 ISSN:2302-8149
e-ISSN:2540-9719

Penilaian Manajemen Risiko TI Menggunakan *Quantitative* dan *Qualitative Risk Analysis*

Andry Gerson Rinding Padang, Awalludiyah Ambarwati*, Eman Setiawan
Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama
Jl. Arief Rachman Hakim No.51 Surabaya 60117, Telp (031)5946404, 5995578, Fax. (031)5931213
*e-mail: ambarwati1578@yahoo.com

(***received*:** 16 Maret 2021, ***revised*:** 22 Juni 2021, ***accepted*:** 13 Juli 2021)

Abstrak

Menurut Pepres no. 95 Tahun 2018, rumah sakit diwajibkan memiliki dan menggunakan teknologi informasi dalam segala pelayanannya. Instalasi IT (*Information Technology*) merupakan unit departemen pada RSUD XYZ yang memiliki fungsi dalam mengatur dan mengelola semua penggunaan TI (Teknologi Informasi) dalam rumah sakit, untuk menjauhkan hal yang tidak diinginkan butuh penilaian manajemen risiko buat meminimalkan ancaman atau risiko yang bisa terjadi. Metode Analisis yang digunakan pada penelitian ini ada dua yaitu *Quantitative* dan *Qualitative Risk Analysis*. Dimana nantinya untuk metode QRA (*Quantitative Risk Analysis*) lebih fokus pada analisis perawatan aset TI untuk menemukan faktor risiko yang memerlukan penanganan utama dan perhatian khusus. Sedangkan untuk metode *qualitative Risk Analysis* menggunakan panduan NIST SP 800-30 untuk menganalisis berbagai atribut ancaman dan risiko, agar dapat menghasilkan rekomendasi kontrol pada Instalasi IT RSUD XYZ. Hasil penelitian dari penilaian risiko menurut metode QRA, ditemukan bahwa ada pada aset TI jenis *Server* mempunyai perhitungan untuk menjadi potensi kerugian terburuk bagi rumah sakit. Hal ini dapat dilihat dari aspek risiko dimana kehilangan daya listrik mempunyai potensi kerugian terbesar. Untuk penilaian manajemen risiko kualitatif dengan NIST SP 800-30 menunjukkan bahwa sumber ancaman listrik dan jaringan internet memiliki tingkat risiko yang tinggi. Tingkat risiko ini bisa didapati pada waktu proses pengolongan sumber-sumber ancaman. Saat semua hasil analisis risiko sudah dikemukakan, hal itu dapat memberikan hasil rekomendasi risiko untuk diberikan kepada pihak management ataupun instalasi IT. Untuk nantinya dapat membantu manajemen senior dalam membuat keputusan tentang kebijakan, prosedur, anggaran, dan operasional sistem dan perubahan manajemen.

Kata kunci: qualitative risk analysis, nist sp 800-30, penilaian manajemen risiko, aset ti

Abstract

According to Perpres no. 96 of 2018, hospitals are required to have and use information technology in all their services. The IT installation is a departmental unit at XYZ Hospital which has a function in regulating and managing all IT usage in the hospital. To stay away from unwanted things, a risk management assessment is needed to minimize any threats or risks that can occur. There are 2 methods of analysis used in this study, namely Quantitative and Qualitative Risk Analysis. Which later for the Quantitative Risk Analysis (QRA) method, it focuses more on analyzing IT asset maintenance to find risk factors that require primary handling and special attention. Meanwhile, the Qualitative Risk Analysis method uses the NIST SP 800-30 guide to analyze various threat and risk attributes, in order to produce control recommendations on the XYZ Hospital IT Installation. The results of the research from the risk assessment according to the QRA method, it was found that the server type IT assets have calculations to be the worst potential loss for the hospital. This can be seen from the aspects of the risks (threats) where the loss of electrical power has the greatest potential loss. The qualitative risk management assessment using NIST SP 800-30 shows that the threat of electricity and internet networks has a high level of risk. When all the results of the risk analysis have been presented, it can provide the results of risk recommendations to be given to the management or IT installation.

Keywords: *qualitative risk analysis, nist sp 800-30, risk management assessment, it asset*

 ISSN:2302-8149
e-ISSN:2540-9719

1 Pendahuluan

Teknologi Informasi (TI) kini memegang banyak peranan di dalam berbagai bidang organisasi maupun perusahaan. Bahkan terkadang memiliki peran yang sangat penting dalam menunjang secara efisiensi dan efektifitas proses bisnis daripada organisasi atau perusahaan tersebut. Terlebih di era pandemi sekarang ini, peranan TI menjadi sangat dibutuhkan, karena segala sesuatu pekerjaan atau bisnis yang dilaksanakan membutuhkan proses yang *paperless* dan daring, seperti halnya pada Rumah Sakit Umum Daerah (RSUD) yang sudah mulai menjalankannya pada proses bisnis dan pelayanan. RSUD juga dituntut untuk dapat menjalankan segala proses pelayanannya menjadi berbasis elektronik sesuai dengan Pepres No. 95 Tahun 2018 [1], tentang Sistem Pemerintah Berbasis Elektronik (SPBE). Dengan adanya Pepres tersebut, rumah sakit diwajibkan memiliki dan menggunakan TI dalam segala pelayanannya, seperti sistem informasi manajemen rumah sakit, ataupun untuk pendataan pasien pada rumah sakit. Hal ini juga tertuang pada Permenkes No. 82 Tahun 2013 yang menyatakan bahwa setiap rumah sakit wajib menyelenggarakan sistem informasi manajemen rumah sakit (SIMRS) [2]. Untuk itu pengunaan TI pada segala proses pelayanan rumah sakit pasti juga dapat menimbulkan berbagai kendala dan ancaman risiko teknologi informasi yang seluruhnya dapat mempengaruhi kualitas pelayanan serta bisa berakibat pada tingkat kepercayaan masyarakat pada kualitas rumah sakit tersebut. Bermacam risiko TI yang hadir ataupun yang bisa jadi mencuat di area rumah sakit telah selayaknya disadari oleh pihak manajemen serta disiapkan strategi untuk mengatur berbagai macam risiko tersebut. Terlebih di dalam standart akreditasi rumah sakit Indonesia, juga disebut dalam pelayanan kesehatan, teknologi juga dibutuhkan sebagai sarana pembantu pelayanan lebih mudah [3].

Instalasi IT (*Information Technology*) merupakan unit departemen pada RSUD XYZ yang memiliki fungsi dalam mengatur dan mengelola penggunaan TI dalam rumah sakit. Unit Instalasi IT ini berperan penting dalam berjalannya seluruh proses kegiatan bisnis atau pelayanan yang menggunakan TI, akan tetapi rumah sakit belum menerapkan implementasi identifikasi risiko TI secara berkala serta terperinci. Pemeliharaan aset TI yang tidak tepat dapat memunculkan berbagai risiko untuk Unit Instalasi IT. Berdasarkan wawancara kepada Kepala IT Unit Instalasi IT RSUD XYZ, terdapat beberapa permasalahan yang pernah terjadi di RSUD XYZ. Kerusakan pada komputer dan komputer yang tidak dapat menyala saat jam operasional dikarenakan belum dilakukannya perawatan secara berkala, sehingga menghambat pekerjaan tenaga medis dan layanan pasien. Selain itu terjadinya kegagalan sistem yang mengakibatkan kerusakan data dokter, data pasien dan data penunjang lainnya sehingga data tersebut tidak dapat diakses dan ditampilkan oleh sistem. Unit Instalasi IT RSUD XYZ belum melakukan penilaian risiko TI yang dilakukan secara berkala. Untuk menghindari kejadian tersebut berulang kembali dan mencegah terjadinya risiko TI yang lain, perlu dilakukan penilaian manajemen risiko TI pada RSUD XYZ.

Penelitian ini bertujuan untuk melakukan analisis perawatan aset TI menggunakan *quantitative risk analysis* dan melakukan analisis berbagai atribut risiko dan ancaman agar mendapatkan mitigasi risiko yang bisa mencegah timbulnya masalah atau kerugian pada Unit Instalasi IT menggunakan *qualitative risk analysis*. Penerapan *quantitative risk analysis* dan *qualitative risk analysis* digunakan untuk mendapatkan rekomendasi manajemen risiko TI yang lebih lengkap secara kuantitatif dan kualitatif bagi Unit Instalasi IT pada RSUD XYZ. Hasil penelitian ini memberikan manfaat bagi Unit Instalasi IT pada RSUD XYZ berupa daftar risiko aset TI beserta hasil analisis risiko secara kuantitatif dan kualitatif sebagai landasan melakukan mitigasi risiko.

2 Tinjauan Literatur

Penelitian terdahulu yang relevan merupakan sesuatu yang memiliki kaitan dan juga hubungan erat dengan pokok permasalahan yang dijelaskan pada judul penelitian ini. Hal itu juga menjadi dasar pembanding agar nantinya dapat memahami kendala yang dahulu ditemukan, lalu mengembangkannya menjadi lebih maju lagi. Penerapan TI hingga pemanfaatan TI harus diiringi dengan pengelolaan yang tepat sasaran sehingga nantinya dapat meminimalisir terjadinya kerugian pada proses bisnis. Dari hasil analis awal menunjukkan dalam satu tahun ancaman terdapat dua ancaman terbesar yang menyerang aset TI, yang pertama adalah Kerugian Daya (*Power Loss*) dan yang kedua Kerugian Komunikasi (*Communication Loss*). Namun setelah dilakukan kalkulasi nilai koefisien dampak dalam nilai finansial (rupiah), menemukan bahwa aspek risiko Kesalahan Tidak Disengaja (*accidental errors*) ternyata menjadi potensi kerugian terbesar bagi perusahaan. Penelitian

 ISSN:2302-8149
e-ISSN:2540-9719

ini belum melakukan *Analysis Control* atau analisia pengendalian risiko yang tepat dan akurat untuk dapat bisa mengurangi nilai potensi kerugian aset TI pada perusahaan dan juga seharusnya dapat dilakukan rekomendasi pengendalian risiko terhadap aset TI kedepannya [4].

Penelitian berikutnya, penyediaan sistem informasi yang dibutuhkan oleh para mahasiswa, dan permasalahan dalam sistem informasi akademik Universitas XYZ, berkaitan dengan kerentanan keamanan informasi yang dapat membuat kebutuhan akan keberlanjutan sistem menjadi semakin penting. Apabila masalah ini tidak dapat di atasi secara terus menerus, akibatnya akan berdampak atau resiko terhadap keberlangsungan sistem (khususnya akademisi). NIST SP 800-30 telah terbukti memberikan lebih banyak kontribusi, seperti: memberikan pembuat keputusan, wawasan keamanan informasi yang konsisten dan komprehensif, pemodelan sumber daya terstruktur, dan wawasan keamanan informasi yang dapat diterima oleh berbagai pemangku kepentingan penentu ancaman dapat diidentifikasi. Pada penelitian ini menggunakan NIST SP 800-26 sebagai *tools* tambahan identifikasi oleh peneliti, nantinya hasil dokumentasi berbasis keamanan informasi. Penelitian tersebut belum memberikan rekomendasi kontrol, dimana pada tahapan ini seharusnya dapat mengkontrol, mengurangi, atau bahkan menghilangkan risiko yang teridentifikasi. Tujuan dari pengendalian direkomendasikan karena adalah untuk mengurangi tingkat risiko pada sistem TI dan datanya ke tingkat yang lebih dapat diterima, setelah itu bisa melanjutkan ketahap berikutnya yaitu mitigasi risiko, evaluasi, dan penilaian risiko [5].

Metode analisis risiko kuantitatif (*Quantitative risk analysis*) yaitu metode analisis risiko yang menggunakan angka numerik untuk menyatakan dampak dan probabilitas. Kuantitatif, dimana estimasi nilai risiko dihubungkan dengan penerapan ukuran numerik - nilai sumber daya didefinisikan dalam jumlah, frekuensi terjadinya ancaman dalam jumlah kasus, dan kerentanan dengan nilai probabilitas kerugiannya, metode tersebut menyajikan hasil dalam bentuk indikator. Tahapan pada QRA (*Quantitative Risk Analysis*) meliputi tujuh tahapan penting [6][7], antara lain: (1) menentukan ruang lingkup penelitian. (2) Menetapkan harga dari setiap aset TI yang dipunyai, yang memiliki fungsi teknologi. (3) Menentukan risiko atau ancaman, dari aset yang sudah dievaluasi diidentifikasi potensi sumber ancaman dan sumber risiko, lalu menyusun daftar. (4) Menentukan koefisien dampak, dengan melaksanakan identifikasi kerentanan aset TI terhadap risiko tertentu atau bahkan tidak sama sekali, Analisis kerentanan aset TI dicoba untuk mengenali *Exposure Factor* (EF), (5) Evaluasi kelompok, (6) Melakukan perhitungan, (7) dan yang terakhir melakukan Analisis dengan menjumlahkan nilai-nilai yang didapat pada *spreadsheet.*

Metode analisis risiko kualitatif menggunakan panduan NIST SP 800-30, dimana pada tahapan ini nantinya dapat digunakan untuk mencari rekomendasi risiko, tahapan yang beberapa peneliti di atas belum menggunakannya. Penggunaan metode NIST ini dikarenakan untuk menganalisis faktor-faktor di luar perawatan aset TI, yakni lebih fokus pada risiko atau ancaman kepada Unit Instalasi IT. Penelitian sebelumnya menggunakan satu metode dalam melakukan analisis risiko. Penelitian ini menggunakan dua metode yaitu *quantitative risk analysis* dan *qualitative risk analysis* sehingga memberikan hasil analisis penilaian risiko yang lebih baik dan dapat saling mengisi kekurangan satu dan lainya dalam menganalisis penilaian risiko. Analisis kuantitatif digunakan untuk mencari faktor-faktor dalam perawatan aset TI, sedangkan analisis kualitatif lebih kepada mencari ancaman atau risiko yang nantinya akan dihadapi pada Instalasi IT di RSUD tersebut.

3 Metode Penelitian

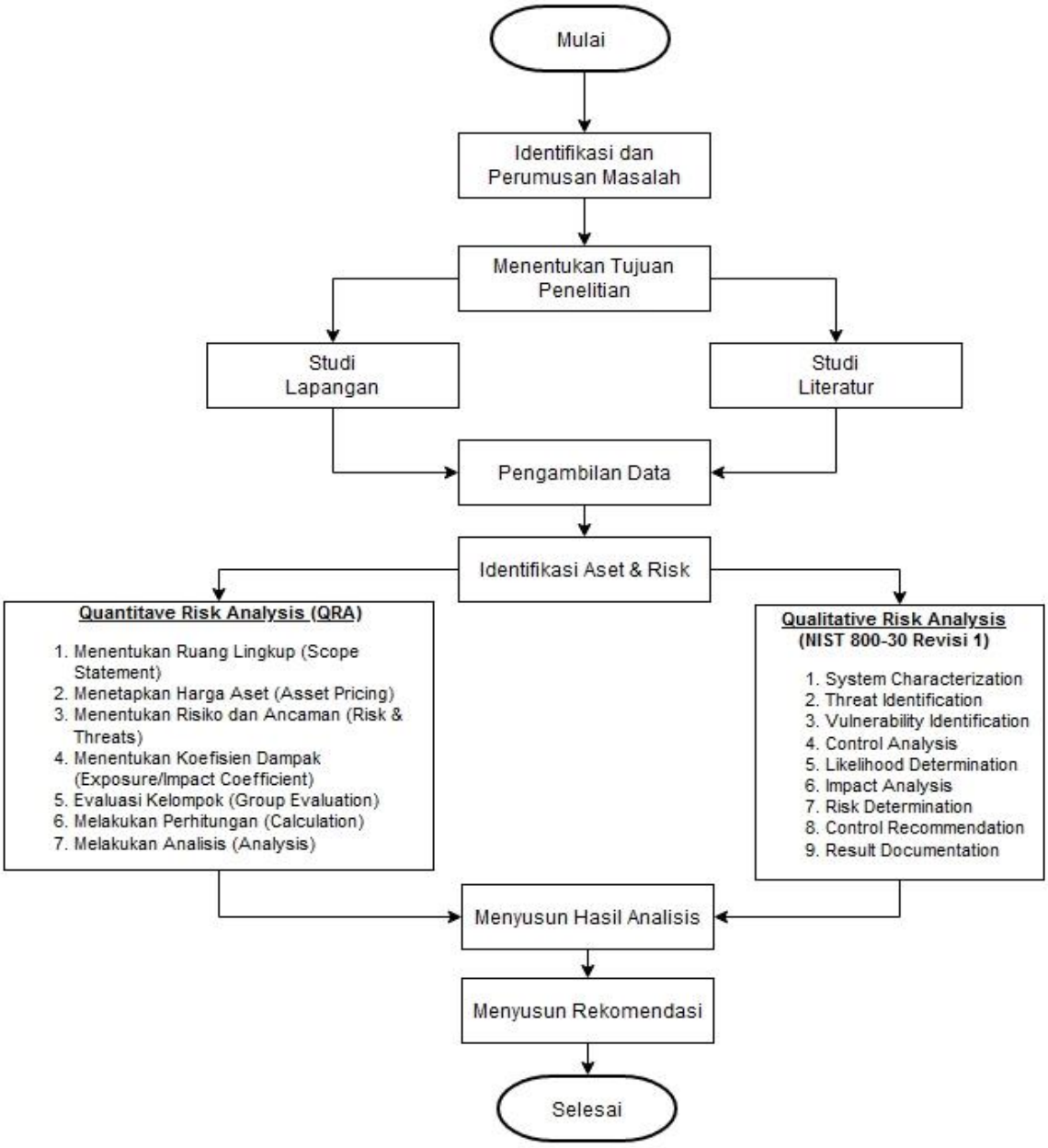
Penelitian ini dilakukan berdasarkan data kualitatif dan kuantitatif. Gambar 1 adalah tahapan penelitian yang dilakukan. Subjek penelitian ini adalah Instalasi IT yang berada pada salah satu Rumah Sakit Umum Daerah (RSUD) yang berlokasi di wilayah Jawa Timur. Pengambilan data penelitian diambil dari Kepala Instalasi IT dan juga Teknisi IT Komputer di RSUD tempat penelitian. Penelitian ini berfokus kepada pembahasan mengenai Risiko TI baik itu untuk aset TI maupun di Instalasi IT itu sendiri, bukan kepada Rumah Sakitnya, oleh karena itu nama daripada rumah sakit tempat dilakukan penelitian dirahasiakan (*confidential*).

Sebagian besar data penelitian adalah data yang relevan dan dapat dipercaya dan dapat dipertanggungjawabkan hasilnya. Sumber data berupa data sumber primer, yaitu data dari tempat Instalasi IT RSUD XYZ dengan melakukan wawancara langsung kepada Kepala Unit IT. Data sekunder berasal dari instansi di luar Instalasi IT RSUD XYZ.

 ISSN:2302-8149
e-ISSN:2540-9719

Teknik pengumpulan data yang digunakan dalam penelitian ini ada beberapa cara yaitu survei, *Google Form* (bit.ly/ITRISK-01 dan bit.ly/ITRISK-02) yang ditujukan kepada Kepala dan staff teknisi IT di Instalasi IT RSUD XYZ mengenai hal-hal yang berhubungan dengan manajemen risiko dan aset TI. *Interview* atau wawancara kepada Kepala Instalasi IT RSUD XYZ dan juga beberapa teknisi IT di RSUD XYZ menggunakan media daring berupa *whatsapp* dan e-mail, dan terakhir menggunakan teknik observasi.

Bagian dari analisis risiko adalah membuat kategori penilaian risiko. Proses penilaian risiko ini dapat dilakukan secara kualitatif dan kuantitatif [8]. Proses analisis dengan dua metode yaitu analisis risiko kuantitatif menggunakan metode *Quantitative Risk Analysis* (QR*A)* yang memiliki tujuh tahapanan dalam menganalisis risiko. Sedangkan untuk analisis risiko kualitatif menggunakan metode NIST SP 800-30. Dalam NIST SP 800-30 terdapat juga tahapan-tahapan analisis yang dapat membantu menemukan masalah dan menghasilkan rekomendasi risiko pada Instalasi IT RSUD XYZ.



Gambar 1. Tahapan Penelitian

 ISSN:2302-8149
e-ISSN:2540-9719

4 Hasil dan Pembahasan

Identifikasi Aset & Risk

Proses identifikasi risiiko harus dilakukan secara komprehensif atau menyeluruh agar nantinya risiko dapat dinilai secara sistematis. Proses ini dimulai dari mengidentifikasi berbagai kemungkinan risiko yang muncul dan terjadi di Instalasi *Information Technology* (IT)[15]. Pada penelitian ini pengelola aset TI, dalam hal ini Kepala Teknisi Instalasi memberikan spesifikasi dan juga jumlah aset TI yang dimiliki oleh Instalasi IT RSUD XYZ. Beberapa jenis aset TI yang dimiliki seperti server, *router, desktop, laptop, printer,* dan *monitor* seperti yang disajikan pada Tabel 1.

Quantitative Risk Analysis

Tahap awal analisis, menentukan ruang lingkup. Lokasi berupa Gedung Instalasi IT yang terletak di wilayah salah satu RSUD di Jawa Timur. Total aset TI yang dianalisis adalah aset sejak bulan Juli 2020 sampai Januari 2021, dengan tipe aset TI meliputi *server, router, monitor, desktop, laptop* dan *printer*. Tahap berikutnya, menentukan harga aset TI. Tabel 1 menyajikan harga aset TI yang disurvei adalah harga pembelian awal aset TI.

Tahap berikutnya menentukan risiko dan ancaman dengan memberikan nilai ARO (*Annualize Rate Occurance*). ARO diperoleh dari perhitungan persentase ancaman yang terjadi dalam jangka 1 tahun di Instalasi IT RSUD XYZ [9], hal ini terpapar pada Tabel 2. Tabel 3 menyajikan nilai *Exposure Factor* (EF) pada setiap aset TI. Disinilah letak perhitungan rumitnya mulai muncul, karena harus menghitung nilai koefisien dampak jenis aset TI satu persatu.

Tabel 1. Penentuan Harga Aset TI

Tipe Aset	Jumlah Aset (Unit)	Harga per Unit (Rp)	Total Harga (Asset Value)
Server	7	125.000.000	875.000.000
Router	5	16.500.000	82.500.000
Desktop	6	8.000.000	48.000.000
Laptop	2	25.000.000	50.000.000
Printer	2	1.500.000	3.000.000
Monitor	6	750.000	4.500.000
Jumlah			1.063.000.000

Sumber: Hasil penelitian, diolah kembali

Tabel 2. Ancaman dalam satu tahun

No	Ancaman (Threats)	ARO
1	Kehilangan Daya Listrik (*Power Loss*)	1.2
2	Kehilangan Komunikasi (*Network Loss*)	1.2
3	Kesalahan tidak sengaja (*Accidental Error*)	0
4	*Virus* Komputer	0.2
5	Pembobolan Hak Akses	0.3
6	Bencana Alam	0.2
7	Penghancuran atau pencurian Aset TI	0.1
8	Akses Paksa dari Luar ke Sistem (*Hack*)	0
9	Penghentian Proses Perangkat TI diluar Bencana	0
10	Kebakaran	0.01
11	Gempa Bumi	0.01

Sumber: Hasil penelitian, diolah kembali

Tabel 4 menyajikan kalkulasi perhitungan dari koefisien dampak aset TI dengan *asset value* (Table 1). Hasil *Single Loss Expetancy* (SLE) dikalkulasi dengan *Annualized Loss Expetancy* (ALE). SLE adalah nilai kerugian terhadap aset TI bila sebuah risiko yang teridentifikasi terjadi. Sedangkan ALE adalah merupakan nilai estimasi kerugian pertahun terhadap aset TI, jika sebuah risiko yang teridentifikasi terjadi [10]. Nilai ALE ada dua yaitu ALE *current* (ALE sebelum menerapkan *safeguards*) dan ALE *projected* (ALE setelah menerapkan *safeguards*)[11].

$$SLE = Asset\ Value\ \times Exposure\ Factor\ (EF) \quad (1)$$

 ISSN:2302-8149
e-ISSN:2540-9719

$$ALE = SLE \times ARO \quad (2)$$

Untuk rumus (1), *asset value* merupakan nilai finansial masing-masing aset TI yang telah ditetapkan nilainya dalam tahap *asset pricing*. Sedangkan *Exposure Factor* (EF), merupakan nilai presentase kehilangan akibat ancaman yang terjadi terhadap aset TI, pada EF memiliki rentang nilai antar 0 hingga 1. Lalu pada rumus (2), *Annualized Rate Occurrence* (ARO), merupakan nilai prosentase potensi setiap *threat* untuk setiap aset TI dalam satu tahun.

Tabel 3. Koefisien Dampak Aset TI

No	Ancaman (Threats)	EF					
		Server	Router	Desktop	Monitor	Laptop	Printer
1	Kehilangan Daya Listrik (*Power Loss*)	0.3	0.3	0.3	0.3	0.5	0.3
2	Kehilangan Komunikasi (*Network Loss*)	0.3	0.0	0.3	0.0	0.0	0.0
3	Kesalahan tidak sengaja (*Accidental Error*)	0.5	0.3	0.3	0.5	0.5	0.5
4	*Virus* Komputer	0.0	0.0	0.0	0.0	00	0.0
5	Pembobolan Hak Akses	0.3	0.3	0.3	0.0	0.3	0
6	Bencana Alam	1	1	1	1	1	1
7	Penghancuran atau pencurian Aset TI	1	1	1	1	1	1
8	Akses Paksa dari Luar ke Sistem	0.3	0.0	0.5	0.0	0.3	0.0
9	Penghentian Proses Perangkat TI diluar Bencana	0.3	0.3	0.3	0.3	0.3	0.3
10	Kebakaran	1	1	1	1	1	1
11	Gempa Bumi	1	1	1	1	1	1

Sumber: Hasil penelitian, diolah kembali

Tabel 4. Kalkulasi Asset Value, Exposure Factor, ALE

No	Ancaman (Threats)	EF					
		Server (Rp)	Router (Rp)	Desktop (Rp)	Monitor (Rp)	Laptop (Rp)	Printer (Rp)
1	Kehilangan Daya Listrik	315.000.000	29.700.000	17.280.000	18.000.000	1.800.000	1.620.000
2	Kehilangan Komunikasi	315.000.000	0	17.280.000	0	0	0
3	Kesalahan tidak sengaja	0	0	0	0	0	0
4	Virus komputer	0	0	0	0	0	0
5	Pembobolan Hak Akses	78.750.000	7.425.000	4.320.000	0	270.000	0
6	Bencana Alam	175.000.000	16.500.000	9.600.000	10.000.000	600.000	900.000
7	Penghancuran atau pencurian Aset TI	87.500.000	8.250.000	4.800.000	5.000.000	300.000	450.000
8	Akses Paksa dari Luar ke Sistem	0	0	0	0	0	0
9	Penghentian Proses Perangkat TI diluar Bencana	0	0	0	0	0	0
10	Kebakaran	8.750.000	825.000	480.000	500.000	30.000	45.000
11	Gempa Bumi	8.750.000	825.000	480.000	500.000	30.000	45.000
	TOTAL	988.750.000	63.525.000	54.240.000	34.000.000	3.030.000	3.060.000

Sumber: Hasil penelitian, diolah kembali

Setelah semua dikalkulasikan, hasilnya dapat digunakan untuk mencari aset TI mana yang memiliki potensi kerugian finansial terbesar, perlu dilakukan *Analysis Across Asset* dengan meranking jumlah total kalkulasi nilai ALE berdasarkan pengurutan jenis aset TI masing-masing mulai dari yang terbesar sampai terkecil. Sebaliknya jika ingin mencari jenis ancaman mana yang merugikan perusahan tinggal meranking jumlah total kalkulasi nilai ALE berdasarkan ancaman masing-masing (*Across Risk*). Dari Tabel 4 diketahui Nilai *Across Asset* tertinggi adalah Server sebesar Rp. 988.750.000 sedangkan Nilai *Across Asset* terendah adalah Laptop senilai Rp 3.030.000. Nilai *Across Risk* tertinggi adalah kehilangan daya listrik (*power loss*) senilai Rp 383.400.000, berikutnya adalah kehilangan komunikasi (*network loss*) senilai Rp 332.280.000. Terdapat empat ancaman yang memiliki Nilai *Across Risk* nol rupiah yaitu kesalahan tidak sengaja (*accidental error*), virus komputer, akses paksa dari luar ke sistem (*hack*) dan penghentian proses perangkat TI di luar bencana.

Qualitative Risk Analysis

Metode Qualitative risk analysis yang digunakan merupakan metode NIST SP 800-30. Metode itu dipilih karena hanya NIST SP 800-30 yang dapat memberikan rekomendasi kontrol pada langkah-langkah analisis risikonya. Tahap awal pada NIST SP 800-30 adalah *System Characterization* atau karakterisasi system. Karakterisasi sistem Teknologi Informasi (TI) menetapkan ruang lingkup upaya penilaian risiko, menggambarkan batasan otorisasi operasional (atau akreditasi), dan memberikan informasi (misalnya, perangkat keras, perangkat lunak, konektivitas sistem, dan divisi yang bertanggung jawab atau personel pendukung). Tabel 5 menampilkan Identifikasi terhadap ancaman (*Threat Identification*).

Tabel 5. Identifikasi Ancaman pada Instalasi IT

Sumber Ancaman	Keterangan Ancaman	Kode Ancaman
Banjir	Sistem Mati, Data Hilang, Infrastruktur Instalasi IT Rusak	A1.1
Gempa Bumi	Sistem Mati, Data Hilang, Infrastruktur Instalasi IT Rusak	A2.1
Listrik	Komputer / Server Mati	A3.1
	Gangguan Tegangan Listrik (Naik Turun)	A3.2
	AC di Ruangan Instalasi Mati	A3.3
	Modem dan Router Mati	A3.4
	Sistem Mati dan Data Hilang	A3.5
Kebakaran	Kebakaran Gedung Instalasi IT	A4.1
Jaringan Internet	Gangguan Jaringan Internet hingga Koneksi Terputus	A5.1
SDM - Internal	Penyalahgunaan Data dari Internal	A6.1
	Kesalahan Input Data (*Human Error*)	A6.2
	Penyalahgunaan Hak Akses dari Internal	A6.3
SDM - Eksternal	Kebocoran Data / Informasi oleh pihak eksternal	A7.1
	Pencurian / Perusakan Aset TI pada Instalasi IT	A7.2
	Hacker / Peretas	A7.3
Sistem & Infrastruktur TI	*Server Down*	A8.1
	Sistem Crash	A8.2
	Overload or Overcapacity Server	A8.3
	Back Up Failure	A8.4
	Gagal *Update Software*	A8.5
	Teknologi Usang (Tidak *Up-to-Date*)	A8.6

Sumber: Hasil penelitian, diolah kembali

Selanjutnya bersama dengan para responden membuat daftar identifikasi kerentanan (*Vulnerability Identification*) terhadap ancaman dan sumber ancaman, kemudian dilakukan diskusi hasil identifikasi kerentanan sesuai dengan yang terjadi di lapangan. Tabel 6 menyajikan hasil diskusi perihal apa saja kerentanan yang akan muncul jika ada ancaman tersebut.

Tahap berikutnya adalah analisis kontrol (*Control Analysis*), hasil observasi pelaksanaan analisis kontrol yang nantinya untuk meminimalkan terjadinya ancaman. Daftar analisis kontrol terdiri dari aturan-aturan atau manajemen-manajemen baru maupun lama yang menaungi jika terjadi kerentanan

 ISSN:2302-8149
e-ISSN:2540-9719

pada Instalasi IT RSUD. Contohnya: Pelatihan dan Sosialisasi tentang IT dan Sistem Informasi, Manajemen *Back-up*, Panduan Standar Operasional Prosedur (SOP) baru dalam penanganan Ancaman TI. Tahap kelima adalah Penentuan Kemungkinan (*Likelihood Determination*), setelah hasil dari analisis risiko dipenuhi, dari situ dapat dijadikan acuan dalam menentukan kemungkinan risiko. Ada 3 tingkatan kategori yaitu *Low* (0.1), *Medium* (0.5), *High* (1) [12]. Penentuan kemungkinan ini untuk menentukan besaran tingkat kemungkinan yang akan terjadi terhadap risiko yang telah teridentifikasi [13].

Tabel 6. Identifikasi Ancaman pada Instalasi IT

Sumber Ancaman	Keterangan Ancaman	Kode Ancaman	Kerentanan	Kode Kerentanan
Listrik	Komputer / Server Mati	A3.1	Terbatasnya *Unit Power System* (UPS)	K1.1
	Gangguan Tegangan Listrik (Naik Turun)	A3.2	Tidak adanya *Genset* sebagai Cadangan Listrik	K1.2
	AC di Ruangan Instalasi Mati	A3.3	*Genset* yang tidak langsung menyala (Respon Lambat)	K1.3
	Modem dan Router Mati	A3.4	Tidak adanya jaringan *Wireless* cadangan	K1.4
	Sistem Mati dan Data Hilang	A3.5	Tidak ada *Recovery data* pada Sistem	K1.5
Kebakaran	Kebakaran Gedung Instalasi IT	A4.1	Tidak adanya Pelatihan tentang SOP pencegahan kebakaran	K2.1
Jaringan Internet	Gangguan Jaringan Internet hingga Koneksi Terputus	A5.1	Tidak ada jaringan internet cadangan lainnya	K3.1
SDM- Internal	Penyalahgunaan Data dari Internal	A6.1	Peraturan untuk Pegawai kurang detail dan jelas	K4.1
	Kesalahan Input Data (Human Error)	A6.2	Tidak ada Pelatihan atau Sosialisasi pengunaan data.	K4.2
	Penyalahgunaan Hak Akses dari Internal	A6.3	Tidak adanya pengecekan Rutin *Log* Akses.	K4.3
SDM - Eksternal	Kebocoran Data / Informasi oleh pihak eksternal	A7.1	Tidak ada *legal unit* yang mengatasi ancaman di luar	K5.1
	Pencurian / Perusakan Aset TI Instalasi IT	A7.2	Tidak adanya penjagaan tambahan terhadap aset TI	K5.2
	Hacker / Peretas	A7.3	Tidak adanya keamanan tambahan pada sistem	K5.3
Sistem & Infrastruktur TI	*Server Down*	A8.1	Tidak ada backupan Host Lain	K6.1
	Sistem Crash	A8.2	Keterlambatan staff IT dalam memperbaharui sistem	K6.2
	Overload or Overcapacity Server	A8.3	Tidak dibatasinya orang yang mengakses *database server*.	K6.3
	Back Up Failure	A8.4	Tidak adanya jadwal teratur *back-up server*	K6.4
	Gagal *Update Software*	A8.5	Keterlambatan staff IT dalam mengupdate *software*	K6.5
	Teknologi Usang (Tidak *Up-to-Date*)	A8.6	Tidak adanya rencana pembelanjaan teknologi baru yang diajukan ke pihak Managemen RSUD	K6.6

Sumber: Hasil penelitian, diolah kembali

Tahap selanjutnya yaitu penentuan risiko (*risk determination*). Tujuan dari langkah ini adalah untuk menilai tingkat risiko pada sistem TI. Penentuan risiko untuk pasangan ancaman atau kerentanan tertentu dapat dinyatakan sebagai fungsi dari besarnya dampak jika sumber ancaman berhasil mengatasi kerentanannya [14]. Kecukupan kontrol keamanan yang direncanakan atau yang

 ISSN:2302-8149
e-ISSN:2540-9719

ada untuk mengurangi atau menghilangkan risiko. Untuk mengukur risiko, skala risiko (*risk scale*) dan matriks tingkat risiko (*risk level matrix)* harus dikembangkan lihat Tabel 7. Penentuan akhir dari mengukur risiko diperoleh dengan mengalikan peringkat yang ditetapkan untuk kemungkinan ancaman (*threat likelihood*) dan dampak ancaman (*impact*) [15].

Tabel 7. Matriks Tingkat Risiko [12]

Threat Likehood	**IMPACT**		
	Low (10)	Medium (50)	High (100)
High (0.1)	Low 10 X 0.1 =10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 50 X 0.5 = 25
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Tabel 8. Penentuan Risiko

Jenis Risiko	**Nilai Kemungkinan Ancaman**	**Nilai Dampak**	**Nilai Risiko**	**Tingkat Risiko**
Listrik	Tinggi (1)	Rendah (10)	10	Rendah
Jaringan Internet	Rendah (0.1)	Rendah (10)	1	Rendah
SDM-Internal	Tinggi (1)	Tinggi (100)	100	Tinggi
SDM-External	Sedang (0.5)	Tinggi (100)	50	Sedang
Sistem & Infrastruktur TI	Sedang (0.5)	Tinggi (100)	50	Sedang

Sumber: Hasil penelitian, diolah kembali

Tabel 9. Kontrol Rekomendasi pada RSUD XYZ

Jenis Risiko	**Tingkat Risiko**	**Rekomendasi**
Listrik	Rendah	Permintaan Penambahan Unit UPS pada beberapa server
		Mempersiapkan Genset biar lebih cepat respon
		Pengecekan Rutin Tanggal Service AC
		Membeli VSAT sebagai cadangan Internet
		Manajemen Back Up diperbaharui
Jaringan Internet	Rendah	Mempersiapkan Cadangan Jaringan
SDM- Internal	Tinggi	Peraturan pada SDM lebih disosialisasi lagi
		Pelatihan Skill & Sosialisasi Pegawai
		Penjadwalan Pengecekan Log History lebih Rutin
SDM - Eksternal	Sedang	Memindahkan Data ke Server Cloud yang lebih terjamin
		Sistem Keamanan CCTV Diperbaharui
		Sistem Keamanan Server di Tingkatkan
Sistem & Infrastruktur TI	Sedang	Sedia cadangan Host / Server Cloud
		Penjadwalan Restart Sistem berkala
		Pembatasan jumlah orang yang mengakses
		Manajemen Backup
		Menyiapkan cadangan software
		Mengajukan pembelian unit peralatan baru ke RSUD

Sumber: Hasil penelitian, diolah kembali

Penentuan risiko ini bertujuan untuk menilai tingkat risiko terhadap sistem, untuk menilai tingkat risiko ini mengacu kepada kemungkinan risiko dan dampak risiko yang sudah ditentukan [16]. Berdasarkan tahapan-tahapan sebelum penentuan risiko didapatkan yang ditentukan seperti pada Tabel 8. Rekomendasi control (*control recommendation*s), pada tahapan ini kontrol dapat mengurangi atau menghilangkan risiko yang teridentifikasi, yang sesuai dengan yang diinginkan oleh Instalasi IT, tujuan dari pengendalian yang direkomendasikan adalah untuk mengurangi tingkat risiko pada sistem TI dan datanya ke tingkat yang dapat diterima seperti pada Tabel 9.

5 Kesimpulan

Penilaian risiko TI pada Instalasi IT RSUD XYZ di Jawa Timur menggunakan dua metode *Quantitative Risk Analysis* dan *Qualitative Risk Analysis* memberikan hasil yang saling melengkapi. Penilaian risiko TI menggunakan *Quantitative Risk Analysis* diketahui bahwa aset TI yang memiliki Nilai Across Asset di atas 50 juta rupiah adalah Server, Router, CPU sehingga manajemen risiko TI dapat lebih fokus pada tiga tipe aset TI tersebut. Ancaman yang memiliki Nilai *Across Aset* diatas 50 juta rupiah adalah kehilangan daya listrik (*power loss*), kehilangan komunikasi (*network loss*), bencana alam, penghancuran atau pencurian aset TI dan pembobolan hak akses. Penilaian risiko TI menggunakan *Qualitative Risk Analysis* memberikan hasil bahwa tingkat risiko tinggi adalah sumber daya manusia internal (SDM-Internal) sedangkan tingkat risiko sedang adalah sumber daya manusia eksternal (SDM–Eksternal) dan Sistem & Infrastruktur TI. Rekomendasi manajemen risiko TI dilakukan tidak hanya pada aset TI dan Sistem & Infrastruktur TI tetapi juga pada SDM baik internal maupun eksternal. Pengamanan dan perawatan aset TI dan Sistem & Infrastruktur TI perlu dilakukan secara berkala dan terdokumentasi. Manajemen RSUD XYZ di Jawa Timur hendaknya memberi perhatian lebih kepada SDM-Internal dengan memberikan investasi jangka panjang berupa pelatihan yang sesuai dengan prioritas *skill* yang dibutuhkan.

Referensi

[1] Presiden-RI, "Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik," *Media Huk.*, 2018.

[2] Kementerian Kesehatan RI, *Peraturan Menteri Kesehatan RI Nomor 82 tentang Sistem Informasi Manajemen Rumah Sakit*, no. 87. Kementerian Kesehatan Indonesia, 2013.

[3] G. Endradita, *Standar Nasional Akreditasi Rumah Sakit Edisi 1*, 1st ed. Jakarta: Komisi Akreditasi Rumah Sakit (KARS), 2017.

[4] A. Yulianto, A. Ambarwati, and C. Darujati, "Analisis Manajemen Risiko TI Pemeliharaan Aset Menggunakan Quantitative Risk Analysis (QRA) pada PT. HMS," in *Prosiding Seminar Nasional Teknologi dan Rekayasa Informasi Tahun 2016*, 2016, pp. 45–51.

[5] W. Syafitri, "Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ)," *J. CoreIT*, vol. 2, no. 2, p. 8, 2016, doi: 10.24014/coreit.v2i2.2356.

[6] B. Muslim, "Quantitative Risk Analysis of Asset Information Technology at STT Pagaralam," *Conf. Senat. STT Adisutjipto Yogyakarta*, vol. 4, 2018, doi: 10.28989/senatik.v4i0.186.

[7] T. R. Peltier, *Information security risk analysis, second edition*. Auerbach Publications, 2005.

[8] J. Jonny, A. Ambarwati, and C. Darujati, "Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005," *Sist. J. Sist. Inf.*, vol. 10, no. 1, pp. 13–25, 2021.

[9] D. A. Permatasari, W. H. N. Putra, and A. R. Perdanakusuma, "Analisis Manajemen Risiko Sistem Informasi E-LKPJ pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 6, pp. 6001–6008, 2019, [Online]. Available: http://j-ptiik.ub.ac.id.

[10] J. W. Meritt, "A Method for Quantative Risk Analysis," *Proc. 22nd Natl. Inf. Syst. Secur. Conf.*, 1999.

[11] K. B. Mahardika, A. F. Wijaya, and D. Cahyono, "Manajemen risiko teknologi informasi menggunakan iso 31000 : 2018 (studi kasus: cv. xy)," *SEBATIK*, vol. 23, no. 1, pp. 277–284, 2019.

[12] NIST, "NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk

ISSN:2302-8149
e-ISSN:2540-9719

Assessments," *NIST Spec. Publ.*, no. September, p. 95, 2012.

[13] D. S. Valena, R. Prabowo, A. R. Irawati, and A. Aristoteles, "Analisis Manajemen Risiko Sistem Informasi Perpustakaan Universitas Lampung Menggunakan Metode Nist Sp 800-30," *J. Komputasi*, vol. 7, no. 1, pp. 1–10, 2019, doi: 10.23960/komputasi.v7i1.2053.

[14] A. Rohmani *et al.*, "Strategi Mitigasi Resiko Keamanan Informasi Berdasarkan Analisa Return on Investment," *Techno.COM*, vol. 15, no. 2, pp. 140–150, 2016.

[15] Z. Yazar, "A qualitative risk analysis and management tool – CRAMM," *SANS Inst. Inf. Secur. Read. Room*, 2021, [Online]. Available: http://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83.

[16] U. Nugraha, "Manajemen Risiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST SP 800-300," in *Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016)*, 2016, vol. ISSN : 250, pp. 121–126.