Desain Sistem Keamanan Pada Infrastruktur Berbasis Jaringan Komputer di Universitas Kristen Petra

Ibnu Gunawan, Agustinus Noertjahyana
Prodi Teknik Informatika Universitas Kristen Petra
Siwalan Kerto 121 – 131 Surabaya, 60236
ibnu@petra.ac.id, agust@petra.ac.id

Untuk menjalankan proses akademik yang senantiasa berkembang, Universitas Kristen Petra mulai menggunakan banyak aplikasi. Banyak diantara aplikasi itu yang menggunakan system berbasis jaringan sehingga sistem yang ada saat ini menjadi semakin rentan terutama dalam hal keamanan. Sehingga diperlukan adanya suatu sistem keamanan yang dapat menjamin keamanan semua sistem informasi yang sudah ada, atau paling tidak mampu untuk meminimalisasi terjadinya serangan.

Pada makalah penelitian ini, akan ditunjukkan langkah langkah serta standard yang diambil beserta masalah di lapangan pada tahun pertama untuk mengembangkan sebuah sistem keamanan yang dapat membantu untuk melakukan desain sistem keamanan mulai dari desain kebijakan, prosedur, manajemen resiko sampai dengan sistem audit .

Hasil penelitian ini adalah pemilihan standard 10 domain CISSP dari banyaknya standard keamanan dalam dunia komputer, sebagai hasil dari pengassesan resiko berdasarkan standard NIST SP 800-39 yang merupakan sebagai pedoman utama dalam melakukan pengevaluasian sistem keamanan pada infrastruktur berbasis jaringan komputer.

Keywords-component; desain; sistem; keamanan; universitas; manajemen; resiko

I. PENDAHULUAN

Dalam menjalankan kegiatan operasional yang berbasis teknologi informasi, terlebih dengan menggunakan infrastruktur jaringan komputer, maka organisasi bukan hanya perlu untuk membuat suatu sistem informasi yang baik, namun juga perlu untuk mempertimbangkan faktor keamanan sebagai salah satu penunjang sistem informasi yang handal. Jaringan komunikasi yang aman mutlak diperlukan untuk menjaga agar supaya organisasi senantiasa mampu memberikan layanan secara terus menerus kepada para anggotanya. Kebutuhan akan sistem keamanan ini perlu untuk didefinisikan secara jelas dan pada akhirnya dapat diimplementasikan secara nyata untuk dapat menunjang kegiatan operasional pada sistem informasi suatu organisasi. Dengan menerapkan prosedur yang tepat untuk setiap aktifitas, maka diharapkan akan dapat dilakukan pengukuran yang tepat terhadap kebutuhan keamanan yang sesuai dengan apa yang dibutuhkan oleh organisasi [1]. Untuk dapat membangun kebijakan keamanan yang dapat memberikan landasan yang bagus pada keamanan sistem di masa yang akan datang, maka langkah awal yang mutlak harus dikembangkan adalah membuat kebijakan keamanan yang dapat mengurangi resiko terjadinya penyalahgunaan terhada sumber daya yang ada pada organisasi.

Langkah paling penting untuk dapat memulai implementasi kebijakan keamanan ini adalah dengan memberikan pemahaman serta pengenalan kepada semua pihak yang terlibat di dalam sistem, menjelaskan semua bentuk tanggung jawab terhadap sistem, hak untuk menggunakan sumber daya yang ada, serta menjelaskan secara detil bagaimana data yang sensitif dapat dilindungi secara sempurna. Hal ini tentu saja membutuhkan penjelasan secara detil terkait dengan kebijakan keamanan yang ada sampai dengan hal-hal yang tidak boleh dilakukan pada sistem. Hal ini dikenal dengan nama Information security governance [2]

Bagi sebagian besar staff yang memang berkecimpung dalam pembuatan kebijakan keamanan ini, seringkali merasa kebingungan untuk memulainya, dikarenakan memang belum mempunyai pengalaman yang cukup atau merasa tidak memerlukan hal tersebut dikarenakan memang belum ada kejadian terkait dengan masalah keamanan. Namun alangkah baiknya apabila berbagai macam jenis serangan dapat dicegah lebih awal untuk dapat memastikan bahwa sistem tetap dapat berjalan secara normal.

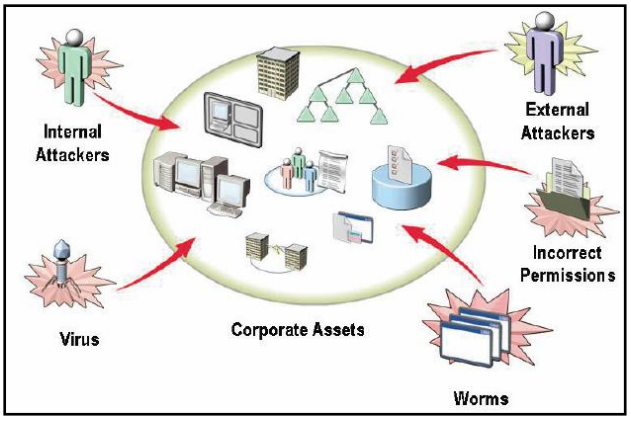
II. TEORI DASAR

A. Penelitian Sebelumnya yang Menunjang

Penelitian sebelumnya yang dilakukan oleh peneliti meliputi penelitian yang berhubungan dengan pemantauan lalu lintas jaringan dengan menggunakan library sharppcap yang bertujuan untuk dapat mengetahui apabila ada serangan virus yang melintas pada jaringan [3]. Untuk dapat mengerti tentang desain sistem keamanan maka peneliti juga menjadi trainer untuk Microsoft terkait dengan permasalahan tentang desain sistem keamanan yang berbasis pada Microsoft Framework. Penelitian mandiri dilakukan pada beberapa perusahaan terkait dengan implementasi desain sistem keamanan pada jaringan berbasis Microsoft.

B. *Desain Sistem Keamanan*

Banyak organisasi meremehkan nilai dari suatu aset IT yang dimiliki, hal ini dikarenakan biasanya IT merupakan biaya tidak langsung. Padahal, jika saja terjadi serangan pada server, maka akan bisa menyebabkan organisasi tidak bisa menjalankan aktifitasnya dengan baik. Serangan pada website dapat menyebabkan organisasi tidak bisa memberikan layanan informasi kepada para pengguna / pelanngan. Dengan demikian maka organisasi akan mengalami kerugian baik itu secara material maupun imaterial. Dengan melakukan desain sistem keamanan yang efektif, maka dapat membantu organisasi untuk dapat melindungi asetnya [4]. Gambaran dari hubungan antara serangan dan aset dapat dilihat pada gambar 1.



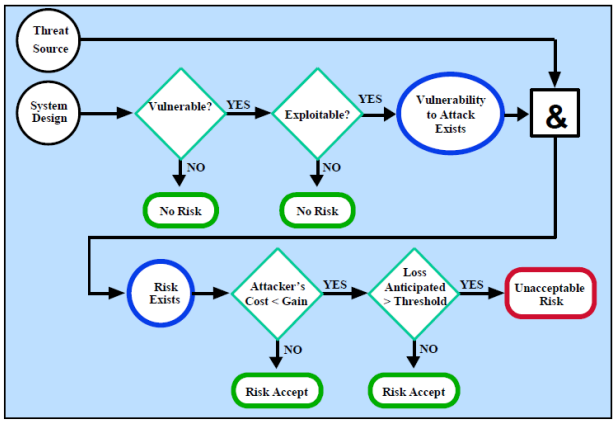
Gambar 1. Hubungan Aset dan Serangan

C. *Kebijakan Keamanan*

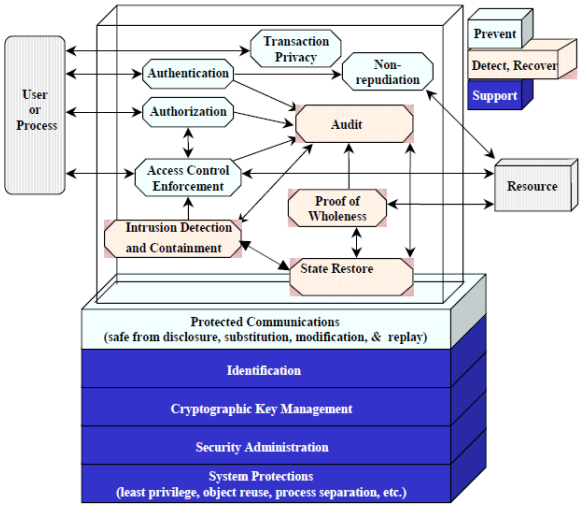
Kebijakan keamanan adalah suatu rencana, yang menjelaskan mengenai apa yang termasuk aset penting organisasi, dan bagaimana cara melindunginya [1]. Tujuan dari kebijakan keamanan ini adalah untuk memberikan penjelasan kepada pengguna sistem atas aset mana yang diijinkan untuk digunakan dan mana yang tidak boleh digunakan, dan untuk selanjutnya akan masuk ke dalam bagian dari sistem keamanan organisasi. Dokumen yang ada harus jelas sumbernya dan mudah bagi setiap pengguna untuk dapat mengerti dan memahami serta mendefinisikan sumber daya yang merupakan potensial target dari segala macam serangan.

D. *Manajemen Resiko*

Manajemen Resiko merupakan gabungan dari 3 proses [5] yaitu : Risk Assessment, Risk Mitigation dan evaluasi. Prosedur untuk melakukan Risk Mitigation dapat dilihat pada gambar 2. Dan prosedur untuk melakukan teknikal kontrol pada resiko dapat dilihat pada gambar 3.



Gambar 2. Risk Mitigation Strategy [5]



Gambar 3. Teknikal Kontrol [5]

III. DESAIN SISTEM KEAMANAN

A. *Tinjauan Sistem Saat Ini*

Kegiatan operasional yang dijalankan oleh Univeristas Kristen Petra senantiasa menggunakan Teknologi Informasi. Layanan yang diberikan kepada mahasiswa mulai dari pendaftaran secara online, penerimaan mahasiswa baru, kegiatan perkuliahan yang meliputi pendaftaran perkuliahan dan praktikum, layanan email baik itu untuk dosen dan mahasiswa, layanan sistem keuangan, sistem nilai online dan berbagai layanan lainnya semakin banyak menggunakan IT. Hal ini tentu membutuhkan perhatian yang lebih mendalam khususnya dalam hal sistem keamanan yang ada terkait dengan sistem IT.

Fokus saat ini adalah dengan menggabungkan beberapa aplikasi agar supaya dapat terintegrasi dengan sempurna sehingga tidak ada data yang terduplikasi. Hal ini tentu berdampak kepada meningkatnya penggunaan IT baik itu hardware dan software sehingga layanan yang ada semakin hari menjadi semakin lebih baik. Dengan koneksi internet yang semakin hari semakin cepat, saat ini sekitar 140 Mbps, sangat memungkinkan bagi UK Petra untuk senantiasa memberikan layanan aplikasi berbasis internet.

Untuk mempublikasikan hasil penelitian juga sudah menggunakan sistem online sehingga sangat memungkinkan pihak luar dapat melakukan akses terhadap hasil penelitian secara online.

Karena fokus yang ada saat ini masih kepada pengembangan aplikasi, maka kebutuhan akan sistem keamanan menjadi sedikit dilupakan. Sebagai contoh : dengan menggunakan sistem login yang terintegrasi, namun ada beberapa aplikasi yang belum memberikan pengamanan pada halaman login. Selain itu juga semua komputer yang ada masih memungkinkan menggunakan hak akses administrator setiap saat. Hal ini tentu bisa berdampak kepada masuknya virus ke dalam jaringan komputer yang dapat berakibat kepada menurunnya kinerja jaringan.

Permasalahan lain yang kelihatan adalah belum adanya informasi terkait dengan kebijakan keamanan yang ada pada Universitas Kristen Petra, serta prosedur untuk mengatasi masalah yang mungkin ditimbulkan karena kebobolan dalam sistem keamanan. Dokumen untuk manajemen resiko juga masih belum ada hingga saat ini sehingga sistem monitoring terhadap keamanan aplikasi juga masih belum dapat dilakukan dengan baik. Hal ini bisa menimbulkan permasalahan di kemudian hari apabila sampai terjadi hal-hal yang membahayakan sistem seperti misalnya pencurian data yang penting, pencurian server dan komputer serta penyerangan terhadap layanan yang diberikan.

Sebuah sistem informasi yang ideal adalah sebuah sistem yang senantiasa ditunjang oleh sistem keamanan yang baik dalam hal ini kebijakan keamanan dan prosedur yang dijalankan dengan baik sehingga dapat meminimalkan resiko yang mungkin terjadi serta dapat membantu dalam pengambilan keputusan terkait upgrade sistem di kemudian hari. Pemilihan sistem yang ideal akan dapat membantu mengurangi pengeluaran yang mungkin terjadi dikarenakan kesalahan dalam desain sistem keamanan.

Selain itu juga dengan adanya desain sistem keamanan serta dokumentasi yang baik maka dapat mempermudah divisi IT untuk senantiasa melakukan monitoring terhadap sistem IT dan dapat membantu mempermudah proses audit sistem informasi ketika dibutuhkan.

B. Risk Assesment

Risk Assesment merupakan salah satu komponen fundamental dari proses manajemen risiko organisasi seperti yang dijelaskan dalam NIST SP800-39.

Penilaian risiko dapat dilakukan di semua tiga tingkatan dalam hirarki-termasuk manajemen risiko Tier 1 (level organisasi), Tier 2 (misi / bisnis tingkat proses), dan Tier 3 (tingkat sistem informasi). Pada Tingkatan 1 dan 2, organisasi menggunakan penilaian risiko untuk mengevaluasi, misalnya, risiko dari sistem informasi yang berhubungan dengan keamanan yang terkait dengan kegiatan organisasi tata kelola dan manajemen, misi / proses bisnis, arsitektur perusahaan, atau dana program keamanan informasi. Pada Tier 3, organisasi menggunakan penilaian risiko untuk lebih efektif mendukung pelaksanaan Kerangka Kerja Manajemen Risiko (yaitu, kategorisasi keamanan; pemilihan kontrol keamanan, pelaksanaan, dan penilaian; sistem informasi dan otorisasi sepengendali, dan pemantauan keamanan kontrol). Tabel 1 menjelaskan tentang *Taxonomy of Predisposing Conditions*. Sedangkan Tabel 2 menjelaskan tentang Skala Penaksiran – *Pervasiveness of Predisposing Conditions.*

TABEL 1. TAXONOMY OF PREDISPOSING CONDITIONS

Tipe dari *Predisposing Condition*	**Deskripsi**
INFORMASI TERKAIT - Baris Informasi Keamanan Nasional - kompartemen - Informasi terklasifikasi Controlled - Informasi pribadi - Program Akses Khusus - Kesepakatan-Ditetapkan - NOFORN - Proprietary	Kebutuhan untuk menangani informasi (seperti yang dibuat, dikirim, disimpan, diproses, dan / atau ditampilkan) dengan cara tertentu, karena sensitivitasnya (atau kurangnya sensitivitas), persyaratan hukum atau peraturan, dan / atau perjanjian kontrak atau organisasi lainnya
TEKNIS • Arsitektur - Kepatuhan dengan standar teknis - Penggunaan produk tertentu atau lini produk - Solusi untuk dan / atau pendekatan kolaborasi berbasis pengguna dan berbagi informasi - Alokasi fungsi keamanan khusus untuk kontrol umum • Fungsional - Jaringan multiuser - *Single-user* - Stand-alone / *nonnetworked* - Fungsi terbatas (misalnya, komunikasi, sensor, controller tertanam)	Kebutuhan untuk menggunakan teknologi dengan cara tertentu.
OPERASIONAL / LINGKUNGAN • Mobilitas - Fixed-situs (sebutkan lokasi) - Semi-mobile - Tanah berbasis, Airborne, Laut berbasis, berbasis Angkasa - Mobile (misalnya, perangkat genggam) • Penduduk dengan akses fisik dan / atau logis untuk komponen dari sistem informasi, proses misi / bisnis, segmen	Kemampuan untuk mengandalkan fisik, prosedural, dan kontrol personel yang diberikan oleh lingkungan operasional

EA - Ukuran populasi - Izin / pemeriksaan penduduk	

TABEL 2. SKALA PENAKSIRAN - *PERVASIVENESS OF PREDISPOSING CONDITIONS*

NILAI KUALITATIF	***NILAI SEMI-KUANTITATIF***		***DESKRIPSI***
VERY HIGH	*96-100*	*10*	*BERLAKU UNTUK SEMUA MISI ORGANISASI / FUNGSI BISNIS (TIER 1), MISI / PROSES BISNIS (TIER 2), ATAU SISTEM INFORMASI (TIER 3)*
HIGH	*80-95*	*8*	*BERLAKU UNTUK SEBAGIAN BESAR MISI ORGANISASI / FUNGSI BISNIS (TIER 1), MISI / PROSES BISNIS (TIER 2), ATAU SISTEM INFORMASI (TIER 3)*
MODERATE	*21-79*	*5*	*BERLAKU UNTUK BANYAK MISI ORGANISASI / FUNGSI BISNIS (TIER 1), MISI / PROSES BISNIS (TIER 2), ATAU SISTEM INFORMASI (TIER 3)*
LOW	*5-20*	*2*	*BERLAKU UNTUK BEBERAPA MISI ORGANISASI / FUNGSI BISNIS (TIER 1), MISI / PROSES BISNIS (TIER 2), ATAU SISTEM INFORMASI (TIER 3)*
VERY LOW	*0-4*	*0*	*BERLAKU UNTUK SEDIKIT MISI ORGANISASI / FUNGSI BISNIS (TIER 1), MISI / PROSES BISNIS (TIER 2), ATAU SISTEM INFORMASI (TIER 3)*

C. CISSP

Dari pembelajaran tentang manajemen resiko menggunakan standard NIST SP 800-39 rev 1 itu diketahui bahwa salah standard tertinggi dalam dunia keamanan pada infrastruktur berbasis jaringan computer adalah CISSP. Tabel 3 berikut akan menjelaskan 10 domain CISSP yang digunakan untuk mengamankan atau meminimalisir resiko yang ditemukan menggunakan standard NIST SP 800-39 rev 1 di atas.

TABEL 3. 10 DOMAIN CISSP

`	**DESKRIPSI**
ACCESS CONTROL	DOMAIN INI MEMBAHAS MEKANISME DAN METODE YANG DIGUNAKAN UNTUK MENGAKTIFKAN ADMINISTRATOR DAN MANAJER UNTUK MENGONTROL APA YANG SUBYEK DAPAT MENGAKSES, SEJAUH MANA KEMAMPUAN MEREKA SETELAH OTORISASI DAN OTENTIKASI, DAN AUDIT DAN PEMANTAUAN KEGIATAN INI. BEBERAPA TOPIK YANG DIBAHAS MELIPUTI: • MODEL KEAMANAN *ACCESS CONTROL* • IDENTIFIKASI DAN OTENTIKASI TEKNOLOGI DAN TEKNIK • ADMINISTRASI *ACCESS CONTROL* • TEKNOLOGI *SINGLE SIGN-ON* • METODE SERANGAN
TELECOMMUNICATIONS AND NETWORK SECURITY	DOMAIN INI MEMBAHAS INTERNAL, EKSTERNAL, PUBLIK, DAN SWASTA SISTEM KOMUNIKASI, STRUKTUR JARINGAN, PERANGKAT, PROTOKOL, DAN AKSES REMOTE DAN ADMINISTRASI. BEBERAPA TOPIK DIBAHAS MELIPUTI: • MODEL OSI DAN LAPISAN • TEKNOLOGI *LOCAL AREA NETWORK* (LAN), *METROPOLITAN AREA NETWORK* (MAN), DAN *WIDE AREA NETWORK* (WAN) • INTERNET, INTRANET, DAN *EXTRANET ISSUES* • *VIRTUAL PRIVATE NETWORKS* (VPN), *FIREWALL, ROUTER, BRIDGES*, DAN *REPEATER* • JARINGAN TOPOLOGI DAN KABEL • METODE SERANGAN
INFORMATION SECURITY AND RISK MANAGEMENT	DOMAIN INI MENELITI IDENTIFIKASI ASET PERUSAHAAN, CARA YANG TEPAT UNTUK MENENTUKAN TINGKAT YANG DIPERLUKAN PERLINDUNGAN YANG DIPERLUKAN, DAN APA JENIS ANGGARAN UNTUK MENGEMBANGKAN UNTUK IMPLEMENTASI KEAMANAN, DENGAN TUJUAN MENGURANGI ANCAMAN DAN KERUGIAN KEUANGAN. BEBERAPA TOPIK YANG DIBAHAS MELIPUTI: • *DATA CLASSIFICATION* • *POLICIES, PROCEDURES, STANDARDS, AND GUIDELINES* • *RISK ASSESSMENT AND MANAGEMENT* • PERSONIL KEAMANAN, PELATIHAN, DAN KEPEDULIAN
APPLICATION SECURITY	DOMAIN INI MEMBAHAS KOMPONEN KEAMANAN DALAM SISTEM OPERASI DAN APLIKASI DAN BAGAIMANA MENGEMBANGKAN TERBAIK DAN MENGUKUR EFEKTIVITAS MEREKA. INI TERLIHAT PADA SIKLUS HIDUP PERANGKAT LUNAK, PENGENDALIAN PERUBAHAN, DAN KEAMANAN APLIKASI. BEBERAPA TOPIK YANG DIBAHAS MELIPUTI: • *DATA WAREHOUSING AND DATA MINING* • *VARIOUS DEVELOPMENT PRACTICES AND THEIR RISKS* • *SOFTWARE COMPONENTS AND VULNERABILITIES* • *MALICIOUS CODE*

CRYPTOGRAPHY	DOMAIN INI MEMBAHAS METODE DAN TEKNIK UNTUK MENYAMARKAN DATA UNTUK TUJUAN PERLINDUNGAN. HAL INI MELIBATKAN TEKNIK KRIPTOGRAFI, PENDEKATAN, DAN TEKNOLOGI. BEBERAPA TOPIK YANG DIBAHAS MELIPUTI: • ALGORITMA SIMETRIS DIBANDINGKAN ASIMETRIS DAN PENGGUNAAN • INFRASTRUKTUR KUNCI PUBLIK (PKI) DAN FUNGSI HASHING • PROTOKOL ENKRIPSI DAN IMPLEMENTASI • METODE SERANGAN

D. Survey dan analisa kebutuhan

Universitas Kristen Petra saat ini berkembang semakin pesat dengan salah satu misinya yaitu "*IT-based campus*" yang artinya penggunaan teknologi informasi semakin banyak dijumpai tidak hanya kalangan dosen, karyawan, maupun staff namun juga mahasiswa yang ada di dalamnya. Sebagai contoh, untuk sistem kepegawaian yang menggunakan aplikasi khusus, untuk sistem *input* nilai yang setiap dosen bisa memasukkan nilai secara *online*, sistem akademik yang memberikan layanan pendaftaran rencana studi mahasiswa secara *online*, serta sistem penunjang yang lain. Dengan contoh tersebut bisa dilihat semakin banyaknya sistem yang mulai ada dan dimana setiap pegawai ataupun mahasiswa menggunakan kode yang sama untuk setiap sistem, maka dalam hal ini diperlukan sebuah *security policy*.

Mengingat adanya permasalahan tersebut maka perlu dilakukan suatu analisa resiko terhadap resiko Teknologi Informasi yang bisa berdampak bagi kegiatan operasional Universitas Kristen Petra. Melalui analisa resiko pihak Universitas terutama pusat komputer yang menjadi sasaran kami dapat lebih mudah mengetahui resiko-resiko apa saja yang bisa terjadi, mengukur seberapa besar resiko tersebut dan bagaimana dampaknya, dan mendapatkan hasil perhitungan resiko manakah yang menjadi perhatian khusus hingga resiko yang tidak menjadi prioritas khusus. Dari perihal yang telah disebutkan itu maka pusat komputer dapat menangani segala permasalahan yang ada dan juga mengambil kebijakan dari hasil perhitungan resiko yang telah dilakukan. Dengan demikian sistem *security* pusat komputer dapat aman dan termonitor dengan baik.

Dari sanalah dapat diputuskan bahwa *requirement analysis* yang sebenarnya adalah sebagai berikut :

1. Software harus bisa mengetahui alur keluar masuk, proses, syarat, dan ketentuan keamanan yang ada di pusat komputer
2. Software harus bisa menentukan serta mem-*filter* permasalahan yang mungkin terjadi dalam sistem *security* di pusat komputer
3. Software harus bisa menentukan dampak yang mugkin terjadi dari permasalahan di dalam sistem *security* di pusat komputer
4. Software harus bisa menentukan sistem *security policy* yang diperlukan di pusat komputer

Setelah mengetahui daftar kebutuhan barulah bisa di buat sketsa tentang bagaimana user interface dari program dan dari sketsa user interface itu barulah bisa menelurkan sebuah schema database yang sedianya akan dilanjutkan pada bulan Desember sampai Januari awal.

IV. KESIMPULAN

Dari penelitian yang telah terlaksana sejauh ini dapat diambil beberapa kesimpulan penting diantaranya:

1. Standard CISSP ternyata merupakan pedoman utama dalam standard sistem keamanan pada infrastruktur berbasis jaringan komputer
2. Standard NIST SP 800-39 baik untuk dipakai sebagai pedoman utama dalam melakukan pengevaluasian sistem keamanan pada infrastruktur berbasis jaringan komputer
3. Dikarenakan sifat psikologis manusia yang selalu menuju ke yang lebih baik dan tentunya hal ini juga tertuang dalam revisi revisi policy keamanan sistem yang ada, maka dibutuhkan semacam timestamp untuk kriteria selesai audit sistem keamanan pada infrastruktur berbasis jaringan komputer

Dan juga saran yang terkait diantaranya:

1. Pada rencana tahap berikutnya akan disisipkan 1 goal tambahan yaitu kriteria selesai atau semacam timestamp seperti yang dijelaskan pada kesimpulan point 3 diatas

Sebaiknya peneliti juga mempunyai sertifikasi di bidang sistem keamanan pada infrastruktur berbasis jaringan computer misal CISSP untuk tolak ukur *state of the art* dari penelitian yang dilakukan.

DAFTAR PUSTAKA

[1] Danchev, Dancho. "Building and Implementing a Successful Information Securit Policy." Internet Software Marketing. Windows Security.com., 2003

[2] Conrad. Eric, Misenar. Seth, and Feldman. Joshua, "CISSP Study Guide", 2nd ed., Syngress, 2012.

[3] Noertjahyana, Agustinus., Andjarwirawan Justinus, Haryanto Tungary. "Visualisasi Lalu Lintas Jaringan Komputer dengan menggunakan library SharpPCap." Senaputro 2012. Surakarta.

[4] Bragg. Roberta, "MCSE Self Paced Training Kit (Exam 70-289) Designing Security for Microsoft Windows Server 2003." Microsoft Press 2003.

[5] Stoneburner. Gary, Alice. Goguen, and Alexis. Feringa, "Risk Management Guide for Information Technology System." NIST Special Publication 800-30. 2002.