LAMPIRAN A

HASIL WAWANCARA

Pada bagian Lampiran A ini berisikan daftar transkrip hasil wawancara dengan pihak Institusi Pendidikan XYZ yang telah dilakukan oleh penulis selama pengerjaan tugas akhir.

Tanggal Wawancara : 4 Mei 2018
Media : Tatap Muka (Wawancara)
Jabatan Narasumber : Kepala Divisi Sistem Informasi
Tujuan Wawancara : Divisi Sistem Informasi Institusi Pendidikan XYZ

Tabel A.1 Transkirp Wawancara Terkait Aset TI

Pertanyaan	Jawaban
Sistem / *Software* apa saja yang dimiliki oleh Divisi Sistem Informasi Institusi Pendidikan XYZ?	Microsoft Office, software database, software streaming, vmware, proxmox, dan aplikasi Sistem Informasi Mahasiswa, dsb.
Apa aset yang paling penting yang dimiliki oleh organisasi?	*Server*, *firewall*, wlc, dan semua hardware yang berada di *data center*.
Apa ada kebijakan khusus dari Divisi Sistem Informasi Institusi Pendidikan XYZ untuk memproteksi aset-aset yang dimiliki?	*Data center* hanya boleh diakses oleh kaur di bagiannya, untuk coding aplikasi ditangani oleh bagian nya, dst.
Apakah ada dokumentasi yang dilakukan untuk setiap aset yang ada ?	Dokumentasi aset di *data center* ada, karena setiap pembelian aset ada rincian barangnya, tapi untuk detail nya bisa ditanyakan kaur masing-masing.
Apakah Divisi Sistem Informasi Institusi Pendidikan XYZ?	Sering terjadi serangan hampir tiap hari, belum pernah terjadi serangan yang fatal, karena dapat ditanggulangi firewall.

pernah mendapatkan serangan dari pihak eksternal maupun internal?	

Kesimpulan Wawancara Tabel A.1 :

Hasil wawancara ke Kepala Divisi Sistem Informasi Institusi Pendidikan XYZ berupa penjelasan tentang identifikasi aset kritis, keamanan aset yang sudah diterapkan dan identifikasi kelemahan yang dimana aset-aset keamanan sudah diterapkan dengan baik, begitu juga untuk proteksi hak akses pada setiap aset sudah ditangani pada setiap bagian-bagian urusannya.

Tanggal Wawancara : 5 Mei 2018
Media : Tatap Muka (Wawancara)
Jabatan Narasumber : Kepala Urusan Infrastruktur Jaringan
Tujuan Wawancara : Aset Infrastruktur Jaringan Institusi Pendidikan XYZ

Tabel A.2 Transkirp Wawancara Terkait Aset TI

Pertanyaan	Jawaban
Sistem / *Software* apa saja yang dimiliki oleh Divisi Sistem Informasi Institusi Pendidikan XYZ?	Software yang include di hardware seperti os router, os acces point, dst. Dalam segi jaringan aplikasi monitoring gabung dengan perangkat *security* dan perangkat WLC *(Wireless LAN Controller).* Security hanya dari *firewall*

Hardware apa saja yang dimiliki oleh Divisi Sistem Informasi Institusi Pendidikan XYZ?	Router, switch layer 3 dan 2, firewall, access point, WLC.
Siapa penanggung jawab aset di atas?	Semua tanggung jawab biro aset secara fisik, operasional tanggung jawab pada bagian divisi sistem informasi
Apa aset yang paling penting yang dimiliki oleh organisasi? Mengapa?	Yang terpenting jika harus memilih 1 yaitu switch layer 3 tapi semua aset jaringan saling terintergerasi.
Apakah ada aset untuk *backup* atau aset yang disiapkan untuk keadaan tidak terduga? (ex. Server *Disaster Recovery Center*)	Backup selama tidak ada kerusakan itu tidak akan di konfigurasi. Jika terjadi kerusakan maka backup nya akan di konfigurasi dahulu baru bisa digunakan.
Aset mana yang akan menimbulkan dampak besar bagi organisasi jika terungkap (*disclosure*) oleh *unauthorized* (orang yang tidak berhak)?	Core swich, begitu routingan nya kacau atau di hapus akan sangat berbahaya dan jika core switch mati maka internet tidak bisa berjalan.
Berapa usia aset yang dimiliki dan bagaimana bentuk pemeliharaan yang dilakukan oleh Divisi Sistem Informasi Institusi Pendidikan XYZ?	3-5 tahun, pemeliharaan reguler secara berkala. Seperti cek fisik.
Seberapa sering aset-aset organisasi terkena serangan?	Serangan sering terjadi tetapi tidak fatal, serangan biasa coba dilakukan dari mahasiswa bisa secara sengaja ataupun tidak sengaja.

Bagaimana pihak Biro Sistem Informasi Universitas Muhammadiyah Yogyakarta mendeteksi serangan?	Dapat dilihat dari log siapa-siapa saja yang sudah mencoba masuk.
Untuk setiap komponen yang dievaluasi, berapa banyak kelemahan yang harus cepat dibenahi dan yang bisa ditunda?	Dalam evaluasi tidak dilakukakan secara berkala tetapi akan dilakukan perbaikan jika saat terjadi masalah saja.

Kesimpulan Wawancara Tabel A.2 :

Software pada perangkat jaringan itu tidak ada. Software adalah sistem operasi, dan konfigurasi pada sistem jaringan. Dalam segi jaringan aplikasi monitoring gabung dengan perangkat *security* dan perangkat WLC *(Wireless LAN Controller).* Security hanya dari *firewall,* Untuk hardware paling berbahaya jika dirertas yaitu Core Switch. Serangan sering terjadi tetapi tidak fatal, serangan biasa coba dilakukan dari mahasiswa bisa secara sengaja ataupun tidak sengaja. Dalam evaluasi tidak dilakukakan secara berkala tetapi akan dilakukan perbaikan jika saat terjadi masalah saja.

Tanggal Wawancara : 5 Mei 2018
Media : Tatap Muka (Wawancara)
Jabatan Narasumber : Kepala Urusan Server dan Keamanan
Tujuan Wawancara : Aset Server dan Keamanan Institusi Pendidikan XYZ

Tabel A.3 Transkirp Wawancara Terkait Aset TI

Pertanyaan	Jawaban
Sistem / *Software* apa saja yang dimiliki oleh Biro Sistem Informasi Universitas Muhammadiyah Yogyakarta?	Linux, ubuntu, window server 2012, dsb

Apakah ada aset dari pihak ke 3 yang pertanggungjawabannya ada dipihak ke 3 itu sendiri?	Tidak ada, jika ada aset pihak ke 3 itu masih jadi tanggung jawab dari pihak Divisi Sistem Informasi Institusi Pendidikan XYZ
Aset mana yang akan menimbulkan dampak besar bagi organisasi jika terungkap (*disclosure*) oleh *unauthorized* (orang yang tidak berhak)?	Aset yang paling berdampak besar yaitu data mahasiswa, sangat berbahaya jika disalahgunakan oleh orang lain
Bagaimana bentuk pemeliharaan yang dilakukan oleh Divisi Sistem Informasi Institusi Pendidikan XYZ ?	Seperti pengecekan suhu ruangan, dilakukan pengecekan rutin untuk AC pada ruangan *data center*.
Apakah ada pelatihan yang dilakukan oleh Divisi Sistem Informasi Institusi Pendidikan XYZ kepada staff/pegawai dalam memelihara atau meningkatkan praktik-praktik keamanan?	Ada, dengan dilakukannya *training* untuk pegawai baru mengenai server dan keamanan.

Kesimpulan Wawancara Tabel A.3 :

Wawancara kepada kepala urusan server dan kemanan menyimpulkan bahwa jika ada aset pihak ke 3 itu masih jadi tanggung jawab dari pihak Divisi Sistem Informasi Institusi Pendidikan XYZ dan untuk bentuk pemeliharaan aset dilakukan pengecekan rutin di *data center*. *Training* juga dilakukakan kepada pegawai baru yang masuk

Tanggal Wawancara : 25 April 2018
Media : Tatap Muka (Wawancara)
Jabatan Narasumber : Kepala Urusan Aplikasi dan Database
Tujuan Wawancara : Aset Aplikasi dan Database Institusi Pendidikan XYZ

Tabel A.4 Transkirp Wawancara Terkait Aset TI

Pertanyaan	Jawaban
Aplikasi apa saja yang dimiliki oleh Divisi Sistem Informasi Institusi Pendidikan XYZ?	Sebagain besar aplikasi desktop maupun *mobile* dari Institusi Pendidikan XYZ dibuat sendiri, seperti aplikasi Sistem Informasi Mahasiswa.
Siapakah penanggungjawab dari semua aplikasi yang ada di Institusi Pendidikan XYZ ?	Secara struktural kepala penanggung jawab berada pada kaur aplikasi dan database.

Kesimpulan Wawancara Tabel A.4 :

Wawancara kepada kepala urusan aplikasi dan database menyimpulkan bahwa pada bagian aplikasi sebagian besar aplikasi desktop dan mobile dibuat sendiri oleh bagian aplikasi dan database, dan penanggung jawab nya sendiri yaitu kepala urusan bagian aplikasi dan database itu sendiri.

LAMPIRAN B

HASIL PENILAIAN ASET KRITIS

Tabel B.1 Hasil Penilaian Aset Kritis

Aset	Kelompok	Problem	*Severity* (Dampak)		*Occurrence* (Frekuensi)		*Detection* (Deteksi)		*RPN*	Level
			Rating	Cause	Rating	Cause	Rating	Cause		
Web Kartu Rencana Studi Daring (KRS Daring).	Data	Percobaan manipulasi dan kebocoran data.	10	Pengamanan data belum maksimal, sehingga memungkinkan terjadi penyalahgunaan data mahasiswa.	3	Baru saja terjadi dan ada kemungkinan akan terjadi lagi.	10	Belum diketahui sumber percobaan kebocoran data	300	*High*
	Software	Mahasiswa masih menggunakan kata sandi bawaan.	8	Human Error	5	Serangan sering terjadi hampir setiap hari	3	Deteksi bisa dimonitor melalui firewall	120	*Medium*

Aset	Kelompok	Problem	Severity (Dampak)		Occurrence (Frekuensi)		Detection (Deteksi)		RPN	Level
			Rating	Cause	Rating	Cause		Cause		
	Data	Masih ada data mahasiswa yang tidak valid.	5	Penyampaian informasi melalui nomor telepon, atau alamat bisa salah karena data tidak valid	1	Terjadi saat pengisian data mahasiswa di KRS	3	Bisa diketahui saat verifikasi data mahasiswa	15	*Low*
Web Repository	Software	Paling banyak terkena serangan dari eksternal.	9	Data skripsi dan artikel civitas diorganisasi bisa diakses dan dimanipulasi oleh orang yang tidak bertanggungjawab	8	Serangan sering terjadi hampir setiap hari	2	Deteksi bisa dimonitor melalui firewall	144	*High*
	Software	Kebutuhan penyimpanan semakin meningkat.	7	Jika *storage* penuh, maka web repository tidak bisa diakses	1	Belum terjadi	3	*Storage* bisa dimonitor secara *real-time*	21	*Low*

Aset	Kelompok	Problem	*Severity* (Dampak)		*Occurrence* (Frekuensi)		*Detection* (Deteksi)		*RPN*	Level
			Rating	Cause	Rating	Cause	Rating	Cause		
	Software	Web belum aman dan tidak ada SSL Certificate	8	Data penting yang terdapat di dalam web bisa terbaca secara *plain text* tanpa *encryption* sehingga memudahkan pencurian data	1	Belum terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
Core Switch	Hardware	Percobaan masuk ke dalam sistem.	9	Jaringan bisa saja menjadi kacau ketika terjadi kerusakan alat atau kesalahan konfigurasi	4	Belum pernah terjadi kegagalan sistem	4	Deteksi berdasarkan laporan	144	*High*
PC Storage Hitachi 4 unit.	Hardware	Perlu pembaharuan storage secara berkala.	9	Jika media penyimpanan penuh, maka semua data sulit diakses	5	Beberapa kali terjadi	2	Berdasarkan laporan kerusakan	90	*Medium*

Aset	Kelompok	Problem	*Severity* (Dampak)		*Occurrence* (Frekuensi)		*Detection* (Deteksi)		*RPN*	Level
			Rating	Cause	Rating	Cause	Rating	Cause		
Web E-Learning	Software	Kebutuhan penyimpanan semakin meningkat.	7	Jika *storage* penuh, maka web *e-learning* tidak bisa diakses	4	Beberapa kali terjadi	3	*Storage* bisa dimonitor secara *real-time*	84	*Medium*
	Software	Web belum aman dan tidak ada SSL Certificate	9	Data penting yang terdapat di dalam web bisa terbaca secara *plain text* tanpa *encryption* sehingga memudahkan pencurian data	1	Belum terjadi	3	Deteksi bisa dimonitor melalui *firewall*	24	*Low*
Kabel LAN	Hardware	Terjadi kerusakan karena sudah lama dan dikarenakan faktor alam	9	Internet akan mati didaerah kabel yang rusak	4	Frekuensi kerusakan berdasarkan laporan	2	Deteksi berdasarkan laporan	72	*Medium*
Switch	Hardware	Belum pernah dilakukan evaluasi pada perangkat tersebut.	6	Identifikasi permasalahan sistem menjadi lebih lama	5	Frekuensi kerusakan berdasarkan laporan	2	Deteksi berdasarkan laporan	60	*Low*

Aset	Kelompok	Problem	*Severity* (Dampak)		*Occurrence* (Frekuensi)		*Detection* (Deteksi)		*RPN*	Level
			Rating	Cause	Rating	Cause	Rating	Cause		
Router	Hardware	Rusak apabila karena faktor alam.	6	Router rusak	3	Frekuensi kerusakan berdasarkan laporan	2	Deteksi berdasarkan laporan	36	*Low*
	Hardware	Belum pernah dilakukan evaluasi pada perangkat tersebut.	6	Identifikasi permasalahan sistem menjadi lebih lama	1	Frekuensi kerusakan berdasarkan laporan	2	Deteksi berdasarkan laporan	12	*Low*
SIM Surat	Software	Kebocoran dan Manipulasi data.	7	Tidak bisa diakses	2	Belum pernah terjadi kegagalan sistem	2	Berdasarkan laporan kerusakan	28	*Low*
DHCP Server	Software	Tidak ada.	7	Jika terjadi gangguan berdampak pada jaringan seluruh institusi mati	2	Belum pernah terjadi kegagalan sistem	2	Berdasarkan laporan kerusakan	28	*Low*

Aset	Kelompok	Problem	*Severity* (Dampak)		*Occurrence* (Frekuensi)		*Detection* (Deteksi)		*RPN*	Level
			Rating	Cause	Rating	Cause	Rating	Cause		
Wireless LAN Controller	Hardware	Perangkat mengalami kerusakan fisik.	6	Koneksi internet disuatu area tidak berjalan	1	Kegagalan sistem beberapa kali terjadi yang diketahui berdasarkan laporan dari stackholder terkait	3	Diketahui saat ada koneksi down di area tertentu	18	*Low*
	Hardware	Kesalahan konfigurasi pada perangkat.	6	Koneksi internet disuatu area tidak berjalan	1	Belum pernah terjadi kegagalan sistem	3	Diketahui saat ada koneksi down di area tertentu	18	*Low*
SIM Anggaran	Software	Kebocoran dan Manipulasi data.	8	Surat Pertanggungjawaban yang dimanipulasi menyebabkan terhambatnya proses bisnis suatu unit kerja dan menyebabkan terhambatnya	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*

				proses pencairan dana untuk kegiatan selanjutnya pada unit kerja tersebut						

Aset	**Kelompok**	**Problem**	***Severity* (Dampak)**		***Occurrence* (Frekuensi)**		***Detection* (Deteksi)**		***RPN***	**Level**
			Rating	**Cause**	**Rating**	**Cause**	**Rating**	**Cause**		
SIM Arsip	Software	Kebocoran dan Manipulasi data.	8	SK pengangkatan seseorang yang sifatnya rahasia, bisa disalahgunakan.	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
SIM Aset	Software	Kebocoran dan Manipulasi data	8	Terjadi kesalahan dalam proses perhitungan audit data. Duplikasi data asset yang bisa menyebabkan pihak lain mengakusisi salah satu atau	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*

				beberapa asset milik Institusi XYZ						

Aset	**Kelompok**	**Problem**	***Severity* (Dampak)**		***Occurrence* (Frekuensi)**		***Detection* (Deteksi)**		***RPN***	**Level**
			Rating	**Cause**	**Rating**	**Cause**	**Rating**	**Cause**		
SIM Kepegawaian	Software	Kebocoran dan Manipulasi data.	8	Penyalahgunaan Informasi bisa menyebabkan penipuan mengatasnamakan perorangan atau instansi	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
SIM MoU	Software	Kebocoran dan Manipulasi data.	8	Kemungkinan terjadinya kebocoran data menyebabkan diketahuinya pihak mana saja yang sudah menjalin kerjasama dengan Institusi XYZ	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*

Web Portal Institusi	Software	Web belum aman dan Tidak ada SSL Certificate.	8	Data penting yang terdapat di dalam web bisa terbaca secara *plain text* tanpa *encryption* sehingga	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*

Aset	**Kelompok**	**Problem**	***Severity* (Dampak)**		***Occurrence* (Frekuensi)**		***Detection* (Deteksi)**		***RPN***	**Level**
			Rating	**Cause**	**Rating**	**Cause**	**Rating**	**Cause**		
Web Portal Fakultas	Software	Web belum aman dan Tidak ada SSL Certificate.	8	Data penting yang terdapat di dalam web bisa terbaca secara *plain text* tanpa *encryption* sehingga	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
Web Portal Program Studi	Software	Web belum aman dan Tidak ada SSL Certificate.	8	Data penting yang terdapat di dalam web bisa terbaca secara *plain text* tanpa *encryption* sehingga	1	Belum pernah terjadi	2	Deteksi bisa dimonitor melalui *firewall*	16	*Low*
Access Point	Hardware	Belum pernah dilakukan evaluasi pada	4	tidak bisa akses wifi pada area tertentu	1	Belum pernah terjadi	2	Berdasarkan laporan kerusakan	8	*Low*

		perangkat tersebut.				kegagalan sistem				
Firewall	Hardware	Tidak ada	8	Jika firewall mati bisa berakibat pada keamanan seluruh aset milik Institusi XYZ	1	Belum pernah terjadi kegagalan sistem	1	Berdasarkan laporan kerusakan	8	*Low*
ASP .NET dan IIS	Software	Tidak ada	1	No	1	No	1	No	1	*Low*