Analisa Keamanan Sistem Informasi RSUD Dr. Soetomo Dengan Framework COBIT

Theodorus Natanael [1], Leo Willyanto Santoso [2], Agustinus Noertjahyana [3]
Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jl. Siwalankerto 121-131, Surabaya 60236
Telp. (031)-2983455, Fax. (031)-8417658
E-mail: theodorusnatanael@gmail.com [1], leow@petra.ac.id [2], agust@petra.ac.id [3]

ABSTRAK

RSUD Dr. Soetomo termasuk salah satu rumah sakit terbesar di Surabaya. Maka dari itu, kompleksitas sistem informasi di RSUD Dr. Soetomo terbilang sangat kompleks dan mencakup wilayah yang sangat luas. Dengan kompleksitas yang dimiliki ini maka menambahkan risiko yang dimiliki oleh sistem informasi RSUD Dr. Soetomo. Melihat pentingnya data di dalam sistem informasi RSUD Dr. Soetomo, maka pengelolaan keamanan TI perlu diperhatikan.

Untuk melaksakan analisa Sistem Informasi tersebut, perlu memiliki standar yang baik untuk dapat dibandingkan dengan standar milik Rumah Sakit. Kerangka kerja *Control Objective for Information and Related Technology* (COBIT) mempunyai tujuan untuk mengendalikan TI terkait dan merupakan standar yang telah diakui cukup baik pada tingat internasional.

Masalah-masalah yang dihadapi oleh TI RSUD Dr. Soetomo adalah tidak adanya surat tugas, tidak ada laporan tertulis, belum adanya penanggulangan risiko, belum dijabarkannya maksud, tujuan, dan ruang lingkup pekerjaan dari *IT Security*. Perusahaan dapat meningkatkan performa keamanan sistem informasi dengan panduan-panduan yang memiliki standar yang baik seperti ISO, NIST, CNSSI.

Kata Kunci: COBIT, Keamanan, RSUD Dr. Soetomo, Standar, Sistem Informasi.

ABSTRACT

RSUD Dr. Soetomo is one of the largest hospitals in Surabaya. Therefore, the complexity of information systems in RSUD Dr. Soetomo is very complex and covers a very wide area. With this complexity, it adds the risks possessed by RSUD Dr. information system. Soetomo. See the importance of data in information systems RSUD Dr. Soetomo, then the management of IT security needs to be considered.

To implement the analysis of the Information System, it is necessary to have a good standard to be comparable with the standards of the Hospital. The Control Objective for Information and Related Technology (COBIT) framework has a goal to control IT related and is a well-recognized standard in international level.

Problems faced by IT RSUD Dr. Soetomo is the absence of a letter of assignment, no written report, no risk mitigation, unfulfilled intent, purpose, and scope of work from IT Security. Companies can improve the security performance of information systems with guidelines that have good standards such as ISO, NIST, CNSSI.

Keywords: *COBIT, Security, RSUD Dr. Soetomo, Standard, Information System.*

1. PENDAHULUAN

Teknologi Informasi sudah berkembang ke dalam dunia kesehatan. Hal ini, dibuktikan, dengan adanya sistem informasi yang membantu proses di sebuah rumah sakit. Sistem informasi pada rumah sakit mengatur banyak data antara lain data pasien, riwayat penyakit, obat, dokter, dll. Perlu sebuah sistem yang kompleks untuk mengolah semua data-data tersebut. Namun, penerapan TI membutuhkan biaya yang cukup besar dengan risiko kegagalan yang tidak kecil, yaitu bila terjadi gangguan pada TI yang dimiliki. Risiko yang ada bukan hanya pada sistem informasi saja namun pada data yang berada pada sistem informasi tersebut. Penerapan TI didalam sebuah rumah sakit dapat membantu seluruh pelayanan di rumah sakit tersebut namun selain itu dapat menjadi sebuah ancaman ketika tidak diikuti dengan keamanan yang *secure* dan baik. Keamanan yang rendah dapat membuat data pasien yang krusial menjadi mudah untuk disalahgunakan oleh orang-orang yang tidak bertanggung jawab. Data pasien merupakan data yang sangat penting dan rahasia dan data pasien dilindungi dalam pasal 47 UU Praktik Kedokteran *(*1) Dokumen rekam medis sebagaimana dimaksud dalam Pasal 46 merupakan milik dokter, dokter gigi, atau sarana pelayanan kesehatan, sedangkan isi rekam medis merupakan milik pasien. (2) Rekam medis sebagaimana dimaksud pada ayat (1) harus disimpan dan dijaga kerahasiaannya oleh dokter atau dokter gigi dan pimpinan sarana pelayanan kesehatan. (3) Ketentuan mengenai rekam medis sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dengan Peraturan Menteri.

RSUD Dr. Soetomo merupakan rumah sakit milik pemerintah Indonesia yang berada di kota Surabaya, Jawa Timur. RSUD Dr. Soetomo termasuk salah satu rumah sakit terbesar di Surabaya yang memiliki 1.505 tempat tidur untuk pasien. Maka dari itu, kompleksitas sistem informasi di RSUD Dr. Soetomo terbilang sangat kompleks dan mencakup wilayah yang sangat luas. Dengan kompleksitas yang dimiliki ini, maka menambahkan resiko yang dimiliki oleh sistem informasi RSUD Dr. Soetomo. Melihat pentingnya data di dalam sistem informasi RSUD Dr. Soetomo, maka pengelolaan keamanan TI pun perlu diperhatikan. Untuk melaksakan analisa Sistem Informasi tersebut, perlu memiliki standar yang baik untuk dapat dibandingkan dengan standar milik Rumah Sakit. Kerangka kerja *Control Objective for Information and Related Technology* (COBIT) mempunyai tujuan untuk mengendalikan TI terkait dan merupakan standar yang telah diakui cukup baik pada tingat internasional. Dalam analisa ini dibahas 1 Domain yang ada di dalam COBIT yaitu *Deliver and Support* dengan pembahasan yang dibatasi pada tingkat *Ensure System Security* (*DS* 5).

2. TINJAUAN PUSTAKA

2.1. Keamanan Sistem Informasi

Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Selain itu, keamanan sistem informasi bisa diartikan sebagai kebijakan, prosedur, dan pengukuran teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan program, pencurian, atau kerusakan fisik terhadap sistem informasi. Sistem pengamanan terhadap teknologi informasi dapat ditingkatkan dengan menggunakan teknik-teknik dan peralatan-peralatan untuk mengamankan perangkat keras dan perangkat lunak komputer, jaringan komunikasi, dan data [1].

2.2 Pengelolaan Teknologi Informasi

Pengelolaan teknologi informasi (*IT Governance*) adalah struktur kebijakan atau prosedur dan kumpulan proses yang bertujuan untuk memastikan kesesuaian penerapan TI dengan dukungannya terhadap pencapaian tujuan perusahaan, dengan mengoptimalkan keuntungan dan kesempatan yang ditawarkan TI, mengendalikan penggunaan *IT resources* dan mengelola risiko-risiko terkait TI (IT Governance Institute, 2000).

Fokus pengelolaan TI terdiri dari lima area, yaitu *strategic alignment*, *value delivery*, *resource management*, *risk management* dan *performance management*.

Detail penjelasan dari area fokus pengelolaan TI adalah sebagai berikut:

- *Strategic Alignment*
  Area ini berfokus untuk menjalin hubungan antara bisnis dan *IT plans*, yaitu dalam mendefinisikan, merawat dan mengesahkan nilai *IT* dan dalam menyesuaikan operasi-operasi *IT* dengan operasi-operasi di dalam perusahaan.
- *Value Delivery*
  Area ini berkaitan dengan persoalan nilai, dengan melaksanakan seluruh siklus pengiriman, serta menjamin bahwa keberadaan *IT* memberi keuntungan dalam strategi perusahaan, melalui pengoptimalan biaya dan memberikan nilai intrinsik dari *IT*.
- *Resource Management*
  Area ini berkaitan dengan pengoptimalan investasi di dalam perusahaan dan manajemen sebelumnya dan sumber daya *IT* yang vital, yaitu *applications*, *information*, *infrastructure* dan *people*.
- *Risk Management*
  Di dalam area ini dibutuhkan kesadaran akan risiko oleh *senior corporate officer*, di dalam pemahaman tentang risiko perusahaan, kebutuhan pelaksanaan, keterbukaan tentang risiko yang signifikan bagi perusahaan dan menanamkan tanggungjawab manajemen risiko dalam perusahaan.
- *Performance Management*
  Area ini menelusuri dan memonitor implementasi strategi, penyelesaian proyek, penggunaan *resource*, kinerja proses, dan layanan pengiriman (*service delivery*). Contohnya menggunakan *balance scorecard*, yang menterjemahkan strategi ke dalam suatu tindakan untuk mencapai tujuan-tujuan (*goals*) yang dapat diukur melalui perhitungan tradisional (*conventional accounting* [5].

2.3 Poliklinik

Menurut Huffman (1994), pelayanan rawat jalan adalah pelayanan yang diberikan kepada pasien yang tidak mendapatkan pelayanan rawat inap di rumah sakit atau institusi pelayanan kesehatan (Dwiastari, 2016).

Secara sederhana yang dimaksud dengan pelayanan rawat jalan adalah pelayanan kedokteran yang disediakan untuk pasien tidak dalam bentuk rawat inap (*hospitalization*). Pelayanan rawat jalan ini termasuk tidak hanya yang diselenggarakan oleh sarana pelayanan kesehatan yang telah lazim dikenal sebagai rumah sakit atau klinik, tetapi juga yang diselenggarakan di rumah pasien (*home care*) serta di rumah perawatan (*nursing homes*). Bentuk pertama dari pelayanan rawat jalan adalah yang diselenggarakan oleh klinik yang ada kaitannya dengan rumah sakit (*hospital based ambulatory care*). Jenis pelayanan rawat jalan di rumah sakit secara umum dapat dibedakan atas 4 macam yaitu:

1. Pelayanan Gawat Darurat (*Emergency Services*)
   adalah untuk menangani pasien yang butuh pertolongan segera dan mendadak
2. Pelayanan Rawat Jalan Paripurna (*Comprehensive Hospital Outpatient Services*)
   adalah yang memberikan pelayanan kesehatan paripurna sesuai dengan kebutuhan pasien
3. Pelayanan Rujukan (*Referral Services*)
   adalah hanya melayani pasien-pasien rujukan oleh saran akesehatan lain. Biasanya untuk diagnosis atau terapi, sedangkan perawatan selanjutnya tetap ditangani oleh sarana kesehatan yang merujuk.
4. Pelayanan Bedah Jalan (*Ambulatory Surgery Services*)
   adalah memberikan pelayanan bedah yang dipulangkan pada hari yang sama [3]

2.4 Control Objective for Information and Related Technology (COBIT)

Control Objective for Information and Related Technology (COBIT) merupakan kerangka kerja untuk tata kelola teknologi informasi. Pada sekitar tahun 1990 ISACA dan ITGI yang merupakan sebuah perusahaan menyusun kerangka kerja COBIT. Pertama kalinya COBIT diterbitkan tahun 1996 kemudian diterbitkan kembali tahun 1998 hingga pada tahun 2000 diterbitkan untuk ketiga kalinya dan untuk tahun 2005 diterbitkan COBIT keempat.

COBIT merupakan standar yang berisi panduan mengenai tata kelola teknologi informasi. Kerangka kerja COBIT merupakan kerangka kerja yang digunakan untuk mengidentifikasi kontrol TI di suatu perusahaan bagi seorang auditor sedangkan bagi pengguna kerangka kerja COBIT dapat menambah kepercayaan *user* terhadap kehandalan aplikasi. Pada *top management*, COBIT dapat digunakan untuk mengambil keputusan yang berkaitan dengan investasi teknologi informasi. Suatu organisasi dapat dikatakan sukses membangun TI dalam kerangka sistem informasi yang lengkap apabila telah memenuhi kriteria ukuran informasi. Kerangka kerja COBIT merupakan kumpulan panduan yang digunakan untuk acuan dalam menentukan proses TI dan *control objective* yang diperlukan dalam pengeloaan TI [2].

3. METODOLOGI PENELITIAN

3.1 RSUD Dr. Soetomo

Rumah Sakit Umum Daerah Dr. Soetomo Surabaya merupakan rumah sakit kelas A yang berdiri di atas tanah dengan luas 163.875 m^2 dan luas bangunan 98.121 m^2. RSUD Dr. Soetomo tidak hanya untuk melayani pengobatan, melainkan juga sebagai rumah sakit pendidikan, penelitian dan pusat rujukan tertinggi untuk wilayah Timur. Hal ini sesuai dengan SK. Menkes 51/Menkes/SK/1179 RSUD Dr. Soetomo.

Rumah Sakit secara umum memiliki etika bisnis berbeda dengan bidang perusahaan. Karena dalam rumah sakit perlu memperhatikan etika berupa pemberi pelayanan kesehatan, sebagai pemberi pekerjaan, dan dapat membantu dengan memberikan tunjangan kepada orang-orang miskin. Secara tidak langsung, rumah sakit sebagai wadah pelayanan masyarakat dalam kesehatan memberikan prioritas kesehatan kepada setiap pasien tidak memandang dari sisi keuangan namun dari sisi kemanusiaan dimana nyawa setiap pasien sangat berharga. Pada RSUD Dr. Soetomo etika bisnis sejalan dengan etika pelayanan kesehatan.

Hal ini, tidak bisa terlepas begitu saja dimana rumah sakit perlu biaya dalam bidang kesehatan seperti investasi alat penunjang, dokter, perawat, dan obat-obatan namun rumah sakit juga perlu dalam merawat pasien dan semaksimal mungkin untuk memulihkan keadaan pasien seperti sediakala. Selain itu, diperlukan biaya yang besar dalam pembuatan aplikasi penunjang pelayanan di rumah sakit. Dimana etika bisnis yang sejalan dengan etika pelayanan kesehatan adalah dengan memprioritaskan pasien dan memberikan pelayanan yang terbaik dengan memberikan bantuan atau tunjangan kepada pasien yang tidak mampu dan memberikan harga standar kepada pasien yang mampu. Dan juga adanya peran aktif pemerintah dalam memberikan anggaran kesehatan yang cukup sehingga dapat membantu semua orang yang kekurangan dalam biaya kesehatan [4].

4. HASIL DAN PEMBAHASAN

4.1 Hasil

DS5.1 : Assurance With Modification
DS5.2 : Assurance With Modification
DS5.3 : Assurance
DS5.7 : Assurance With Modification
DS5.8 : Non Assurance

4.2 Pembahasan

4.2.1 DS5.1 Management of IT Security

Pada DS5.1 dapat dilihat bahwa TI RSUD Dr. Soetomo sudah memaparkan inti dari manajemen dari TI sendiri, seperti tujuan, ruang lingkup, tangung jawab, risiko, dan performa. Namun, didalam tujuan dari TI RSUD Dr. Soetomo masih hanya sebatas umum belum mengklasifikasikan secara detail mengenai keamanan sistem informasi. Pada ruang lingkup juga belum terlihat jelas mengenai hal yang dilakukan mengenai keamanan sistem informasi, cara-cara menangani sebuah risiko, walaupun sudah dilakukan monitoring. Pada tanggung jawab keamanan sudah dijelaskan dalam tiga point dan masih belum adanya sanksi jika melakukan kesalahan, dan tim keamanan hanya menjalankan sedikit tugas keamanan dan lebih banyak menjalankan tugas yang diluar keamanan sistem. Untuk risiko secara spesifik TI RSUD Dr. Soetomo belum mengelompokkan dan belum adanya tindakan preventif untuk menanggualangi risiko. Hal ini terlihat pada tahun 2014 saat terjadi hack kepada website RSUD Dr. Soetomo. Sedangkan performa keamanan sangat terbatas karena hampir 90% dikelola oleh pihak ketiga, namun dari hasil wawancara dengan wakil TI RSUD Dr. Soetomo bahwa pada tahun 2018 TI akan mengambil peranan hingga 50% dan ini akan lebih mudah untuk dijangkau sehingga keamanan TI dan SI akan lebih terjamin dan mudah untuk dilakukan tindakan preventif ketika terjadi sebuah serangan.

Pada kebijakan keamanan TI sudah sesuai dengan persyaratan bisnis dengan mengacu pada Peraturan Menteri Kesehatan namun secara individual RSUD Dr. Soetomo belum memiliki peraturan tambahan dalam persyaratan bisnis melalului kebijakan keamanan TI.

TI RSUD Dr. Soetomo sudah memiliki struktur organisasi, fungsi pengelolaan, dan administrasi keamanan. Untuk keamanan dikelola dibawah koordinator strategi & arsitektur enterprise yaitu *Data Center* & *Security*. Namun, pada pengelolaan keamanan TI masih sangat minim dan melalui hasil wawancara bahwa tim keamanan TI ini lebih banyak membantu untuk menyelesaikan masalah sehari-hari di TI RSUD Dr. Soetomo seperti membantu rumah sakit dalam mengelola website, memperbaiki jaringan, dan proyek lapangan. Untuk struktur organisasi TI sendiri banyak *staff* yang memiliki dua sampai tiga jabatan sehingga pengerjaan tidak terfokus.

4.2.2 DS5.2 IT Security Plan

Untuk mekanisme pelaporan TI RSUD Dr. Soetomo belum pernah melakukan dan belum ada pencatatan resmi mengenai laporan. Tim TI biasanya hanya menyampaikan secara lisan pada rapat rutin yang dilakukan satu bulan satu kali dengan pimpinan TI. Namun, rapat rutin ini terkadang tidak dihadiri oleh semua tim TI dikarenakan ada proyek lapangan, ataupun ada panggilan dari rumah sakit mengenai error sistem ataupun masalah jaringan. Sehingga tidak semua permasalahan dapat disampaikan secara lisan perlu adanya pelaporan tertulis. Pelaporan tertulis dimaksudkan supaya permasalahan dapat dituliskan secara detail dan rinci sehingga ada rekomendasi yang tepat dari kepala TI dan bagain terkait mengenai permasalahan yang terjadi.

TI RSUD Dr. Soetomo memiliki kebijakan dan standar keamanan sesuai dengan TIA-942, namun hal ini baru dilakukan pada periode ke-3 (triwulan) pada tahun 2017 sedangkan tentang *recovery planning* baik dari segi *disaster*, hack, dan gangguan lainnya baru akan dilakukan pada periode pertama (triwulan) pada tahun 2018. Sehingga masih dalam tahapan proses mengenai kebijakan dan standar keamanan. Untuk pelatihan keamanan masih belum pernah dilakukan, namun untuk pelatihan jaringan, software, dan hardware sudah dilakukan. Untuk investasi keamanan TI jumlahnya sangat kecil dan keamanan tidak digolongkan menjadi prioritas pada TI RSUD Dr. Soetomo.

4.2.3 DS5.3 Identity Management

TI RSUD Dr. Soetomo sudah mengidentifikasi, mengautentikasi, dan memberikan otorisasi sesuai dengan jobdesk yang dikerjakan sehingga hak akses diberikan kepada user yang tepat. Pemberian hak akses dilakukan secara manual dan di review secara berkala yaitu 3 bulan sekali. Review dilakukan untuk mengecek hak akses yang dilakukan oleh user sekaligus melakukan pergantian ataupun pencanutan hak akses jika memang dibutuhkan. Perlu juga dilakukan sesuai dengan standar ISO 27000 mengenai *access control* dimana ada standar dan peraturan mengenai pemberian hak akses, pencabutan hak akses, dan identifikasi ketika *user* salah memasukkan *password* misalnya sebanyak tiga kali. Dengan adanya standar baku mengenai hak akses dan identifikasi *user*

maka akan lebih terjamin mengenai keamanan dan mengurangi risiko penyalahgunaan hak akses.

4.2.4 DS5.7 Protection of Security Technology

Belum dilakukan Algoritma enkripsi. Menurut ISO/ IEC 18033-3: 2005, Tujuan utama teknik enkripsi (atau encipherment) adalah untuk melindungi kerahasiaan data yang tersimpan atau dikirim. Algoritma enkripsi diterapkan pada data (sering disebut plaintext atau cleartext) untuk menghasilkan data terenkripsi (atau ciphertext); Proses ini dikenal sebagai enkripsi. Enskripsi membantu menambah perlindungan terhadap data-data penting terlebih RSUD Dr. Soetomo merupakan rumah sakit terbesar di Jawa Timur yang memiliki banyak dokumen. Proteksi pada keamanan teknologi sangat diperlukan karena sensitifitas data, dan program yang sangat kompleks akan menjadi terganggu jika sistem yang ada sampai terkena sebuah serangan seperti hack. Pemulihan akan memakan waktu yang cukup lama. Maka dari itu, sangat diperlukan proteksi yang perlu dievaluasi dimana evaluasi keamanan sangat diperlukan dan perlu untuk melakukan kajian dimana evaluasi dapat dilakukan minimal tiap bulan.

4.2.5 DS5.8 Cryptographic Key Management

Belum dilakukan Algoritma enkripsi. Menurut ISO/ IEC 18033-3: 2005, Tujuan utama teknik enkripsi (atau encipherment) adalah untuk melindungi kerahasiaan data yang tersimpan atau dikirim. Algoritma enkripsi diterapkan pada data (sering disebut plaintext atau cleartext) untuk menghasilkan data terenkripsi (atau ciphertext); Proses ini dikenal sebagai enkripsi. Enskripsi membantu menambah perlindungan terhadap data-data penting terlebih RSUD Dr. Soetomo merupakan rumah sakit terbesar di Jawa Timur yang memiliki banyak dokumen. Proteksi pada keamanan teknologi sangat diperlukan karena sensitifitas data, dan program yang sangat kompleks akan menjadi terganggu jika sistem yang ada sampai terkena sebuah serangan seperti hack. Pemulihan akan memakan waktu yang cukup lama. Maka dari itu, sangat diperlukan proteksi yang perlu dievaluasi dimana evaluasi keamanan sangat diperlukan dan perlu untuk melakukan kajian dimana evaluasi dapat dilakukan minimal tiap bulan.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil analisa yang telah dilakukan, dapat diambil beberapa kesimpulan antara lain:

- Divisi TI perlu melakukan evaluasi khususnya pada keamanan supaya lebih diprioritaskan supaya tidak terjadi gangguan keamanan sistem informasi sesuai dengan standar ISO khususnya ISO 27001 mengenai keamanan sistem informasi.
- Perlu adanya tambahan standar yang mengatur mengenai sistem keamanan pada TI RSUD Dr. Soetomo seperti NIST.

5.2 Saran

Saran yang dapat diberikan untuk penyempurnaan dan pengembangan analisa ini antara lain:

- Penggunaan COBIT 5.0 yang lebih disempurnakan
- RSUD Dr. Soetomo perlu menganalisa kesiapan IT dengan menggunakan standar ISO 27001 tentang *IT Security*

6. DAFTAR PUSTAKA

[1] D., Karina 2013. Keamanan Sistem Informasi. Retrieved October 29, 2017 from http://karina-d-p-fisip11.web.unair.ac.id/artikel_detail-79279-Tugas%20-Keamanan%20Sistem%20Informasi.html

[2] IT Governance Institute. Retrieved September 4, 2017 from https://www.isaca.org/KnowledgeCenter/cobit/Documents/COBIT4.pdf

[3] Poliklinik. Retrieved September 7, 2017 from http://erepo.unud.ac.id/18995/3/1306013007-3BAB%20II.pdf

[4] RSUD Dr. Soetomo. Retrieved September 4, 2017 from http://rsudrsoetomo.jatimprov.go.id/id/

[5] Suryana, Elsa 2013. *Keamanan Sistem Informasi*. Retrieved October 29, 2017 from http://elsa-suryana-fisip12.web.unair.ac.id/artikel_detail-79306-Umum Keamanan%20Sistem%20Informasi.html