AUDIT *SECURITY SERVICES* PADA PT. XYZ

Aulia Primadani[1], Basuki Rahmad[2], M.Teguh Kurniawan[3]
[1,2,3] Prodi Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
Email: primadanul@gmail.com[1], azkaku@gmail.com[2], ujangtegoeh@gmail.com[3]

Abstrak

Untuk mengetahui apakah layanan keamanan informasi yang terdapat pada PT. XYZ sudah memenuhi kriteria atau belum dilakukan penelitian audit terhadap layanan keamanan informasi pada PT. XYZ. Penelitian yang dilakukan meliputi layanan perlindungan terhadap *malware*, pengelolaan jaringan dan konektivitas jaringan, pengelolaan keamanan *endpoints*, pengelolaan identitas pengguna dan akses logik, pengelolaan akses fisik dan aset TI dan perhitungan *capability level* pada setiap layanan keamanan yang telah diterapkan pada PT. XYZ. Penelitian audit yang dilakukan melakukan framework COBIT 5 dan INTOSAI.

Kata kunci : COBIT 5, INTOSAI, *Audit Security Services, Capability Level*

Abstract

To determine whether the security service information on PT. XYZ has met the criteria or have not done the research audits of information security services at PT. XYZ. The research undertaken include protection against malware services, network management and network connectivity, security management of endpoints, user identity management and logical access, physical access and management of IT assets and computation capability of each service level of security that has been applied to the PT. XYZ. Conduct audits conducted research framework COBIT 5 and INTOSAI.

Keywords : COBIT 5, INTOSAI, *Audit Security Services, Capability Level*

1. Pendahuluan

Pada masa sekarang ini,informasi sangat dibutuhkan oleh semua pihak dalam membangun suatu organisasi yang bersifat operasional yang digunakan untuk mengambil keputusan strategis untuk semua masalah yang terjadi ditengah organisasi tersebut. Informasi dibutuhkan apabila sudah terdapat banyak masalah yang tingkat kompleksitasnya sudah tinggi, sehingga solusi yang didapatkan haruslah bersifat efektif, tepat sasaran dan efisien yang bertujuan membantu organisasi tersebut dalam mewujudkan visi dan misinya.

PT. XYZ merupakan perusahaan yang memakai penerapan teknologi informasi dalam mencapai semua visi dan misi perusahaannya yang di implementasikan dalam berbagai tujuan bisnis yang telah di tetapkan oleh PT. XYZ itu sendiri. Informasi yang terdapat pada sebuah perusahaan merupakan sebuah aset yang harus dilindungi dari berbagai ancaman keamanan terhadap layanan pada PT. XYZ seperti ancaman virus, *sniffer, hacker* dan semacamnya. Informasi yang sudah diolah harus memiliki keamanan yang telah mencukupi dengan standar yang telah disepakati. Keamanan informasi sangatlah berperan besar dalam sebuah perusahaan. Informasi yang terdapat pada sebuah perusahaan merupakan sebuah aset yang harus dilindungi dari berbagai ancaman keamanan terhadap layanan pada PT. XYZ seperti ancaman virus, *sniffer, hacker,*dan semacamnya. Informasi yang menjadi komponen inti suatu perusahaan harus menjadi perhatian utama yang harus dilindungi dari segala serangan, baik dari internal maupun eksternal perusahaan. Apabila tidak diterapkan keamanan informasi, informasi yang terdapat pada perusahaan sangatlah mudah untuk dilihat, dimodifikasi bahkan di ambil.

Pada tahun 2013, terdapat kejadian ancaman keamanan informasi terhadap keberlangsungan operasi perusahaan PT. XYZ , yaitu masuknya pengguna yang sudah tidak mempunyai hak dan melakukan kerusakan pada sistem internal, yaitu merubah nominal pada laporan keuangan per kuartal sehingga menimbulkan kekacauan pada laporan tersebut. Untuk menanggulangi agar tidak terjadi lagi hal yang tidak diinginkan tersebut, maka harus melakukan manajemen keamanan informasi. Untuk membuat kebijakan perihal manajemen keamanan informasi terlebih dahulu dilakukan penelitia audit *security services* terkait.

Penelitian terhadap *audit security services* juga bertujuan untuk mengetahui sejauh mana PT. XYZ dalam menerapkan berbagai tingkat keamanan yang diperlukan, harus menggunakan sebuah penilaian atau pengukuran terhadap *security services* pada PT. XYZ. Penelitian juga bertujuan untuk memberikan penilaian terhadap *security services* yang telah diterapkan dan memberikan perbaikan keamanan yang diperlukan oleh PT. XYZ pada waktu sekarang dan masa depan.

Untuk mengetahui sejauh mana PT. XYZ dalam menerapkan berbagai tingkat keamanan yang diperlukan, harus menggunakan sebuah penilaian atau pengukuran terhadap *security services* pada PT. XYZ. Untuk mengukur sudah sejauh mana tingkat keberhasilan PT. XYZ dalam menerapkan *security services*, maka diperlukan evaluasi melalui audit keamanan informasi terhadap *security services* yang bertujuan untuk memberikan penilaian terhadap *security services* yang telah diterapkan dan memberikan perbaikan keamanan yang diperlukan oleh PT. XYZ pada waktu sekarang dan masa depan.

Berdasarkan latar belakang diatas, rumusan masalah yang terdapat pada penelitian ini yang bertujuan untuk mengetahui hal-hal apa saja yang bisa diperbaiki dan juga dioptimisasi kinerjanya untuk membantu perusahaan dalam mencapai visi dan misinya kedepan adalah sebagai berikut:

1. Bagaimana penerapan kontrol-kontrol terkait *security services* di PT. XYZ?
2. Bagaimana kapabilitas *security services* di PT. XYZ?

3. Bagaimana rekomendasi perbaikan keamanan TI pada *security services* di PT. XYZ supaya terus dapat dipercaya oleh berbagai pihak, baik pihak internal maupun pihak eksternal perusahaan?

Berdasarkan rumusan masalah yang sudah dijelaskan diatas,maka tujuan utama dari penelitian ini yang nantinya dapat memberikan dampak positif ke pihak perusahaan adalah sebagai berikut:

1. Mengukur efektivitas kontrol sistem informasi terhadap *security services* di PT. XYZ.
2. Melakukan penilaian (*assesment*) kapabilitas *security services* yang terdapat di PT. XYZ.

Manfaat pada penelitian ini diharapkan dapat berdampak positif baik dari sisi perusahaan maupun dari sisi pendukung lainnya,beberapa manfaat yang diperoleh dalam penelitian ini adalah sebagai berikut :

1. Meningkatkan perbaikan keamanan TI yang terdapat pada PT. XYZ.
2. Meningkatkan kinerja perusahaan baik dari sisi sumber daya manusia maupun dari sisi sarana dan prasarananya.

Pada penelitian ini kami menentukan beberapa batasan masalah yang digunakan untuk batasan fokus penelitian kami seperti dibawah ini:

1. Objek penelitian hanya pada divisi keamanan dan *Quality Assurance* pada direktorat teknologi informasi dan jasa keuangan wilayah kantor pusat PT. XYZ.
2. Penilaian kontol terhadap *security services* yang digunakan hanya pada domain *Deliver Service Support* 05.01, 05.02, 05.03 05.04 dan 05.05.
3. Penilaian Kapabilitas level menggunakan *Process Assesment Model* (PAM) pada *framework* COBIT 5.
4. Penilaian audit hanya bersifat rekomendasi terbuka tidak sampai tahap konfirmasi perusahaan untuk menerima hasil audit atau tidak.

2. Dasar Teori dan Metode Penelitian

2.1 Pengertian Sistem Informasi

Menurut Maniah dan Surendro (2005), sistem informasi merupakan aset bagi suatu perusahaan yang bila diterapkan dengan baik akan memberikan kelebihan untuk berkompetensi sekaligus meningkatkan kemungkinan bagi kesuksesan suatu usaha.

2.2 Aspek Keamanan Informasi

Menurut Garfinkel (1995), aspek keamanan terdiri dari :

1. ***Privacy/Confidentiality***

Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Menggunakan Enkripsi merupakan salah satu usaha yang dapat dilakukan.

2. ***Integrity***

Usaha untuk menjaga informasi agar tetap utuh, tidak diubah, baik ditambah maupun dikurangi kecuali mendapat izin dari pemilik informasi. Virus maupun *Trojan Horse* merupakan salah satu contoh dari masalah dan penggunaan antivirus, enkripsi dan *digital signatures* merupakan salah satu usaha untuk menangkalnya.

3. ***Authentication***

Merupakan metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Penggunaan Access Control seperti *Login* dan *Password* adalah salah satu usaha untuk memenuhi aspek ini.

4. ***Availability***

Merupakan Informasi yang tersedia manakala dibutuhkan. Contoh serangannya adalah *DoS attack* dan *MailBomb.*

2.4 Aspek Ancaman Keamanan Informasi

Menurut William Stallings (2005), serangan dan ancaman terhadap keamanan sistem informasi ada beberapa macam, yaitu :

1 ***Interruption***

Merupakan perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah “denial of service attack”.

2 ***Interception***

Merupakan pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan *(wiretapping).*

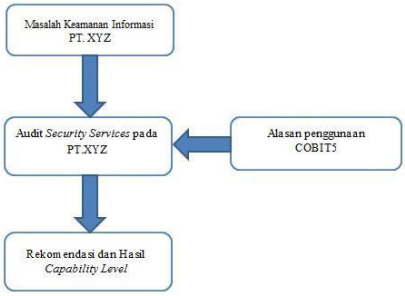
3 ***Modification***

Merupakan pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah aset. Contoh dari serangan ini antara lain adalah mengubah isi dari *web site* dengan pesan-pesan yang merugikan pemilik *web site*.

4 ***Fabrication***

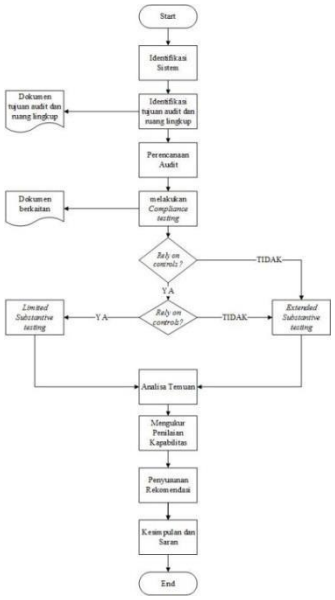
Merupakan pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

2.5 Model Konseptual



Gambar III 1 Metode Konseptual

2.6 Sistematika Penulisan



Gambar III 2 Sistematika Penulisan

a. Identifikasi Sistem

   Identifikasi sistem atau masalah pada tahapan kerja audit bertujuan untuk mengetahui masalah inti yang terdapat pada objek audit yang telah dipilih.Masalah yang didapatkan harus sesuai dan relevan dengan bidang yang telah ditentukan dan disetujui baik oleh pihak perusahaan maupun dari pihak *auditor*.

b. Identifikasi Tujuan dan ruang lingkup
   Tujuan dari diadakannya kegiatan Audit harus sudah jelas dan disepakati oleh kedua pihak,baik perusahaan maupun pihak *auditor*.Perusahaan maupun auditor berhak melakukan teguran kepada salah satu pihak apabila kegiatan audit sudah jauh melenceng dari tujuan awal.

c. Perencanaan Audit
   Perencanaan audit merupakan total lamanya waktu yang dibutuhkan oleh auditor untuk melakukan perencanaan audit awal sampai pada pengembangan rencana audit dan program audit menyeluruh.

d. Penyusunan program audit
   Program audit merupakan kumpulan prosedur audit yang dibuat tertulis secara rinci dan dijalankan untuk mencapai tujuan audit dan akan lebih baik jika audit program dibuat terpisah untuk *compliance test* dan *substantive test.*

e. *Timeline audit*

Pada kegiatan audit, *timeline* dimaksudkan untuk mengelola penjadwalan dalam melakukan pengumpulan bukti yang dilakukan oleh auditor. Pengumpulan bukti yang diperlukan oleh auditor adalah dengan memeriksa langsung berbagai sarana dan prasarana serta dokumen t.erkait dalam kegiatan audit tersebut.

f. Melakukan *Compliance testing*
Berbagai pertanyaan *Compliance test* yang terdapat pada program audit yang sudah dibuat oleh *auditor* dalam perencanaan audit,dituangkan dan dilaksanakan dalam kegiatan melakukan *compliance testing.*

g. Evaluasi bukti
Analisa bukti yang terdapat pada kegiatan audit yang telah dilaksanakan digunakan untuk penilaian terhadap kinerja perusahaan selama sebelum kegiatan audit berlangsung. Bukti-bukti yang sudah didapatkan oleh pihak *auditor* dapat menjadi bahan acuan untuk perbaikan kedepannya

3. Analisa Data

3.1. Identifikasi Sistem

IV.1.1 Arsitektur Keamanan

3.1.1.1 Perlindungan terhadap malware

Pada PT. XYZ, perlindungan terhadap *malware* dengan menggunakan antivirus yang diperbaharui informasi dan versinya secara berkala.Antivirus yang digunakan adalah antivirus dari pihak ketiga, yaitu Kaspersky dari perusahaan Kaspersky Lab. Perlindungan dilakukan secara terintegrasi antar setiap perangkat, sehingga setiap perangkat mendapatkan perlakuan yang sama terhadap perlindungan *malware*.

3.1.1.2 Mengelola jaringan dan konektivitas keamanan

Pada PT. XYZ, perlindungan terhadap pengelolaan jaringan dan konektivitas yang dilakukan adalah dengan menempatkan perangkat dan konfigurasi yang sesuai yang bertujuan untuk melakukan penghalauan terhadap berbagai serangan yang dilakukan oleh pihak luar.

3.1.1.3 Mengelola keamanan endpoints

Pada PT. XYZ pengamanan yang dilakukan pada pengelolaan *endpoints* adalah dengan menggunakan IDS (*Intrusion Detection System*) berbasis *network* dan IDS berbasis *host*. Sistem NIDS dan HIDS yang dilakukan bertujuan untuk menganalisa berbagai lalu lintas paket data yang masuk kepada *endpoints*. Paket data yang berbahaya akan langsung ditindak lanjuti dan akan menghasilkan log. Sistem HIDS hanya diterapkan pada *host-host* tertentu, sedangkan NIDS digunakan untuk menganalisa keseluruhan jaringan pada *endpoints*.

3.1.1.4 Mengelola identitas pengguna dan akses logik

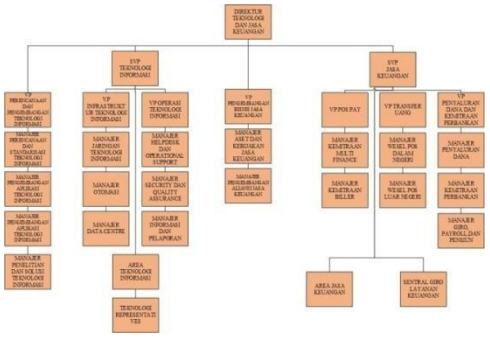
Pada PT. XYZ pengamanan yang dilakukan pada pengelolaan identitas pengguna dan akses logik, yaitu dengan menerapkan sistem authentikasi *One Time Password* untuk setiap login pengguna ke sistem internal perusahaan. Sistem authentikasi *One Time Password* bertujuan untuk menghalau pengguna yang tidak berkepentingan untuk dapat merusak sistem yang terdapat pada PT. XYZ.

3.1.1.5 Mengelola akses fisik dan aset TI

Pada PT. XYZ pengamanan yang dilakukan pada pengelolaan akses fisik dan aset TI adalah dengan memberikan batasan akses pkepada semua pihak yang ingin masuk ke dalam wilayah akses fisik seperti server,dll.

IV.1.2 Pengelolaan Keamanan

Berbagai kebijakan dan surat edaran yang telah dibuat dan diterapkan oleh PT. XYZ ditentukan oleh pihak- pihak yang berkaitan, salah satunya adalah divisi keamanan dan *Quality Assurance* yang bertanggungjawab penuh dengan semua keputusan dan kebijakan yang diterbitkan. Berikut struktur organisasi direktorat teknologi dan jasa keuangan.



Gambar IV 1 Stuktur Organisasi Direktorat Teknologi dan Jasa Keuangan PT. XYZ

IV.1.3 Framework Manajemen Keamanan

Manajemen keamanan yang terdapat pada PT. XYZ masih menggunakan keputusan direksi dalam kebijakan untuk menjalankan operasi keamanan informasi pada sistem informasi di perusahaan tersebut.

Perencanaan Audit

3.3.1 Risk Assessment

Tabel IV- 1 Pemetaan Risiko PT. XYZ pada layanan DSS 05

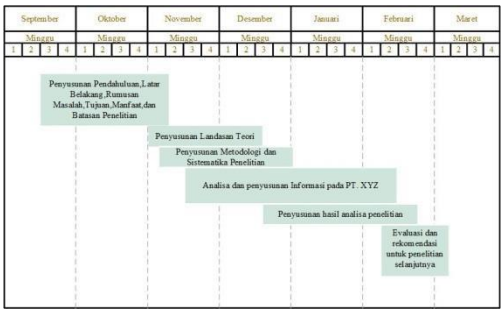
No	Ancaman	Tempat Kejadian				*Risk Assessment*			
		DRP	DC	KP	KC	*Probability*	*Impact*	*Risk Quadrant*	*Risk Level*
1	Serangan terhadap *endpoints* berasal dari pihak eksternal (usb,aplikasi,dll)		✓	✓	✓	*High*	*High*	I	*High*
2	Pencopotan e*ndpoints* dilakukan tanpa melakukan penghapusan informasi secara keseluruhan		✓	✓	✓	*Medium*	*High*	III	*High*
3	Serangan *Hack System internal* oleh pihak *eksternal* maupun *internal*			✓	✓	*High*	*High*	I	*High*
4	Serangan membanjiri informasi pada sistem *internal* sehingga mengalami *'System-down'*			✓	✓	*Medium*	*Medium*	V	*Medium*
5	Serangan dari pihak luar kepada *user* pengguna sistem yang menyamar dan meminta informasi pribadi seperti *password, PIN*, dll			✓	✓	*Medium*	*Medium*	V	*Medium*
6	Serangan spam yang menyamar sebagai paket data maupun *link website* oleh pihak *eksternal* maupun *internal*		✓	✓	✓	*High*	*Medium*	II	*High*
7	User ID yang tidak terpakai tidak segera dihapus dan disalahgunakan oleh pihak yang tidak bertanggungjawab			✓	✓	*High*	*High*	I	*High*
8	Pendampingan dan pemeriksaan pihak ketiga untuk menuju *IT sites* perusahaan tdak dilaksanakan sesuai prosedur		✓			*Medium*	*High*	III	*High*

3.3.2 Program Audit

Program audit pada penelitian Audit *Security services* bertujuan untuk mengatur secara sistematis berbagai pertanyaan terkait tentang operasional kegiatan layanan keamanan pada PT. XYZ.

3.3.3 Timeline Audit

Tabel IV- 2 *Timeline Audit*



3.2. Melakukan *Compliance Testing*

Proses *Compliance Testing* pada penelitian Audit *Security services* pada PT. XYZ bertujuan untuk memeriksa kepatuhan perusahaan terhadap kebijakan dan standar yang terkait dan digunakan dalam operasional perusahaan. Proses *compliance testing* dilakukan pada program audit.Program audit yang dibuat berisi tentang pertanyaan terhadap ketaatan perusahaan pada kebijakan dan standar terkait yang telah diterapkan.

3.3. Analisa Temuan

Proses analisa temuan pada penelitian dilakukan Audit *Security services* pada PT. XYZ bertujuan untuk melakukan analisa terhadap hasil *compliance testing* yang telah dilakukan pada proses sebelumnya.

3.4. Mengukur Penilaian Kapabilitas

3.6.1 DSS 05.01 Perlindungan terhadap malware

Tabel IV- 1 Daftar *Work Product* dan *Base Practice* yang belum dilakukan pada DSS 05.01

Work Product	*Base Practices*
1 Melakukan pelatihan dan menerapkan kepada	1 Melakukan pelatihan perlindungan perangkat

para pihak yang terkait dan berdasarkan acuan yang telah ditetapkan	terhadap pengguna secara berkala 2 memastikan para pengguna perangkat mampu menerapkan hasil pelatihan yang telah dilakukan

3.6.2 DSS 05.02 Mengelola jaringan dan konektivitas jaringan

Tabel IV- 5 Daftar *Work Product* dan *Base Practice* yang belum dilakukan pada DSS 05.02

Work Product	*Base Practices*
1 Melakukan implementasi hanya *authorized devices* yang bisa masuk ke dalam jaringan perusahaan dan tingkatan hak akses *user*	1 Mengimplementasikan hanya perangkat yang terautorisasi yang boleh masuk ke jaringan internal perusahaan
2 Melakukan pengelolaan jaringan berdasarkan kebijakan yang berlaku	2 Memiliki kebijakan dalam pengamanan jaringan
3 Melakukan konfigurasi *authorized devices* berdasarkan kebijakan yang berlaku	3 Mempunyai kebijakan aturan tentang *device* mana saja yang boleh akses dan tidak

3.6.3 DSS 05.03 Mengelola keamanan *endpoints*

Tabel IV- 6 Daftar *Work Product* dan *Base Practice* yang belum dilakukan pada DSS 05.03

Work Product	*Base Practice*
1 Melakukan implementasi enkripsi informasi dalam sebuah media penyimpanan	1 Melakukan enkripsi terhadap semua informasi di media penyimpanan
2 Melakukan pengamanan terhadap sistem terintegrasi	2 Melakukan implementasi pengamanan terhadap sistem integrasi
3 Melakukan pengelolaan terhadap sistem *lockdown*	3 Melakukan perbaikan terhadap sistem *lockdown* yang diterapkan

3.6.4 Mengelola identitas pengguna dan hak akses logic

Tabel IV- 7 Daftar *Work Product* dan *Base Practice* yang belum dilakukan pada DSS 05.04

Work Product	*Base Practice*
1 Melakukan perawatan terhadap hak akses yang sesuai terhadap fungsi bisnis,peran dan tanggung jawab	1 Memastikan informasi yang didapat sesuai dengan hak akses pengguna
2 Melakukan otentikasi akses ke aset informasi berdasarkan hak akses yang sudah diklasifikasikan untuk memastikan kontrol otentikasi berjalan sesuai dengan ketentuan	2 Menggunakan *identity management* dalam melindungi *user*
3 Melakukan implementasi pengelolaan identitas pengguna dan akses logik	3 Mempunyai pihak yang bertanggung jawab dalam pengelolaan identitas pengguna dan akses logik

3.6.5 Mengelola akses fisik dan aset TI

Tabel IV- 8 Daftar *Work Product* dan *Base Practice* yang belum dilakukan pada DSS 05.05

Work Product	*Base Practice*
1 Mengelola permintaan dan memberikan akses ke situs fisik IT	1 Melakukan pembaharuan informasi dalam menentukan pihak-pihak mana saja yang diperbolehkan masuk ke situs IT

Tabel IV- 9 Daftar Hasil Penilaian *Capability level security services* PT. XYZ

No	Layanan Keamanan	PA	Capability Level	Level	No	Layanan Keamanan	PA	Capability Level	Level
1	DSS 05.01	1.1	83%	1	4	DSS 05.04	1.1	75%	1
		2.1					2.1		
		2.2					2.2		
2	DSS 05.02	1.1	75%	1	5	DSS 05.05	1.1	75%	1
		2.1					2.1		
		2.2					2.2		
3	DSS 05.03	1.1	88%	2					
		2.1	33%						

4.1 Kesimpulan

4.1.1 Perlindungan terhadap malware

Tabel V- 1 Rekomendasi Layanan DSS 05.01

No	Ineffective Control	Control Reference	Rekomendasi
1	Melakukan pelatihan dan menerapkan kepada para pihak yang terkait dan berdasarkan acuan yang telah ditetapkan	05.01.07	PT. XYZ harus bisa memastikan pelatihan yang telah dilakukan dapat diimplementasikan oleh peserta pelatihan.

4.1.2 Pengelolaan jaringan dan keamanan

Tabel V- 2 Rekomendasi Layanan DSS 05.02

No	Ineffective Control	Control Reference	Rekomendasi
1	Melakukan implementasi hanya *authorized devices* yang bisa masuk ke dalam jaringan perusahaan dan tingkatan hak akses *user*	05.02.01	PT. XYZ harus melakukan implementasi hanya *authorized devices* yang bisa masuk ke dalam jaringan perusahaan dan tingkatan hak akses *user* untuk semua sistem internal.
2	Mengimplementasikan pengelolaan konfigurasi keamanan jaringan	05.02.03	Semua tingkatan keamanan jaringan harus mendapatkan pemberharuan versi keamanan secara rutin dan berkala
3	Melakukan implementasi enkripsi data sesuai dengan klasifikasinya	05.02.04	PT. XYZ harus melakukan enkripsi data pada semua sistem internal yang terdapat pada perusahaan

4.1.3 Pengelolaan keamanan *endpoints*

Tabel V- 3 Rekomendasi Layanan DSS 05.03

No	Ineffective Control	Control Reference	Rekomendasi
1	Melakukan implementasi enkripsi informasi dalam sebuah media penyimpanan	05.03.03	PT. XYZ harus melakukan implementasi enkripsi informasi dalam sebuah media penyimpanan
2	Melakukan pengelolaan keamanan *endpoints* berdasarkan standar keamanan yang diperlukan	05.03.010	PT. XYZ harus melakukan pengelolaan keamanan *endpoints* berdasarkan standar keamanan yang diperlukan untuk semua perangkat pendukung yang terdapat pada perusahaan
3	Melakukan pengelolaan terhadap enkripsi informasi	05.03.013	PT. XYZ harus melakukan perbaikan terhadap enkripsi informasi

4.1.4 Pengelolaan identitas pengguna dan akses logik

Tabel V- 4 Rekomendasi Layanan DSS 05.04

No	Ineffective Control	Control Reference	Rekomendasi
1	Melakukan perawatan terhadap hak akses yang sesuai terhadap fungsi bisnis,peran dan tanggung jawab	05.04.01	Perawatan hak akses yang dilakukan oleh PT. XYZ harus dapat memastikan informasi yang didapat oleh pengguna sudah sesuai dengan fungsi jabatan
2	Melakukan otentikasi akses ke aset informasi berdasarkan hak akses yang sudah diklasifikasikan untuk memastikan kontrol otentikasi berjalan sesuai dengan ketentuan	05.04.02	PT. XYZ melakukan otentikasi akses ke aset informasi harus menggunakan *identity management* dalam melindungi *user*
3	Melakukan implementasi pengelolaan identitas pengguna dan akses logik	05.04.04	Semua fungsi keamanan pada pengelolaan identitas dan akses harus dapat ditangani oleh pihak yang bertanggung jawab pada PT. XYZ
4	Melakukan pengelolaan hak	05.04.05	PT. XYZ harus menggunakan standar dalam

	akses		mengelola identitas pengguna dan akses logik

4.1.5 Pengelolaan akses fisik dan aset TI

Tabel V- 5 Rekomendasi Layanan DSS 05.05

No	Ineffective Control	Control Reference	Rekomendasi
1	Memastikan hanya pihak tertentu yang dapat memasuki situs IT(*server*,*data center*)	05.05.02	PT. XYZ harus melakukan pembaharuan informasi dalam menentukan pihak-pihak mana saja yang diperbolehkan masuk ke situs IT

4.1.6 Kesimpulan perhitungan *capability level*

Tabel V- 6 Rekomendasi perhitungan *capability level*

No	Rekomendasi
1	PT. XYZ membuat dokumentasi terkait proses kerja yang telah dilakukan
2	PT. XYZ telah membuat dokumentasi definisi terkait proses kerja yang dilakukan.
3	PT. XYZ melakukan pemantauan secara berkala terhadap proses kerja yang telah dilakukan
4	PT. XYZ melakukan dokumentasi terkait tugas, hak dan kewajiban setiap pihak yang bertanggung jawab dalam proses kerja yang telah dilakukan.

Tabel V- 7 Hasil Keseluruhan Perhitungan *Capability Level*

No	Layanan	*Level*
1	DSS 05.01	1
2	DSS 05.02	1
3	DSS 05.03	2
4	DSS 05.04	1
5	DSS 05.05	1
Rata-rata		1

4.2 Saran

Untuk penelitian selanjutnya :

1. Melakukan audit TI pada layanan lain seperti layanan surat dan jasa pada PT. XYZ.
2. Melakukan audit TI pada layanan lain menggunakan domain lain seperti, *Align, Plan and Organise.*

DAFTAR PUSTAKA

[1] G.J Simson, & Gene Spafford., 2005. *Practical UNIX & Internet Security* :*O'Reilly & Associates Inc. 2nd edition*.
[2] Gondodiyoto, S., 2007. Audit Sistem Informasi: Pendekatan Cobit, Edisi Revisi. Jakarta: Mitra Wacana Media.
[3] Gondodiyoto, Sanyoto, Henny Hendarti, Ariefah,. 2007. Pengolahan Fungsi Audit Sistem Informasi. Jakarta: Penerbit Mitra Wacana Media.
[4] Howard, John D., *An Analysis Of Security Incidents On The Internet 1989 - 1995*, *PhD thesis*, *Engineering and Public Policy*, Carnegie Mellon University, 1997
[5] ISACA., 2013. *COBIT 5 for Assurance.*
[6] ISACA., 2012 COBIT 5 *Enabling Process*, USA: ISACA
[7] ISACA., 2011 ISACA *issues COBIT process assessment model technology & business journal*
[8] ISACA., (2012) *COBIT 5*,U.S.A.
[9] ISO/IEC 17799:2005 diakses April 22, 2015, dari http://www.iso.org.
[10] ITIL Knowledge diakses April 22,2015, dari http://www.itiltraining.com.
[11] Keputusan Direksi PT. XYZ Nomor KD.18/DIRUT/0604 Tentang Rencana Strategis Teknologi Informasi (RSTI) pada PT. XYZ (Persero).
[12] Keputusan Direksi PT. XYZ Nomor: KD.20/DIRUT/0312 Tentang Penerapan Sistem Keamanan Informasi
[13] Kristanto, A., 2003. Perancangan Sistem Informasi dan Aplikasinya. Yogyakarta: Gava Media.
[14] Maniah & Surendro, K., 2005. Usulan Model Audit Sistem Informasi (Studi Kasus: Sistem Informasi Perawatan Pesawat Terbang).
[15] O'Brien, James A. 2005. Pengantar Sistem Informasi. Jakarta: Penerbit Salemba Empat.
[16] Peter Wood., 2005 *Implementing identity management security - an ethical hacker's view*.Network Security.
[17] Raharjo, Budi., Keamanan Sistem Informasi Berbasis Internet, Jakarta: PT Insan Infonesia.
[18] Sarno, Riyanarto. Iffano, Irsyat., 2009. Sistem Manajemen Keamanan Informasi berbasis ISO 27001. Surabaya: ITS Press
[19] Stallings, William., 2005. *Cryptography and Network Security Principles and Practices (4th Edition)* :Prentice Hall.
[20] Surat Edaran PT. XYZ Nomor: SE.09/DIRTEKJASGUNG Tentang Pengendalian hak akses.
[21] Surat Edaran PT. XYZ Nomor: SE.95/DIRTEKJASGUNG/1012 Tentang Implementasi Aplikasi *One Time Password.*
[22] Surat Edaran PT. XYZ Nomor: SE.102/DIRTEKJASGUNG/1112 Tentang Prosedur klarifikasi, *backup*, pelabelan, dan penghapusan data elektronik.
[23] Surat Edaran PT. XYZ Nomor: SE.96/DIRTEKJASGUNG/1012 Tentang Penggunaan sumber daya informasi berbasis teknologi informasi.
[24] Surat Edaran PT. XYZ Nomor: SE.86/DIRTEKJASGUNG Tentang Penerapan *Clear Desk and Clear Screen.*
[25] Surat Edaran PT. XYZ Nomor: SE.53 /DIRTEKJASGUNG Tentang Tata Cara Pengamanan *Password*.
[26] Weber, Ron., (2003). *Information System Control And Audit*. *Prentice Hall*.