*, BSS & BST dan FORLAP. Yang kedua aset perangkat keras yang terdiri dari Server, *Personal Computer* (PC), *Printer*, *Scanner*, *FAX*. yang ketiga aset data yang terdiri dari data mahasiswa, data nilai, data dosen, data presensi. Dan yang terakhir adalah aset sumber daya manusia yang terdiri dari *Staff*. Kemudian keamanan informasi antara unit kerja dengan yang masih bertumpu pada unit kerja PPTI yang di mana bertugas sebagai pengembang teknologi informasi yang berada di universitas dinamika, sehingga jika ancaman dan kegagalan pada sistem, unit kerja atau bagian harus melaporkan kejadian tersebut ke unit kerja PPTI agar segera mendapatkan penanganan sesuai dengan prosedur yang sudah ada.

Pentingnya aset informasi dan keterkaitan antara Bagian AAK dengan unit kerja

lain, membuat keamanan informasi penting untuk dilakukan. Nilai sebuah informasi menyebabkan sering kali informasi hanya boleh diakses oleh orang tertentu. Pada kondisi saat ini, masih rendahnya penanganan terhadap keamanan informasi sehingga masih menimbulkan *Threat* (Ancaman) dan *Vulnerability* (Kelemahan) yang dapat mengakibatkan target tidak terpenuhi dan mempengaruhi *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan) dan *Availability* (Ketersediaan) yang akan berdampak pada *Business Continuity* (Sarno & Iffano, 2009).

Berdasarkan wawancara yang dilakukan dengan kepala Bagian AAK yaitu Ibu Sekar Dewanti A.Md, pada kondisi saat ini ditemukan adanya *Threat* (Ancaman) dan *Vulnerability* (Kelemahan) dari internal dan eksternal, yaitu : *Threat* (Ancaman) yang terjadi atas sisi eksternal yaitu serangan yang dilakukan oleh peretas (*Hacker*), di antaranya serangan *Distributed Denial of Service* (DDOS) yaitu terkait adanya laporan sistem yang secara tiba-tiba tidak tersedia atau *Down*. Kemungkinan terjadi serangan lain meliputi : virus *Ransomware*, Remote acces trojan, *Man in the middle attack*. *Vulnerability* (Kelemahan) yang terjadi dari sisi internal yaitu adanya celah keamanan pada sistem terkait dengan adanya laporan mengenai usaha perubahan nilai dan data absen secara paksa pada sistem Bagian AAK. Kemungkinan adanya kelemahan lain yang ada pada sistem meliputi *Sqlinjection*, *Cross site scripting*, *CSRF*, *Local file inclusion*, *Click jacking*, *Bypass Sql injection*.

Kemudian dampak yang dapat ditinjau dari sisi *Confidentiality* (Kerahasiaan) adalah data dan sandi yang digunakan oleh pegawai diketahui oleh pihak tidak bertanggung jawab. *Integrity* (Keutuhan) adalah data dan informasi yang disediakan oleh Bagian AAK menjadi tidak akurat. *Availability* (Ketersediaan) yaitu terkait dengan adanya laporan mengenai sistem yang tidak tersedia atau *Down*.

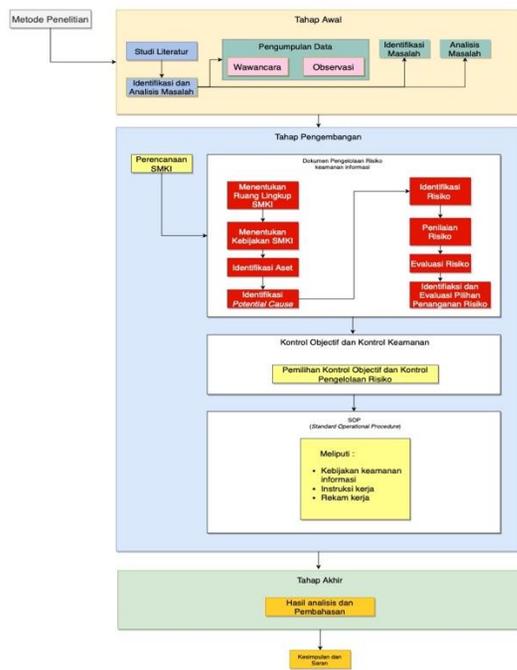
Berdasarkan fakta yang ditemukan pada kondisi saat ini, solusi yang sudah dilakukan AAK untuk menanggulangi ancaman, kelemahan dan dampak meliputi proses secara manajemen, yaitu : pengelolaan hak akses pengguna pada sistem yang digunakan oleh Bagian AAK. Solusi keamanan informasi yang ada saat ini, belum bisa memberikan perubahan yang signifikan terhadap penanganan keamanan informasi yang ada di Bagian AAK.

Mengingat pentingnya keamanan informasi yang dimiliki Bagian AAK, dukungan

yang diberikan terhadap pengendalian sistem manajemen keamanan informasi adalah penyusunan dokumen terkait dengan pengendalian keamanan informasi dan pembuatan dokumen *Standard Operational Procedure* (SOP). Dengan tujuan memberikan panduan atau pedoman kerja agar kegiatan dapat terkontrol dengan baik, dan terwujudnya target yang ingin dicapai secara maksimal. Penyusunan dokumen SOP menyesuaikan dengan kontrol objektif dan kontrol keamanan yang ada di *International Organization for Standardization* (ISO/IEC) 27001:2013. Hasil dari penelitian ini adalah berupa dokumen pengelolaan risiko yang berkaitan dengan keamanan informasi, dan dokumen SOP. Harapan dari penelitian ini adalah meningkatkan pengelolaan dan penanganan terkait dengan keamanan informasi di Bagian AAK Universitas dinamika.

METODOLOGI

Pada penelitian ini metode yang digunakan terbagi menjadi 3 (tiga) tahap, yaitu tahap awal, tahap pengembangan, dan tahap akhir. Untuk detail terkait dengan metodologi dan tiga tahap yang disebut kan dapat dilihat pada gambar 1.



Gambar 1 - Metode Penelitian

Pada tahapan awal yaitu melakukan studi literatur dan pengumpulan data yang

kemudian dilakukan proses identifikasi masalah dan analisis masalah guna menghasilkan data atau informasi yang dapat digunakan pada tahap selanjutnya yaitu tahap pengembangan.

Proses yang dilakukan pada tahap pengembangan adalah proses identifikasi aset, menentukan ruang lingkup dan menentukan kebijakan keamanan SMKI. Setelah proses tersebut selesai maka dilanjutkan ke proses pengelolaan risiko di mana ada proses identifikasi *potential cause* dengan menggunakan metode *Failure Mode And Effect Analysis* (FMEA) dengan tujuan mendapatkan hasil dari *Risk Priority Number* (RPN). setelah proses identifikasi *potential cause* maka dilanjutkan dengan proses identifikasi risiko, penilaian risiko serta identifikasi dan evaluasi pilihan penanganan risiko.

Pada proses selanjutnya adalah proses pemilihan kontrol objektif dan kontrol keamanan kemudian diteruskan dengan pembuatan dokumen SOP yang meliputi dokumen kebijakan, dokumen instruksi kerja dan dokumen rekam kerja. Pada tahap akhir berisikan kesimpulan dan saran mengenai penelitian yang sudah dilaksanakan.

HASIL DAN PEMBAHASAN

Tahapan Awal

Hasil dari tahapan awal ini adalah sebagai berikut :

- Proses bisnis dan layanan pada Bagian AAK
- Daftar aset yang dimiliki oleh Bagian AAK
- Ancaman dan kegagalan secara sistem maupun non sistem yang pernah terjadi di Bagian AAK
- Tindakan apa saja yang sudah di lakukan

Tahapan Pengembangan

Tahap pengembangan merupakan tahapan penyusunan dokumen pengelolaan risiko yang berisi kan proses identifikasi *potential cause*, identifikasi risiko, penilaian risiko, identifikasi dan evaluasi pilihan penanganan risiko.

Tabel 1 - Identifikasi *Potential Cause*

Aset	Ancaman	Kelemahan	<i>Potential Cause</i>	Asal
<i>Hardware</i>				
Server	Kurangnya prosedur pemeliharaan	Kerusakan pada media dan peralatan	Maintenance tidak dilakukan secara berkala	A,D
Komputer				
Printer	Kurangnya skema pergantian perangkat keras			
Scanner				
Fax				
Ups	Kerentanan terhadap debu dan kotoran	Perangkat eror secara tiba-tiba	Kerusakan fisik	A,D, E

Aset	Ancaman	Kelemahan	Potential Cause	Asal
	Hubungan arus pendek	Pasokan listrik hilang	Konsteling listrik	A,D,E
	Supply listrik tidak stabil	Pasokan listrik hilang	Pemadaman listrik	A,D,E
	Beban kerja server terlalu tinggi	AC mati atau rusak	Server Overheat	A
Data				
Data mahasiswa	Data terlalu sering di update	Redudansi data	Kesalahan input data dan hapus	A
Data nilai	Bermasalah pada saat backup	Data hilang	Prosedur backup gagal	A,E
Data dosen	Jaringan internet tidak optimal	Data rusak	Koneksi internet tidak stabil	D
Data presensi	Data yang dimasukkan terlalu banyak	Database penuh	Server Down	A
Aplikasi				
Sicyca	Lemahnya otentikasi pengguna	Sistem di akses orang tidak berwenang	Pergantian password tidak dilakukan secara berkala	A
Perwalian online	Kelemahan sistem diketahui orang lain	Penyalahgunaan hak akses	Staff mengetahui kelemahan sistem	A,D
Presensi online	Pengujian perangkat lunak masih kurang	Penyalahgunaan hak akses	Pergantian password tidak dilakukan secara berkala	A,D
Penilaian online	Kerentanan sistem	Data bocor ke pengguna umum	Pergantian password tidak dilakukan secara berkala	A,D
BSS & BST	Kerentanan sistem	Data bocor ke pengguna umum	Informasi tidak akurat	A
FORLAP	Kerentanan sistem	Data bocor ke pengguna umum	Informasi tidak akurat	A
Jaringan				
Jaringan	Arsitektur jaringan tidak aman	Celah untuk melakukan remote spying	Kurangnya keamanan sistem	A,D
	Manajemen jaringan kurang optimal	Jaringan LAN lambat	Kurangnya mekanisme pemantauan jaringan	A,D
	Bencana alam	Koneksi terputus	Kerusakan infrastruktur jaringan	A
	SDM tidak kompeten	Kesalahan konfigurasi IP	Kesalahan pada konfigurasi	A
	Kualitas jaringan buruk	Internet tidak stabil	Gangguan dari provider	A,D
Karyawan				
Karyawan	Kurangnya kesadaran akan keamanan informasi	Kesalahan pengguna	Kurangnya regulasi dan sanksi terhadap keamanan informasi	E,D
	Kurangnya mekanisme pemantauan	Pengolahan data ilegal	Pengolahan data ilegal yang dilakukan oleh karyawan	A,D

Setelah proses identifikasi *potential cause*, untuk detail dari hasil yang ada pada kolom asal adalah sebagai berikut :

- A = Tidak disengaja
- D = Disengaja
- E = Lingkungan

A digunakan untuk tindakan SDM yang tidak sengaja dapat merusak aset informasi, D digunakan untuk semua tindakan sengaja yang ditunjukkan ke aset informasi, E digunakan untuk insiden yang tidak didasarkan pada tindakan manusia.

Setelah proses identifikasi *potential cause* maka selanjutnya adalah proses penilaian risiko, detail dapat dilihat pada tabel 2.

Tabel 2 - Penilaian Risiko

RISIKO	POTENTIAL CAUSE	SEV	OCC	DET	RPN	LEVEL
Hardware Failure	Server Overheat	9	1	6	54	Low
	Maintenance kurang teratur	9	3	3	81	Low
	Kerusakan fisik pada Hardware	9	3	3	81	Low
Software Failure	Kesalahan program pada functional aplikasi	5	4	3	60	Low
Network Failure	Lemahnya keamanan pada sistem	6	4	5	120	High
	Kurangnya pemantauan terhadap jaringan	7	1	6	42	Low
	Gangguan dari pihak Provider	9	7	6	378	High
	Kabel digigit hewan	7	3	6	126	High
	Kesalahan pada saat melakukan konfigurasi Acces Point	7	4	6	168	High
Power Failure	Pemadaman listrik	9	7	6	378	High
Back up data failure	Server down	9	7	6	378	High
Human error	PC terkena virus	5	4	3	60	Low
	Staf tidak logout ketika meninggalkan komputer	6	5	4	120	high
	Kurangnya mekanisme pemantauan	4	3	5	60	Low
	Kesalahan pada saat input data dan hapus data	6	4	4	96	Low
Serangan hacker	Lemahnya keamanan pada sistem	6	4	5	120	High
Penyalahgunaan hak akses	Password tidak pernah diganti	6	4	5	120	High
Pencurian data dan informasi	Kurangnya pengamanan organisasi	6	4	4	96	Medium
	Kurangnya mekanisme pemantauan	4	3	5	60	Low
	Tidak ada peraturan terkait keamanan informasi	6	4	4	96	Low

RISIKO	POTENTIAL CAUSE	SEV	OCC	DET	RPN	LEVEL
Konsleting listrik	Kebakaran	9	1	6	54	Low
Modifikasi dan pencurian data	Staf mengetahui kelemahan pada sistem	9	1	5	45	Low
	Pengelolaan data ilegal	9	1	5	45	Low
Pelanggaran terhadap aturan dan regulasi	Kurangnya sosialisasi tentang regulasi dan sanksinya	5	4	4	80	Low

Penjelasan dari SEV, OCC, DET dan RPN adalah sebagai berikut :

- SEV = *Severity*
- OCC = *Occurence*
- DET = *Detection*
- RPN = *Risk Priority Number*

Kontrol objektif dan kontrol keamanan
Pemilihan kontrol objektif dan kontrol keamanan

Proses ini menjelaskan hasil dari penentuan kontrol objektif dan kontrol keamanan yang disesuaikan dengan hasil identifikasi *potential cause* dan identifikasi risiko, detail dapat dilihat pada tabel 3.

Tabel 3 - Pemetaan Kontrol Objektif Dan Kontrol Keamanan

Kategori aset	Potential cause	Risiko yang terjadi	Kontrol keamanan
Perangkat keras	Server error	Kurangnya pemantauan terhadap kinerja server	A.11.2.4 <i>Equipment maintenance</i>
	Kerusakan fisik	Minimnya pemantauan dan perawatan	
Perangkat lunak	Sistem di akses oleh orang yang tidak memiliki wewenang	Username dan password diketahui oleh orang yang tidak memiliki wewenang	A.9.1.1 <i>Access control policy</i> A.9.4.1 <i>Information access restriction</i>
		Sistem memiliki celah keamanan yang tidak diperbaiki	A.9.4.2 <i>Secure log-on procedures</i> A.9.4.3 <i>Password management system</i> A.10.1.2 <i>Key management</i>
Informasi	Kesalahan pada informasi yang disampaikan	Adanya kesalahan pada penyampaian informasi yang di akibatkan oleh <i>human error</i>	A.5.1.1 <i>Policies for information security</i> A.5.1.2 <i>Review of the policies for information security</i>

Kategori aset	Potential cause	Risiko yang terjadi	Kontrol keamanan
Data	Data corrupt	Adanya kelalaian pada peran dan tanggung jawab dalam menyampaikan informasi	A.6.1.1 <i>Information security roles and responsibility</i>
		Kurangnya pemantauan dan adanya kelalaian seorang teknisi	A.9.1.1 <i>Access control policy</i> A.9.3.1 <i>Use of secret authentication information</i> A.12.4.3 <i>Administrator and operator logs</i>
	Data corrupt	Perangkat penyimpanan rusak	A.12.3.1 <i>Information backup</i> A.11.2.4 <i>Equipment maintenance</i>
	Data hilang	Username dan password diketahui oleh orang luar	A.9.2.3 <i>Management of privileged access rights</i> A.9.4.2 <i>Secure log-on procedures</i> A.9.4.3 <i>Password management system</i>
Jaringan	Remote spying	Kesalahan konfigurasi	A.13.1.1 <i>Network controls</i>
SDM	Tidak melakukan prosedur log-out pada saat meninggalkan komputer	Kelalaian staf yang memiliki wewenang pada sistem	A.7.1.2 <i>Term and condition of employment</i> A.7.2.2 <i>Information security awareness, education and training</i>
			A.9.1.1 <i>Access control policy</i>
	Data tidak valid	Kesalahan pada saat input data	A.12.4.1 <i>Event logging</i> A.12.4.2 <i>Protection of log information</i>

Standart operational procedure (SOP)

Pada proses ini menghasilkan dokumen kebijakan yang diambil dari proses pemetaan kontrol objektif dan kontrol keamanan, yang terdiri dari dokumen kebijakan, instruksi kerja

dan rekam kerja. Hasil pemetaan antara kebijakan dan risiko dapat dilihat pada tabel 4.

Tabel 4 - Pemetaan Risiko Dengan Kebijakan

Kategori aset	Risiko yang terjadi	Kategori kebutuhan	Kontrol keamanan	Dokumen kebijakan
Perangkat keras	Kurangnya pemantauan terhadap kinerja server	Teknikal	A.11.2.4 Equipment maintenance	KB - 02 Kebijakan keamanan fisik
	Minimnya pemantauan dan perawatan			
Perangkat lunak	Username dan password diketahui oleh orang yang tidak memiliki wewenang	Teknikal	A.9.1.1 Access control policy	KB - 03 Kebijakan kontrol akses
	Sistem memiliki celah keamanan yang tidak diperbaiki			
Informasi	Adanya kesalahan pada penyampaian informasi yang di akibatkan oleh human eror Adanya kelalaian pada peran dan tanggung jawab dalam menyampaikan informasi	Manajemen	A.5.1.1 Policies for information security	KB - 04 Kebijakan penanganan keamanan informasi
			A.5.1.2 Review of the policies for information security	
			A.6.1.1 Information security roles and responsibility	
			A.13.2.1 information transfer and procedures	
Data	Kurangnya pemantauan dan adanya kelalaian seorang teknisi	Teknikal	A.9.1.1 Access control policy	KB - 03 Kebijakan kontrol akses
			A.9.3.1 Use of secret authentication information	
	Perangkat penyimpanan rusak	Operational	A.12.4.3 Administrator and operator logs	KB - 01 Human resource security
			A.12.2.1	

Kategori aset	Risiko yang terjadi	Kategori kebutuhan	Kontrol keamanan	Dokumen kebijakan
			Controls against malware	
			A.12.3.1 Information backup	
		Teknikal	A.11.2.4 Equipment maintenance	KB - 03 Kebijakan kontrol akses
			A.9.2.3 Management of privileged access rights	
Jaringan	Remote spying	Teknikal	A.9.4.2 Secure log-on procedures	KB - 04 Kebijakan penanganan perangkat jaringan
			A.9.4.3 Password management system	
			A.13.1.1 Network controls	
SDM	Kelalaian staf yang memiliki wewenang pada sistem	Teknikal	A.9.1.1 Access control policy	KB - 03 Kebijakan kontrol akses
			A.9.3.1 Use of secret authentication information	
	Kesalahan pada saat input data	Operational	A.12.4.3 Administrator and operator logs	KB - 05 Kebijakan penggunaan otentikasi
			A.7.1.2 Term and condition of employment	
			A.7.2.2 Information security awareness, education and training	KB - 01 Human resource security
			KB - 06 Kebijakan keamanan pengguna	

Untuk penjelasan dari warna tabel merupakan kategori untuk membedakan antara aset satu dengan yang lain, untuk detailnya adalah sebagai berikut :

- Warna biru = perangkat keras
- Warna hijau = perangkat lunak
- Warna orange = Informasi
- Warna kuning = Data
- Warna merah = jaringan
- Warna pink = SDM

KESIMPULAN

Berdasarkan hasil dari penyusunan tugas akhir yang didapatkan dari penelitian ini dan sudah disesuaikan dengan metode yang sudah direncanakan, menghasilkan kesimpulan sebagai berikut :

1. Pada penyusunan tahap perencanaan SMKI dihasilkan beberapa proses yang terdiri dari menentukan ruang lingkup SMKI, menentukan kebijakan SMKI, Identifikasi aset, identifikasi *potential cause*, identifikasi risiko, penilaian risiko, identifikasi dan evaluasi penanganan risiko. Setelah dilakukan penyusunan tahap pengembangan, selanjutnya adalah menyusun dokumen kontrol objektif dan kontrol keamanan yang digunakan untuk mendukung penyusunan dokumen SOP yang terdiri atas kebijakan, instruksi kerja, rekam kerja.
 2. Pada tahap penyusunan kontrol objektif dan kontrol keamanan, dihasilkan beberapa kebutuhan keamanan informasi, pemilihan kontrol objektif dan kontrol keamanan menyesuaikan dengan hasil dari tahap pengembangan yang sudah dilakukan, yaitu dengan melakukan pemetaan terhadap risiko dengan kontrol objektif dan kontrol keamanan. Sehingga menghasilkan delapan kontrol dari sisi *teknikal*, lima kontrol dari sisi manajemen dan delapan kontrol dari sisi operasional. Kemudian hasil dari kontrol ini akan digunakan untuk pemetaan dari hasil perencanaan SMKI dan digunakan pada tahap penyusunan dokumen SOP.
 3. Pada tahap penyusunan dokumen SOP dihasilkan dokumen perencanaan SOP yang meliputi kebijakan keamanan informasi pada proses bisnis akademik, yang di dalamnya berisi instruksi kerja (IK) yang terdiri atas instruksi kerja penanganan fisik hardware, instruksi kerja pengolahan hak akses, instruksi kerja pengolahan kerentanan sistem, instruksi kerja klasifikasi keamanan informasi, instruksi kerja peran dan tanggung jawab, instruksi kerja backup dan restore data. Rekam kerja (RK) pemantauan kondisi perangkat keras, berita acara kerusakan, rekam kerja laporan penggunaan TI, rekam kerja log penggunaan hak akses, rekam kerja pelaporan kerentanan, rekam kerja pemantauan dan monitoring keamanan informasi, rekam kerja reset password, rekam kerja pemeliharaan perangkat keras jaringan, rekam kerja evaluasi kegiatan pelatihan.
- Djohanputro, B. (2008). *Manajemen Risiko Korporat. Pendidikan dan Pembinaan Manajemen*. Jakarta.
- Forum, I. I. (2009). *Guideline for Information Asset Valuation*. ISO27k Implementer's Forum.
- Hanafi, M. (2006). *Manajemen Risiko*. Yogyakarta: Unit Penerbit dan Percetakan Sekolah Tinggi Ilmu Manajemen YKPN.
- Hughes, G. (2006). *Five Steps to IT Risk Manejement Best Practices*.
- Indonesia, P. M. (2012). *Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan*, .
- ISO/IEC 27001. (2013). *Information Technology-Security Techniques-Information Security Management System-Requirements*. ISO/IEC.
- Peraturan Menteri Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi Republik Indonesia. (2012). *Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan*.
- Sarno, R., & Iffano, I. (2009). *Sistem Manajemen Keamanan Informasi berbasis ISO 27001*. Surabaya: ITSPress.

RUJUKAN