JURNAL PETIR
Vol. 11, No. 2, September 2018, P-ISSN 1978-9262, E-ISSN 2655-5018

IMPLEMENTASI OCTAVE-S DAN STANDAR PENGENDALIAN ISO 27001:2013 PADA MANAJEMEN RISIKO SISTEM INFORMASI PERGURUAN TINGGI

Rima Rizqi Wijayanti

Fakultas Teknik Informatika, Universitas Muhammadiyah Tangerang
rimarizqiwijayanti@gmail.com

ABSTRAK

Pada perguruan tinggi sistem informasi menjadi alat bantu strategis bagi kelangsungan perguruan tinggi atau Lembaga itu sendiri khususnya pada proses bisnis yang berjalan. Terganggunya sistem informasi pada perguruan tinggi akan memberikan dampak yang buruk terutama bagi kelangsungan proses bisnis, sistem informasi yang semula sebagai alat bantu akan berubah menjadi ancaman bahkan menjadi risiko apabila tidak diperhatikan dan dimitigasi dengan baik. Masalah yang muncul adalah Universitas Muhammadiyah Tangerang belum pernah melakukan penilaian analisis risiko sistem Informasi yang ada, termasuk kebijakan yang berkaitan dengan keamanan teknologi informasi. Penelitian ini bertujuan memberikan informasi kepada Universitas Muhammadiyah Tangerang mengenai risiko-risiko, ancaman, serta kelemahan teknologi informasi yang ditemukan serta rekomendasi-rekomendasi yang dapat diterapkan untuk memitigasi risiko yang dapat muncul. Penelitian ini menggunakan metode analisa resiko octave-s yang dikombinasikan dengan standar pengendalian ISO 27001:2013. Hasil dari penelitian ini berupa dokumen akhir yang dapat dijadikan sebagai pedoman dan membantu dalam pengembangan penilaian analisis risiko di UMT kedepannya. Hasil evaluasi yang didapatkan, diketahui bahwa manajemen risiko berada pada posisi SEDANG, artinya UMT tidak mengalami risiko yang dapat menghentikan / merusak sistem informasi yang berdampak pada berhentinya proses belajar mengajar, namun risiko dan kelemahan pada universitas dapat berdampak pada menurunnya kinerja universitas jika tidak ditangani dengan segera.

Kata Kunci : *risiko, manajemen risiko, mitigasi risiko, OCTAVE-S, ISO 27001/2013*

ABSTRACT

In higher education, information systems become a strategic tool for the continuity of universities or institutions themselves, especially in the running business processes. The disruption of information systems in higher education will have a bad impact, especially for the continuity of business processes, information systems that initially as a tool will then turn into a threat and even become a risk if it is not properly addressed and mitigated. The problem that arises is that University of Muhammadiyah Tangerang has never conducted a system risk analysis assessment of existing information, including policies relating to information technology security. This study aims to provide information to the University of Muhammadiyah Tangerang regarding the risks, threats and weaknesses of information technology found and recommendations that can be applied to mitigate risks that can arise. This study uses the octave-s risk analysis method combined with ISO 27001: 2013 control standards. The results of this study are in the form of a final document that can be used as a guideline and help in the future development of a risk analysis assessment at UMT. The results of the evaluation obtained, it is known that risk management is in the MEDIUM position, meaning that UMT does not experience risks that can stop / damage information systems that have an impact on the cessation of teaching and learning, but risks and weaknesses in universities can have an impact on decreasing university performance immediately.

Keywords : *risk, risk management, risk mitigation, OCTAVE-S, ISO 27001/2013*

PENDAHULUAN

Universitas Muhammadiyah Tangerang memiliki suatu sistem informasi yang hingga saat ini belum pernah dilakukan penilaian analisis resiko, serta minimnya kebijakan yang jelas berkaitan dengan keamanan teknologi informasi, sehingga Universitas Muhammadiyah Tangerang tidak tahu pasti sampai sejauh mana kesiapan universitas dalam menghadapi ancaman – ancaman yang mungkin muncul saat resiko – resiko yang sebenarnya ada tidak teridentifikasi dengan baik, semakin lama celah keamanan dibiarkan tanpa adanya pengendalian yang tepat, maka sangat besar kemungkinan terjadi kekacauan yang akan ditimbulkan dari pihak internal maupun eksternal.

Sehingga dengan dilakukannya penelitian ini diharapkan dapat memberikan pemahaman akan pentingnya analisis risiko bagi universitas dan kaitannya dengan bisnis organisasi. Membantu Universitas Muhammadiyah Tangerang dengan memberikan informasi kepada organisasi mengenai risiko-risiko, ancaman, serta kelemahan teknologi informasi yang ditemukan. Membantu memberikan solusi dalam melindungi aset-aset informasi universitas, dalam bentuk rekomendasi-rekomendasi yang dapat diterapkan oleh Universitas Muhammadiyah Tangerang.

LANDASAN TEORI

Manajemen Risiko

Stoneburner, Goguen, & Feringa (2002) dari *National Institute of Standards and Technology* (NIST) menyatakan bahwa manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan antara biaya operasional dan biaya ekonomi, dari langkah-langkah protektif untuk mencapai keuntungan, sesuai dengan misi universitas, dengan melindungi sistem TI dan data yang mendukung misi organisasi mereka.

OCTAVE

Komponen penting *OCTAVE* adalah tim penganalisa dapat dibangun dari internal universitas itu sendiri yang memiliki keterampilan teknis serta keterampilan organisasi yang terkait dengan praktek – praktek bisnis (Coleman, 2004). Pendekatan *OCTAVE* didasari pada dua aspek :

1) Risiko Operasional
2) Praktek – praktek keamanan

Tabel 1. Perbedaan utama antara *OCTAVE* dan pendekatan lain.
(Alberts, Dorofee, Stevens, & Woody, 2005)

OCTAVE	**Metode Lain**
Evaluasi terhadap organisasi	Evaluasi terhadap sistem
Fokus pada praktek – praktek keamanan	Fokus pada teknologi
Mengedepankan permasalahan strategis	Mengedepankan permasalahan taktis
Dapat dilakukan oleh internal maupun eksternal.	Dilakukan oleh ahli eksternal universitas

OCTAVE-S

OCTAVE-S merupakan variasi dari *OCTAVE* yang digunakan untuk melakukan evaluasi terhadap universitas kecil, yang memiliki struktur hirarki organisasi yang sedikit, atau memenuhi kriteria sebagai berikut :

a. Fungsi – fungsi teknologi informasi dilakukan secara *outsource*.
b. Memiliki infrastruktur teknologi informasi yang relatif sederhana yang dapat dimengerti paling tidak oleh satu orang dalam organisasi.
c. Keterbatasan pemahaman mengenai alat yang dapat digunakan untuk evaluasi risiko terhadap aset informasi.

d. Organisasi lebih menyukai metode yang sangat terstruktur dibandingkan metode terbuka yang dapat lebih mudah disesuaikan.

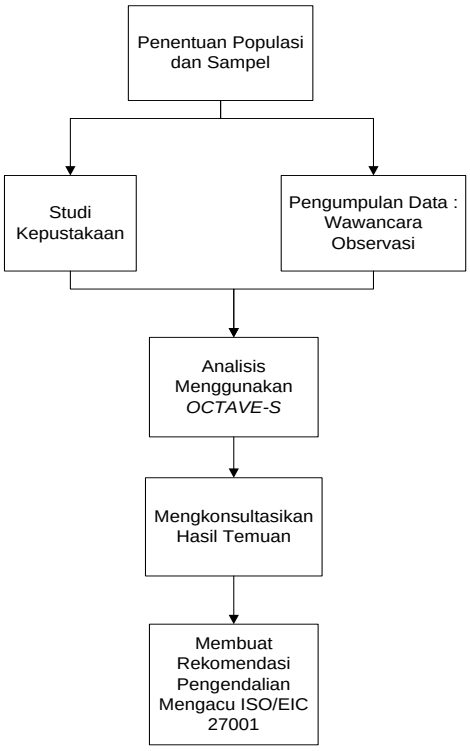
ISO/EIC 27001:2013

ISO/EIC 27001:2013 merupakan standar Internasional yang dipersiapkan untuk memberikan model untuk membangun, mengimplementasikan, mengoperasikan, memonitor, serta merawat dan mengembangkan sistem manajemen keamanan informasi (SMKI), termasuk didalamnya unsur – unsur seperti orang, proses dan sistem TI dengan menerapkan proses manajemen risiko. (ISO & EIC, 2013).

ISO/EIC 27001:2013 adalah versi terbaru dari ISO 27001 yang diterbitkan pada tanggal 1 Oktober 2013 lalu. Versi ini merupakan pembaharuan dari versi sebelumnya, yaitu versi 2005. Banyak penyempurnaan yang telah dilakukan pada versi terbaru ini, tujuannya adalah agar lebih mudah diimplementasikan serta diintegrasikan dengan sistem manajemen berbasis ISO lainnya (misalnya ISO 22301 untuk *Business Continuity Management*, ISO 20000 untuk IT *Service Management*, dan sebagainya). ISO 27001:2013 terdiri atas 14 klausul manajemen dan 113 kontrol yang harus diterapkan berdasarkan analisis risiko keamanan informasi.

METODE PENELITIAN

Kerangka pemikiran ini merupakan tahap-tahap yang dilakukan dalam melakukan penelitian. Adapun garis besar dari kerangka pmikiran ini akan digambarkan secara umum dalam diagram berikut:



Gambar 1. Kerangka Pemikiran

HASIL DAN PEMBAHASAN

1. Membangun aset berbasis profil ancaman.

Universitas Muhammadiyah Tangerang saat ini memiliki reputasi yang baik. Hal ini dapat dilihat dari penambahan jumlah mahasiswa dari tahun 2011 sampai 2013 sebesar 48,5 persen per tahun. Ini membuktikan bahwa terdapat kepuasan mahasiswa terhadap layanan yang selama ini

diberikan UMT. Namun di tahun 2014 sampai 2016 terjadi penurunan mahasiswa yang mencapai 1,6 persen per tahun.

Tabel 2. Rekapitulasi Jumlah Mahasiswa

	2011	**2012**	**2013**	**2014**	**2015**	**2016**
Jumlah Mahasiswa Baru	2,066	2,827	4,536	4,962	5,413	4,713
Persentase Peningkatan Mhs Pertahun		37%	60%	9%	9%	-13%

2. Mengidentifikasi aset-aset informasi universitas

Pada aktivitas yang kedua ini, dilakukan identifikasi aset-aset informasi yang dimiliki oleh Universitas Muhammadiyah Tangerang, dibagi dalam tiga kategori aset, kategori informasi, sistem, dan aplikasi-aplikasi , Hardware (Perangkat Keras) ,dan *people*(karyawan)

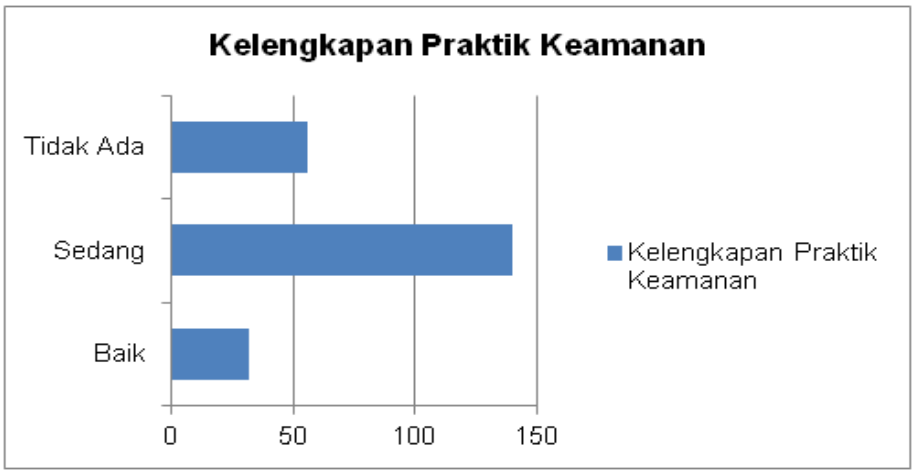
3. Mengevaluasi keamanan universitas yang telah berjalan

Tabel 3. Kesimpulan Hasil Kuesioner 15 Praktek Keamanan

Praktek Keamanan	**RESUME**		
	BAIK	**SEDANG**	**TIDAK ADA**
1. Kesadaran Keamanan dan Pelatihan			
Jumlah	0	12	4
Persentase	**0%**	**75%**	**25%**
STOPLIGHT	**YELLOW**		
2. Strategi Keamanan			
Jumlah	0	4	8
Persentase	**0%**	**33%**	**67%**
STOPLIGHT	**RED**		
Praktek Keamanan	**RESUME**		
	BAIK	**SEDANG**	**TIDAK ADA**
3. Manajemen Keamanan			
Jumlah	0	24	4
Persentase	**0%**	**86%**	**14%**
STOPLIGHT	**YELLOW**		
4. Kebijakan Keamanan dan Peraturan			
Jumlah	0	12	4
Persentase	**0%**	**75%**	**25%**
STOPLIGHT	**YELLOW**		
5. Manajemen Keaman dan Kolaboratif			
Jumlah	0	8	8
Persentase	**0%**	**50%**	**50%**
STOPLIGHT	**YELLOW**		
6. Rencana Kemungkinan atau pemulihan dari Bencana			

Jumlah	0	16	0
Persentase	**0%**	**100%**	**0%**
STOPLIGHT		**YELLOW**	
7. Pengendalian Akses Fisik			
Jumlah	0	12	4
Persentase	**0%**	**75%**	**25%**
STOPLIGHT		**YELLOW**	
8. Pemantauan dan audit keamanan fisik			
Jumlah	8	0	4
Persentase	**67%**	**0%**	**33%**
STOPLIGHT		**GREEN**	
9. Sistem dan Manajemen Jaringan			
Jumlah	12	16	8
Persentase	**33%**	**44%**	**22%**
STOPLIGHT		**YELLOW**	
10. Pemantauan dan audit keamanan IT			
Jumlah	0	8	0
Persentase	**0%**	**100%**	**0%**
STOPLIGHT		**YELLOW**	
11. Pengesahan dan Otorisasi			
Jumlah	0	8	4
Persentase	**0%**	**67%**	**33%**
STOPLIGHT		**YELLOW**	

Berdasarkan kuesioiner yang diberikan kepada empat orang responden yang merupakan karyawan yang bertanggung jawab langsung terhadap manajemen teknologi informasi yang ada di Univeritas Muhammadiyah Tangerang didapatkan hasil seperti gambar 4.5 mengenai kelengkapan praktik keamanan secara keseluruhan dibawah ini.



Gambar 2. Kelengkapan Praktik Keamanan Keseluruhan

4. Mengidentifikasi kebutuhan keamanan aset-aset penting

Dari lima aset yang dimiliki universitas ditentukanlah aset – aset yang paling penting diantara aset-aset yang ada tersebut, dan didapatkanlah dua aset yang paling penting, yaitu SIAKAD dan Komputer Server, disisi lain kebutuhan keamanan terhadap seluruh aset–aset penting universitas dikategorikan dalam 3 hal: *Confidentiality, Integrity, Availability*, dan kebutuhan keamanan dari tiap aset berbeda beda namun lebih cenderung untuk memilih availability, dikarena jika data atau informasi yang diperlukan tidak ada, maka proses bisnis universitas tidak dapat berjalan.

5. Mengidentifikasi ancaman-ancaman terhadap aset-aset penting

Tabel dibawah menggambarkan rata-rata frekuensi ancaman yang terjadi untuk setiap aset penting pertahun.

Tabel 4. Frekuensi ancaman terhadap asset SIAKAD

SIAKAD					
Sumber Ancaman	**Motif**	**Frekuensi Ancaman/Tahun**			
		Penyingkapan	**Modifikasi**	**Data Hilang**	**Interupsi**
Internal	Tidak Sengaja	8	7	4	0
	Sengaja	10	1	0	20
Ekxternal	Tidak Sengaja	0	0	0	0
	Sengaja	0	0	0	10
Total		**18**	**8**	**4**	**30**

Tabel 5. Frekuensi ancaman terhadap asset Komputer Server

KOMPUTER SERVER					
Sumber Ancaman	**Motif**	**Frekuensi Ancaman/Tahun**			
		Penyingkapan	**Modifikasi**	**Data Hilang**	**Interupsi**
Internal	Tidak Sengaja	0	5	5	5
	Sengaja	10	1	0	20
Ekxternal	Tidak Sengaja	0	0	0	0
	Sengaja	0	0	0	25
Total		**10**	**6**	**5**	**50**

6. Membuat rencana mitigasi risiko

Pada tahap ini dibuatnya rencana mitigasi risiko dengan mengambil kontrol – kontrol pengendalian yang terdapat pada ISO 27001:2013 sebagaimana terdapat pada tabel 6 di bawah ini :

Tabel 6. Rencana Mitigasi Risiko

ANCAMAN	ASPEK	PENGENDALIAN ISO 27001:2013	PERENCANAAN	IMPLEMENTASI	RENCANA EVALUASI
1. Organisasi tidak menjadikan pelatihan kesadaran keamanan kepada karyawan sebagai kegiatan yang harus dilakukan dan didokumentasikan.	Kesadaran keamanan dan pelatihan.	1. Semua karyawan organisasi dan, bila relevan, kontraktor dan pengguna pihak ketiga harus menerima pelatihan kesadaran yang tepat dan update reguler mengenai prosedur dan kebijakan organisasi, sebagai bagian dari fungsi pekerjaan mereka.(A.7.2.2)	1. Pembuatan peraturan dan sangsi, yang harus ditandatangai oleh manajemen tertinggi.	Diberlakukan setelah setidaknya Wakil Rektor II, menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	Periodik 2 x dalam satu tahun
2. Belum adanya strategi dan kebijakan kamanan yang dimasukan kedalam pertimbangan strategi bisnis dan tujuan universitas.	Strategi Keamanan	2. Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan direview berdasarkan kebutuhan keamanan bisnis dan informasi.(A.9.1.1)	1. Pembuatan peraturan dan sangsi, yang harus ditandatangai oleh manajemen tertinggi. 2. Pembuatan prosedur operasi berkaitan dengan strategi, tujuan dan sasaran keamanan.	Diberlakukan setelah setidaknya Wakil Rektor II, menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	
3. Belum adanya dokumentasi mengenai strategi, tujuan dan sasaran keamanan yang ditinjau secara rutin, yang terus diperbaharui dan dikomunikasikan ke seluruh civitas akademik kampus.		3. Prosedur Operasi harus didokumentasikan dan dapat tersedia kepada siapa saja yang membutuhkan. (A.12.1.1) 4. Perubahan organisasi, proses bisnis, pengolahan informasi fasilitas dan sistem yang mempengaruhi keamanan informasi harus dikontrol. (A.12.1.2)			Periodik 2 x dalam satu tahun

Tabel 6. (Lanjutan)

ANCAMAN	ASPEK	PENGENDALIAN ISO 27001:2013	PERENCANAAN	IMPLEMENTASI	RENCANA EVALUASI
4. Belum ada prosedur terdokumentasi yang mengatur otorisasi semua staf yang bekerja dengan informasi sensitif atau bekerja dilokasi dimana informasi tersebut berada.	Manajemen Keamanan	5.Prosedur Operasi harus didokumentasikan dan dapat tersedia kepada siapa saja yang membutuhkan. (A.12.1.1)	1. Pembuatan prosedur operasi yang mengatur otorisasi semua staf yang bekerja dengan informasi sensitif atau bekerja di lokasi dimana informasi tersebut berada. 2. Sosialisasi SOP yang telah disetujui	Diberlakukan setelah setidaknya Wakil Rektor II, menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	
5. Kurangnya dokumentasi proses untuk melakukan evaluasi dan memastikan kepatuhan terhadap kebijakan keamanan, hukum-hukum yang dipakai dan aturan-aturan, dan kebutuhan penjaminan.	Kebijakan keamanan dan peraturan.	6. Dipublikasikan dan dikomunikasikan kepada seluruh karyawan dan pihak eksternal. (A.8.2.3) 7. Prosedur operasional harus didokumentasikan, dipertahankan, dan tersedia untuk semua pengguna yang membutuhkannya. (A.10.1.1) 8. Kebijakan keamanan informasi harus ditinjau pada selang waktu terencana atau jika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan, dan efektifitas. (A.5.1.2)	1.Pembuatan prosedur operasi yang mengatur untuk melakukan evaluasi dan memastikan kepatuhan terhadap kebijakan keamanan, hukum-hukum yang dipakai dan aturan-aturan serta kebutuhan penjaminan. 2.Sosialisasi peraturan yang telah disetujui.	Diberlakukan setelah setidaknya Wakil Rektor II, menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	Periodik 2 x dalam satu tahun
6. Tidak adanya kebijakan dan prosedur dalam melindungi informasi ketika bekerja dengan instansi lain.	Manajemen Keamanan dan Kolaboratif	9. Prosedur Operasi harus didokumentasikan dan dapat tersedia kepada siapa saja yang membutuhkan. (A.12.1.1)	1. Pembuatan prosedur operasi yang mengatur melindungi informasi ketika bekerja dengan instansi lain. 2. Sosialisasi peraturan yang telah disetujui	Diberlakukan setelah setidaknya Wakil Rektor II, menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	Periodik 2 x dalam satu tahun

Tabel 6. (Lanjutan)

ANCAMAN	ASPEK	PENGENDALIAN ISO 27001:2013	PERENCANAAN	IMPLEMENTASI	RENCANA EVALUASI
7. Belum adanya dokumentasi kebijakan dan prosedur untuk mengendalikan akses fisik ketempat kerja dan perangkat keras dan media perangkat lunak.	Pengendalian Akses Fisik	10. Prosedur untuk bekerja di daerah aman harus dirancang dan diterapkan.(A.11.1.5) 11. Parameter keamanan harus didefinisikan dan digunakan untuk melindungi area yang memiliki informasi penting dan fasilitas yang mengolah informasi. (A.11.1.1)	1. Pembuatan prosedur mengendalikan akses fisik ketempat kerja dan perangkat keras serta media perangkat lunak. 2. Sosialisasi peraturan yang telah disetujui.	Diberlakukan setelah setidaknya Wakil Rektor II, menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	Peridik 2 x dalam satu tahun
8. Tidak adanya catatan audit dan monitoring diperiksa secara rutin untuk meneliti anomali dan serta belum adanya aksi perbaikan.	Pemantauan dan Audit Keamanan Fisik	12. Persyaratan audit dan kegiatan yang melibatkan verifikasi operasionalsistem harus hati-hati direncanakan dan disetujui untuk meminimalkan adanya gangguan proses bisnis.(A.12.7.1)	1. Pembuatan prosedur untuk audit dan monitoring 2. Sosialisasi peraturan yang telah disetuui	Diberlakukan setelah setidaknya Wakil Rektor II, menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	Periodik 2 x dalam satu tahun
9. Tidak adanya dokumentasi dan rencana uji keamanaan untuk menjaga sistem dan jaringan.	Manajemen sistem dan jaringan.	13. Prosedur Operasi harus didokumentasikan dan dapat tersedia kepada siapa saja yang membutuhkan. (A.12.1.1)	1. Pembuatan peraturan dan sangsi, yang harus ditandatangai oleh manajemen tertinggi.	Diberlakukan setelah setidaknya Wakil Rektor II, menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	Periodik 2 x dalam satu tahun
10. Tidak adanya dokumentasi dan rencana uji data cadangan untuk backup perangkat lunak dan data.		14. Salinan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan backup yang disepakati . (A.12.3.1)	2.Pembuatan SOP kebiijakan backup.		
			3.Sosialisasi peraturan yang telah disetujui.		

Tabel 6. (Lanjutan)

ANCAMAN	ASPEK	PENGENDALIAN ISO 27001:2013	PERENCANAAN	IMPLEMENTASI	RENCANA EVALUASI
11. Tidak adanya dokumentasi kebijakan dan prosedur untuk membuat dan menghapus hak akses kesuatu informasi baik individu maupun grup.	Pengesahan dan Otorisasi	15. Proses pendaftaran pengguna akan diimplementasikan untuk memungkinkan pengalihan hak akses.(A.9.2.1)	1. Pembuatan peraturan dan sangsi, yang harus ditandatangai oleh manajemen tertinggi.	Diberlakukan setelah setidaknya Wakil Rektor II, menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	Periodik 2 x dalam satu tahun
		16. Sebuah proses penyediaan akses pengguna resmi dilaksanakan untuk menetapkan atau mencabut hak akses untuk semua jenis pengguna untuk semua sistem dan jasa.(A.9.2.2)			
		17. Alokasi dan penggunaan hak akses istimewa akan dibatasi dan dikontrol.(A.9.2.3)	2. Pembuatan SOP kebijakan untuk membuat dan menghapus akses ke suatu informasi baik individu maupun grup		
		18. Alokasi informasi otentikasi rahasia harus dikendalikan melalui proses manajemen formal.(A.9.2.4)	3. Sosialisasi peraturan yang telah disetujui		
		19. Pemilik aset harus meninjau hak akses pengguna secara berkala.(A.9.2.5)			
		20. Hak akses dari seluruh karyawan dan pengguna pihak eksternal untuk informasi dan pengolahan informasi fasilitas harus dihapus setelah pemutusan hubungan kerja mereka, kontrak atau perjanjian, atau disesuaikan pada perubahan.(A.9.2.6)			

Tabel 6. (Lanjutan)

ANCAMAN	ASPEK	PENGENDALIAN ISO 27001:2013	PERENCANAAN	IMPLEMENTASI	RENCANA EVALUASI
12. Tidak adanya dokumentasi prosedur untuk mengidentifikasi, melaporkan dan menanggapi dugaan pelanggaran keamanan dan insiden.	Manajemen Indisen	21. Event log merekam aktivitas pengguna, pengecualian, kesalahan dan informasi peristiwa keamanan harus diproduksi, disimpan dan direview secara teratur (A.12.4.1)	1. Pembuatan peraturan dan sangsi, yang harus ditandatangai oleh manajemen tertinggi.	Diberlakukan setelah setidaknya Wakil Rektor II, menandatangani peraturan yang telah dibuat dan telah disosialisasikan, serta melaksanakan pelatihan kepada user.	
		22. Fasilitas logging dan log informasi harus dilindungi terhadap sabotase dan akses yang tidak sah.(A.12.4.2)	2. Pembuatan SOP kebijakan untuk mengidentifikasikan, melapor, dan menanggapi dugaan pelanggaran keamanan		Periodik 2 x dalam satu tahun
13. Belum adanya prosedur manajemen insiden yang diperbaharui secara periodik.		23. Manajemen tanggung jawab dan prosedur harus ditetapkan untuk memastikan respon yang cepat, efektif dan teratur untuk informasi insiden keamanan.(A.16.1.1)	3. Sosialisasi peraturan yang telah disetujui		

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian dan analisis yang telah dilakukan maka dapat diambil beberapa kesimpulan dari penggunaan OCTAVE-S sebagai acuan dasar melakukan evaluasi risiko pada Universitas Muhammadiyah Tangerang serta ISO 27001:2013 yang dijadikan sebagai pengendalian atas ancaman-ancaman dari aspek keamanan sistem informasi yang dipilih. Kesimpulannya adalah:

1. Dengan melakukan evaluasi risiko dengan menggunakan OCTAVE-S maka universitas dapat memetakan risiko dan kelemahan sistem informasi universitas.
2. Dengan dilakukannya manajemen risiko sistem informasi, Universitas Muhammadiyah Tangerang dapat mengetahui seberapa besar dampak risiko, ancaman serta kelemahan yang muncul.
3. Universitas Muhammadiyah Tangerang kurang dalam melakukan dokumentasi – dokumentasi, khususnya dalam prosedur – prosedur operasional bagian TI, serta dokumentasi yang berkenaan dengan penilaian terhadap asset penting universitas.
4. Dari hasil evaluasi, dapat diketahui bahwa manajemen risiko berada pada posisi SEDANG, artinya universitas tidak mengalami risiko yang dapat menghentikan / merusak sistem informasi yang berdampak pada berhentinya proses belajar mengajar jika terjadi risiko tersebut, namun risiko dan kelemahan pada universitas dapat berdampak pada menurunnya kinerja universitas jika tidak ditangani dengan segera.
5. Dengan menggunakan pengendalian yang ada pada ISO 27001:2013 dapat membantu universitas dalam melakukan persiapan saat akan mengimplementasikan standar ISO khususnya pada bagian teknologi informasi.

Saran

Berdasarkan evaluasi sistem informasi manajemen risiko menggunakan OCTAVE-S ini, hanya memberikan informasi tentang risiko dan kelemahan pada universitas dan masukan untuk penanganan risiko dan kelemahan. Oleh karena itu saya menyampaikan saran kepada pihak manajemen Universitas Muhammadiyah Tangerang agar :

1. Melengkapi praktik keamanan yang disarankan OCTAVE setidaknya yang dijadikan prioritas dari 15 praktik keamanan.
2. Membuat prosedur mengenai praktik-praktik keamanan secara lebih formal untuk menjalankan kemanan TI secara konsisten.
3. Implementasikan SOP manajemen risiko dalam prosedur sekecil apapun karena risiko dan kelemahan selalu berawal dari sebuah kesalahan kecil yang menimbulkan lubang pada keamanan sistem informasi.
4. Menyediakan pelatihan-pelatihan kesadaran keamanan pada seluruh karyawan Universitas Muhammadiyah Tangerang. Hal ini penting agar karyawan mengerti bagaimana menjaga keamanan yang akan meminimalkan risiko. Misalnya dengan proteksi virus disetiap perangkat lunak, meletakan kamera pengintai dan alat penjaga keamanan, memberikan pelatihan dan edukasi tentang pentingnya menjaga keamanan sistem informasi.
5. Secara berkala melakukan audit keamanan sistem informasi untuk mengetahui kebutuhan dan kelemahan keamanan sistem informasi karena terus berkembangnya teknologi menyebabkan jenis serangan / risiko akan semakin berkembang.

DAFTAR PUSTAKA

Albert, C. &. (2003). Managing Information Security Risks: The OCTAVESM Approach. USA: Addison Wesley.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. USA: Carnegie Mellon University.

Coleman, J. (2004). Assessing Information Security Risk in Healthcare Organizations of Different Scale. Proceedings of the 18th International Congress and Exhibition (hal. 125-130). Elsevier.

Hakemi, A., Jeong, S. R., Ghani, I., & Sanaei, M. G. (2014). KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS. Enhancement of VECTOR Method by Adapting OCTAVE for Risk Analysis in Legacy System Migration, VOL. 8, NO. 6.

ISO, & EIC. (2005). International Standard, Information Technology - Security Techniques - Information Security Management System - Requirements. London: British Standard Institution.

Jake Kouns, D. M. (2010). Information Technology Risk Management in Enterprise Enviroments. New Jersey: John Wiley & Sons.

Kloman, H. F. (2000). Risk Management Reports. USA: Press Inc.

Laudon, K. C., & Laudon, J. P. (2007). Sistem Informasi Manajemen. Basingstoke: Palgrave.

PDDIKTI. (2016, MARET 1). Grafik Jumlah Perguruan Tinggi. Retrieved MARET 5, 2016, from Pangkalan Data Pendidikan Tinggi: http://forlap.ristekdikti.go.id/perguruantinggi/homegraphpt

S., Drisi., Houmani. H& Medromi, H. (2013). International Journal of Advanced Computer Science and Applications(IJACSA), Vol. 4, No. 12 Pages :143-148.

Satti, M. M., Nagrial, M. H., & Garner, B. J. (2002). Framework of Information Security Management System (ISMS) Standards ISO 17799 / BS 7799. Journal of Managemen.

Stephanus. (Desember 2014). ComTech Vol. 5 No. 2 . IMPLEMENTATION OCTAVE-S AND ISO 27001CONTROLS, 683-693

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. USA: National Institute of Standards and Technology.

UMT. (2016). Sejarah&Profil Universitas Muhammadiyah Tangerang. Retrieved Maret 5, 2016, from Universitas Muhammadiyah Tangerang: http://umt.ac.id/index.php/web/halaman/9