Faktor Exacta

Vol. 15, No. 1, March 2022, pp. 1~9
eISSN: 2502-339X, pISSN: 1979-276X, DOI: doi.org/10.30998/faktorexacta.v15i1.12040

Implementasi Metode *Quantitative* dan *Qualitative* Pada *Risk Analysis & IT Risk Management*

Asep Syaputra[1], Buhori Muslim[2]
[1]Program Studi Teknik Informatika, Institut Teknologi Pagaralam, Indonesia
[2]Program Studi Teknik Informatika,Universitas Putra Indonesia (UNPI) Cianjur, Indonesia

Article Info

Article history:

Received 16 Feb 2022
Revised 23 May 2022
Accepted 25 May 2022

Keywords:

Assessment IT Governance
Quantitative risk analysis
Qualitative risk analysis
Nist sp 800-30

ABSTRACT

The purpose of this study is to produce blue prints based on the level that positively and negatively affects hardware and software in one of the Agencies in City which will later become a benchmark to avoid or overcome problems that will be faced in the IT governance and IT infrastructure. IT governance is a process relationship structure that guides and controls an organization to achieve its vision and mission by creating value that balances risk with IT and its processes. An IT facility is an entity that performs the administrative and management functions of all IT applications in the Department XYZ environment for protection against unwanted threats that require risk management assessment. Minimize the danger or risk that may arise. The two analytical methods used in this study are quantitative and qualitative risk analysis. In the future, the quantitative risk analysis (QRA) approach will focus more on analyzing the condition of IT assets to find risk factors that need serious consideration and handling. For qualitative risk analysis methods, NIST SP 80030 is used to analyze various threat and risk attributes for to provide guidelines for the management of IT facilities in Department XYZ. Based on the QRA risk assessment, it was concluded that server-class IT resources are counted as the biggest potential loss to the Service. This is reflected in the risk aspect, where power losses have the most potential damage. Qualitative assessment of risk management according to NIST SP 80030 found that the sources of high-risk threats are high-risk power grids and the Internet. This level of risk can be identified during the threat source classification process. Submission of all risk analysis results can provide the results of risk recommendations communicated with departement IT management. To then be able to help the campus make decisions that include policies, procedures, budgets, operating systems and change management.

Corresponding Author:

Asep Syaputra
Program Studi Teknik Informatika
Institut Teknologi Pagaralam
JL. Simpang Bacang No.43, Karang Dalo, Dempo Tengah, Kota Pagar Alam, Sumatera Selatan, Indonesia
Email: asepsyaputra68@sttpagaralam.ac.id

1. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) yang begitu pesat dewasa ini, memberikan pengaruh yang besar terhadap peranannya dalam berbagai bidang kegiatan organisasi dan perusahaan. Bahkan memainkan peran penting dalam menjaga proses bisnis yang efisien dan efektif untuk organisasi dan bisnis [1]. Dimasa pandemi seperti saat ini, peran IT sangat penting karena semua pekerjaan dan bisnis yang dijalankan membutuhkan proses *paperless* dan *online*, seperti halnya pemerintah kota yang sudah mulai menjalankannya dalam proses pelayanan yang optimal dan maksimal. Keberhasilan pemerintah kota saat ini tergantung pada

tingkat pengelolaan TI yang sejalan dengan tujuan pemerintah kota yaitu mewujudkan kota kecil berbasis teknologi [2].

Tata kelola pada departemen TI merupakan bagian dari tata kelola instansi atau perusahaan. Beberapa perhatian utama dalam tata kelola perusahaan adalah tata kelola TI, yang mengacu pada bagaimana manajemen puncak memastikan bahwa CIO dan organisasi TI mampu memberikan nilai bagi organisasi. Kegiatan utama dalam bidang pemerintahan salah satunya adalah pelayanan kepada masyarakat sesuai dengan fungsi utamanya yaitu pelayanan optimal [3]. Dalam mengimplementasikan layanan pada masyarakat ini, sangat penting untuk menggunakan IT yang dapat menjaga kecepatan, kenyamanan dan kemudahan dalam layanan pada masyarakat untuk memberikan kepada masyarakat layanan yang berkualitas tinggi [4]. Adopsi **TI** untuk penggunaan **TI** harus disertai dengan tata kelola khusus untuk meminimalkan gangguan lebih lanjut terhadap proses bisnis. Penelitian sebelumnya telah mengungkapkan dua ancaman utama terhadap aset TI selama bertahun-tahun. Yang satu kehilangan koneksi internet, yang lain kehilangan daya. Perhitungan Financial Value Impact Factor (Rs) menunjukkan bahwa resiko kesalahan yang tidak disengaja merupakan potensi kerugian terbesar bagi perusahaan. Studi ini tidak memberikan manajemen resiko atau analisis manajemen yang akurat untuk mengurangi potensi biaya kehilangan aset TI pada sebuah instansi, hal ini juga tidak perlu memberikan panduan tentang cara mengelola resiko yang terkait dengan aset TI masa depan [5].

Penelitian lebih lanjut, kebutuhan stabilitas sistem menjadi semakin penting karena penyediaan layanan TI yang dibutuhkan masyarakat dan tantangan yang dihadapi layanan TI, salah satunya adalah Sistem Pemetaan (GIS) yang memiliki kerentanan dalam keamanan informasi [6]. Jika masalah ini tidak dapat diatasi secara berkelanjutan, konsekuensinya akan mengancam atau merusak keberlanjutan sistem (khususnya sains). NIST SP 80030 memberi pembuat keputusan intelijen keamanan yang terbukti komprehensif dan konsisten, pemodelan sumber daya terstruktur untuk mengidentifikasi ancaman, dan analisis keamanan informasi multi-stakeholder yang dapat diidentifikasi. Menawarkan lebih banyak fitur [7]. Dalam penelitian ini, peneliti menggunakan NIST SP80026 sebagai alat identifikasi tambahan berdasarkan hasil dokumen berbasis keamanan informasi. Studi ini tidak merekomendasikan pengendalian yang dirancang untuk mengendalikan, mengurangi, atau menghilangkan risiko yang diidentifikasi pada tahap ini. Membangun kontrol sangat penting karena dapat meminimalkan tingkat resiko dalam data ke tingkat yang lebih terkendali secara terstruktur. Kemudian akan berlanjut ke langkah berikutnya, yaitu mitigasi dan penilaian resiko [8].

Penggunaan TI dalam semua proses pemberian layanan kepada masyarakat tentunya dapat menimbulkan berbagai ancaman dan hambatan terhadap resiko TI yang mempengaruhi kualitas layanan dan meningkatkan kepercayaan masyarakat terhadap kualitas layanan yang diberikan oleh pemkot [9]. Seberapa besar resiko menggunakan IT dan tidak pernah melakukan riset. Pada studi ini melakukan proses evaluasi yang diperpanjang (referensi NIST 800300). Manajemen harus mewaspadai berbagai ancaman TI yang ada atau mungkin muncul di lingkungan Unit Pelayanan dan menyusun strategi untuk mengelola berbagai resiko tersebut. Fasilitas TI (teknologi informasi) merupakan unit pelayanan dari Dinas XYZ dengan tugas mengatur dan mengelola penggunaan TI pada layanan tersebut. Bagian dari fasilitas TI ini memainkan peran penting dalam mengelola aktivitas bisnis atau layanan apa pun yang didukung oleh TI, tetapi tidak memiliki identifikasi ancaman TI yang terorganisir dan terperinci di unit pelayanan tersebut. Manajemen sumber daya TI yang tidak tepat dapat menimbulkan banyak resiko bagi TI [10]. Menurut wawancara dengan Manajer Fasilitas TI Dinas XYZ, Unit Pelayanan pada Dinas XYZ telah mengalami beberapa masalah. Kerusakan komputer yang tidak menyala pada jam kerja akibat kurangnya perawatan secara berkala menghambat pelayanan optimal yang diharapkan masyarakat dan sistem tidak dapat mengakses dan menampilkan data. Tim kesiapan TI Dinas XYZ tidak melakukan penilaian resiko TI secara berkala untuk mencegah terulangnya insiden ini dan ancaman TI lainnya, penilaian manajemen resiko TI harus dilakukan untuk Dinas XYZ.

Tujuan dari penelitian ini adalah untuk menganalisis pemeliharaan aset TI melalui analisis resiko kuantitatif, menganalisis berbagai resiko dan ancaman, dan memperoleh rencana mitigasi resiko, yang dapat mencegah tantangan, ancaman dan kerugian pada infrastruktur jaringan backbone TI melalui analisis resiko kualitatif. Penggunaan analisis resiko kuantitatif dan analisis resiko kualitatif diharapkan dapat memberikan rekomendasi manajemen resiko TI kuantitatif dan kualitatif yang lebih komprehensif kepada tim TI Unit Layanan XYZ. Hasil penelitian ini bermanfaat bagi instalasi TI pada Dinas XYZ sebagai inventarisasi resiko pada aset TI berdasarkan mitigasi resiko sebagai dasar analisis resiko secara kuantitatif dan kualitatif.

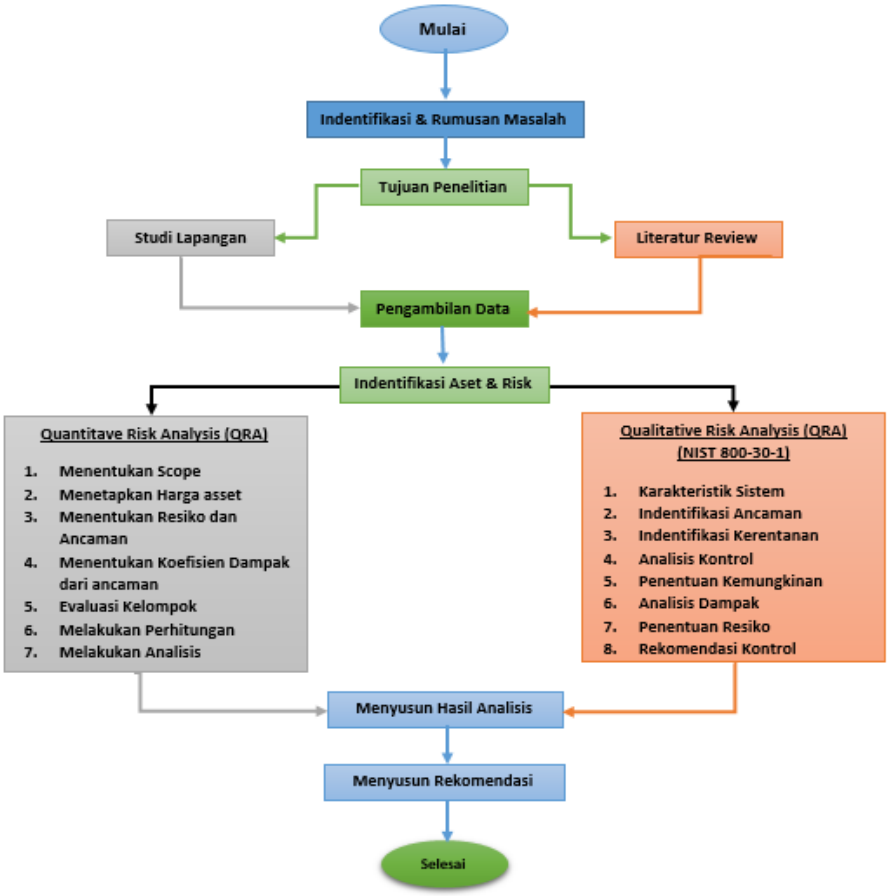
2. METODE PENELITIAN

Analisis resiko kuantitatif adalah teknik analisis resiko yang menggunakan angka untuk mewakili efektivitas dan kemungkinan. Jika nilai resiko kuantitatif yang diharapkan diterapkan pada penerapan ukuran numerik dari biaya sumber daya yang terkait dengan kuantitas, bersama dengan kemungkinan kerusakan, jumlah kasus dan nilai frekuensi kejadian dan kerentanan ancaman, metode ini memperoleh hasil berupa indicator [11]. *Fase QRA (Quantitative Risk Analysis)* terdiri dari tujuh fase penting berikut ini. (1)

Mengidentifikasi aspek survei, (2) Mengidentifikasi harga setiap aset TI sesuai fungsi TI, (3) Mengidentifikasi ancaman dan resiko sumber daya yang dinilai, Mengidentifikasi dan membuat daftar akar penyebab potensi ancaman dan penyebab resiko, (4) Upaya untuk mengidentifikasi faktor-faktor yang Mempengaruhi dengan mengidentifikasi kerentanan aset TI terhadap resiko tertentu dan menganalisis kerentanan aset TI untuk mengidentifikasi peningkatan faktor eksposur (EF), (5) penilaian kelompok, (6) perhitungan, (7) penilaian akhir adalah dibuat dengan memasukkan nilai yang ditentukan dalam *spreadsheet* [12].

Dengan menggunakan panduan NIST SP80030 tentang metode analisis resiko kualitatif, panduan ini dapat digunakan di tahap selanjutnya untuk menemukan rekomendasi ancaman dan resiko untuk entitas TI [13]. Penelitian sebelumnya menggunakan metode ini untuk analisis resiko. Dua metode diterapkan dalam penelitian ini, analisis resiko kuantitatif dan analisis resiko kualitatif untuk menemukan hasil analisis penilaian resiko yang lebih kuat dan mengintegrasikan kekurangan masing-masing ke dalam analisis penilaian resiko [14]. Kuantitatif digunakan untuk menemukan item pemeliharaan aset TI, sedangkan kualitatif analisis lebih mungkin digunakan untuk menemukan ancaman dan resiko yang dihadapi fasilitas TI di unit layanan Dinas XYZ. Data kualitatif dan kuantitatif menjadi dasar penelitian ini. Gambar 1 menunjukkan proses penelitian. Subyek penelitian ini adalah instalasi komputer yang ada di salah satu unit pelayanan di kawasan kota Pagar Alam. Data penelitian diperoleh dari pengelola fasilitas TI serta teknisi TI unit layanan tempat penelitian dilakukan. Nama unit layanan tempat penelitian dilakukan bersifat rahasia karena penelitian ini berfokus pada analisis resiko TI terhadap aset TI di Unit Pelayanandan fasilitas TI itu sendiri.

Bagian Analisis Resiko merupakan penilaian resiko dalam bentuk portofolio. Proses evaluasi bagian resiko dapat dilakukan secara kuantitatif dan kualitatif. Analisis menggunakan dua metode, yaitu analisis resiko kuantitatif *(QRA)* dan analisis resiko kuantitatif, yang merupakan analisis resiko tujuh langkah [15]. Metode NIST SP 80030 digunakan sebagai analisis resiko kualitatif, NIST SP 80030 juga memiliki langkah analisis yang menemukan masalah, diikuti dengan rekomendasi penyelesaian resiko pada infrastruktur TI unit layanan XYZ. Proses penelitian dapat dilihat pada Gambar 1.



Gambar 1. Alur Penelitian

3. HASIL DAN PEMBAHASAN

3.1. Indentifikasi aset dan resiko

Dalam penelitian ini, manajer aset TI *(chief installation engineer),* memberikan spesifikasi TI dan jumlah aset IT pada Unit Pelayanan Dinas XYZ. Beberapa jenis aset TI yang dianggap sebagai aset yang paling

berpengaruh penting *server, router, Computer, laptop, printer* dan *Genset*, seperti pada Tabel 1 dibawah. Tahap pertama analisis untuk menentukan volume yaitu instalasi teknologi informasi yang berada pada salah satu Unit Pelayanan Dinas di Kota XYZ. Penelitian ini berjalan selama 4 bulan dan mencakup jenis aset TI termasuk *server, router, Komputer, laptop, printer,* dan *generator.*

3.2. *Quantitative risk analysis*

Pada langkah selanjutnya, harga sumber daya TI ditentukan. Tabel 1 menunjukkan biaya aset TI yang dievaluasi berdasarkan harga pembelian awal aset TI. Langkah selanjutnya adalah menetapkan nilai *Annualized Rate Occurrence (ARO)* untuk mengidentifikasi resiko dan ancaman. ARO dihitung dengan menghitung persentase ancaman yang terdeteksi dalam setahun saat Unit Pelayanan Dinas XYZ dipasang, yang dapat dilihat pada Tabel 2, dan Tabel 3 menunjukkan nilai faktor dampak (faktor ancaman) untuk setiap TI sumber. Penjumlahan dimulai dengan metode perhitungan yang rumit, karena pada tahap ini nilai faktor dampak harus dihitung untuk setiap bagian dari jenis aset TI.

Tabel 1: Daftar Harga Aset TI

Asset Type	Jumlah	Harga Per-Satuan	Total Harga
Server	1	150,000,000	150,000,000
Router	5	7,000,000	35,000,000
Laptop	3	9,000,000	27,000,000
Printer	10	1,400,000	14.000.000
Komputer	10	4.000,000	40,000,000
Genset	1	20,000,000	20,000,000
	Jumlah		286,200,000

Tabel 2: Ancaman (1 Tahun)

No	Ancaman	ARO
1.	Kehilangan daya Tegangan Listrik	1. 2
2.	Network Error	1. 2
3.	Kesalahan secara tidak sengaja (Accidental Error)	0. 2
4.	Terserang Virus	0. 5
5.	Pelanggaran hak akses	0. 3
6.	Bencana alam	0. 2
7.	Pencurian dan Perusakan Aset TI	0. 1
8.	Hacking ke dalam sistem	0
9.	Penghentian sistem untuk perangkat TI non-darurat	0
10.	Bencana Kebakaran	0. 1
11.	Bencana Alam Gempa Bumi	0. 1

Pada langkah selanjutnya, harga sumber daya TI ditentukan. Tabel 1 menunjukkan biaya aset TI yang dievaluasi berdasarkan harga pembelian awal aset TI. Langkah selanjutnya adalah menetapkan nilai *Annualized Rate Occurrence (ARO)* untuk mengidentifikasi risiko dan ancaman [16]. ARO dihitung dengan menghitung persentase ancaman yang terekspos dalam setahun saat Unit Pelayanan TI Dinas XYZ dipasang, yang dapat dilihat pada Tabel 2, dan Tabel 3 menunjukkan nilai faktor dampak (faktor ancaman) untuk setiap TI sumber. Penjumlahan dimulai dengan metode perhitungan yang rumit, karena pada tahap ini nilai faktor dampak harus dihitung untuk setiap bagian dari jenis aset TI.

Tabel 3: Koefisien Dampak Sumber Daya IT

No	Ancaman	EF					
		Server	Router	Laptop	Printer	Komputer	Genset
1	Kehilangan daya Tegangan Listrik	0,3	0,3	0,5	0,3	0,3	0.1
2	Network Error	0,5	0,0	0,0	0,0	0,0	0
3	Kesalahan secara tidak sengaja (Accidental Error)	0,5	0,3	0,3	0,5	0,5	0.5
4	Terserang Virus	0,0	0,0	0,5	0,0	1.0	0
5	Pelanggaran hak akses	0,3	0,3	0,3	0,0	0.5	0
6	Bencana alam	1,0	1,0	1,0	1,0	1,0	1.0
7	Penghancuran atau pencurian Aset IT	1,0	1,0	1,0	1,0	1,0	1.0
8	Hacking ke dalam sistem	0,3	0,0	0,5	0,0	0,3	0
9	Penghentian proses perangkat TI diluar bencana	0,3	0,3	0,3	0,3	0,3	0.5

10	Bencana Kebakaran	1.0	1.0	1.0	1.0	1.0	1.0
11	Bencana Alam Gempa Bumi	1.0	1.0	1.0	1.0	1.0	1.0

Setelah semuanya dihitung, hasilnya dapat digunakan untuk mengidentifikasi aset TI pada bagian mana yang memiliki potensi kerugian finansial terbesar, dan dilakukan *Across Asset Analysis* dengan memeringkatkan jumlah total perhitungan ALE pada pengurutan masing-masing jenis aset IT dari terbesar hingga paling kecil. Di sisi lain, untuk mengetahui ancaman mana yang berbahaya bagi perusahaan, cukup dengan mengurutkan jumlah total nilai ALE yang dihitung berdasarkan setiap *(Across Risk)* ancaman. Dari Tabel 4 dibawah, dapat diketahui bahwa Nilai Aset setelah dikalkulasi Aset paling tinggi yaitu *Server* Rp. 247.500.000, dan Nilai Aset Terendah adalah *printer* Dengan nilai Rp. 13.440.000. Nilai kumulatif resiko tertinggi yaitu Network Error atau kehilangan koneksi internet dengan nilai Rp. 90.000.000, selanjutnya kehilangan Kehilangan daya listrik dengan nilai Rp. 54.000.000. Ada 2 ancaman yang memiliki nilai resiko 0, yaitu akses paksa dari luar sistem *(hacking)* dan penghentian paksa peralatan IT selain dalam situasi darurat.

Tabel 4: Nilai Aset Kalkulasi, Faktor Eksposur, ALE

No	Ancaman	EF					
		Server (Rp)	Router (Rp)	Laptop (Rp)	Printer (Rp)	Komputer (Rp)	Genset (Rp)
1	Kehilangan daya tegangan listrik	54.000,000	12.600.000	16.200.000	5.040.000	14.400.000	2.400.000
2	Network Error	90.000,000	0	0	0	0	0
3	Kesalahan tidak sengaja (Accidental Error)	15.000.000	2.100.000	1.620.000	1.400.000	4.000.000	2.000.000
4	Terserang Virus	0	0	6.750.000	0	20.000.000	0
5	Pelanggaran hak akses	13.500,000	3.150.000	2.430.000	0	6.000.000	0
6	Bencana alam	30.000.000	7.000.000	5.400.000	2.800.000	8.000.000	4.000.000
7	Penghancuran dan pencurian Aset IT	15.000.000	3.500.000	2.700.000	1.400.000	4.000.000	2.000.000
8	Hacking ke dalam Sistem	0	0	0	0	0	0
9	Penghentian proses perangkat TI diluar bencana	0	0	0	0	0	0
10	Bencana Kebakaran	15.000.000	3.500.000	2.700.000	1.400.000	4.000.000	2.000.000
11	Bencana Alam Gempa Bumi	15.000.000	3.500.000	2.700.000	1.400.000	4.000.000	2.000.000
	Total	247.500.000	35.350.000	40.300.000	13.440.000	64.400.000	14.400.000

3.3. *Qualitative Risk Analysis*

Metode NIST SP 80030 digunakan sebagai metode analisis resiko kualitatif. Metode NIST SP 80030 dapat memberikan rekomendasi untuk pengendalian selama fase analisis resiko [17]. Fase awal dalam NIST SP 80030 adalah karakterisasi sistem, yang mendefinisikan ruang lingkup penilaian resiko, mendefinisikan batas otorisasi (perizinan), dan menyediakan informasi (misalnya, informasi tentang *Hardware, Software*, komunikasi sistem, manajer sistem, dll. Departemen atau staf pendukung). Tabel 5 menunjukkan identifikasi ancaman (*Threat Identification*).

Tabel 5: Indentifikasi Ancaman Terhadap Instalasi IT

Ancaman Utama	Keterangan	Kode
Bencana Banjir	Infrastruktur IT yang rusak, kegagalan proses pada sistem dan kehilangan data	a.1- 1
Gempa Bumi	Infrastruktur IT yang rusak, kegagalan proses pada sistem dan kehilangan data	a.2- 1
Sumber Daya Listrik	Kehilangan daya listrik yang menyebabkan *server down*	a.3- 1
	Kurang optimal tegangan listrik (Kekurangan Daya)	a.3- 2
	Kerusakan AC pada ruang server dan instalasi listrik	a.3- 3
	Hilangnya daya listrik pada *Modem* dan *Router*	a.3- 4
	System Crash dan kehilangan data	a.3- 5
Kebakaran	Kebakaran gedung pada tempat insfratruktur IT	a.4- 1
Jaringan Internet	Gangguan jaringan Internet atau terputusnya koneksi internet pada server	a.5- 1
SDM -Internal	Penyalahgunaan data internal	a.6- 1
	Kesalahan entri data *(Human Error)*	a.6- 2
	Hak akses internal yang disalahgunakan sebagai tindakan negatif	a.6- 3
	Penyalahgunaan data internal	a.6- 1
SDM - Eksternal	Pembobolan data/informasi dari pihak eksternal	a.7- 1

	Perusakan serta pencurian Aset IT pada Insfratruktur IT	a.7- 2
	Hacker	a.7- 3
Sistem dan Infrastruktur IT	*Server Down*	a.8- 1
	Kerusakan sistem dan aplikasi	a.8- 2
	Server kelebihan kapasitas *(Overload)*	a.8- 3
	Pencadangan data yang gagal	a.8- 4
	Pembaruan perangkat lunak gagal	a.8- 5
	Kurang *update* pada sistem ataupun perangkat IT *(out of date)*	a.8- 6

Setelah tahap pembuatan daftar untuk mengidentifikasi kerentanan resiko dan sumber ancaman dengan responden, kemudian mendiskusikan hasil identifikasi kerentanan berdasarkan apa yang terjadi di lapangan. Tabel 6 menunjukkan hasil pembahasan tentang kerentanan yang muncul ketika ancaman tersebut ada. Tahap selanjutnya adalah analisis pengendalian, hasil pengamatan untuk mengimplementasikan analisis pengendalian yang akan meminimalkan terjadinya ancaman. Pindai daftar periksa aturan manajemen lama dan baru untuk menentukan apakah ada kerentanan di Unit Pelayanan TI Dinas XYZ. Misalnya: pelatihan dan sosialisasi TI dan sistem informasi, manajemen cadangan, pedoman baru tentang *SOP* (*Standard Operating Procedure)* dalam manajemen ancaman dunia maya. Langkah kelima adalah menentukan probabilitas, yang dengan mengetahui hasil analisis resiko yang akan dipenuhi, dapat dijadikan acuan untuk menentukan resiko yang mungkin timbul. Ada 3 kategori level yaitu Rendah (0,1), Sedang (0,5), Tinggi (1).Menentukan prediksi probabilitas ini terdiri dari menentukan tingkat probabilitas yang terjadi sebelum resiko yang teridentifikasi.

Tabel 6: Indentifikasi Ancaman pada Insfrastruktur IT

Ancaman Utama	Keterangan Ancaman	Threat code	Kerentanan	Kode Kerentanan
Tenaga Listrik	Kehilangan daya listrik yang menyebabkan *server down*	a.3- 1	Terbatas *'UPS'* untuk server	k1.1
	Kurang optimal tegangan listrik (Kekurangan Daya)	a.3- 2	Adanya kerusakan pada MCB dan aliran pada pemakaian listrik secara tidak beraturan	k1.2
	Kerusakan AC pada ruang server dan instalasi listrik	a.3- 3	Generator/genset tidak segera hidup (respons lambat)	k1.3
	Hilangnya daya listrik pada *Modem* dan *Router*	a.3- 4	Tidak ada *backup* jaringan internet untuk erver	k1.4
	System Crash dan kehilangan data	a.3- 5	Tidak ada pemulihan data dan *backup* pada sistem.	k1.5
Bencana Kebakaran	Kebakaran gedung pada tempat insfratruktur IT	a.4- 1	Kurangnya pelatihan tentang *SOP* keselamatan Aset pada saat terjadi kebakaran gedung insfratruktur IT	k2.1
Jaringan Internet	Gangguan jaringan Internet atau terputusnya koneksi internet pada *server*	a.5- 1	Tidak tersedianya *backup* jaringan internet	k3.1
SDM - Internal	Penyalahgunaan data dari pihak internal	a.6- 1	Aturan untuk petugas kurang detail dan tidak mudah dipahami.	k4.1
	Kesalahan entri data *(Human Eror)*	a.6- 2	Kurangnya pelatihan atau distribusi data pada sistem	k4.2
	Hak akses internal yang disalahgunakan sebagai tindakan negatif	a.6- 3	*Log* akses tidak diperiksa secara teratur dan menambahkan keamanan *software*	k4.3
	Kesalahan entri data *(Human Eror)*	a.6- 2	Kurangnya pelatihan atau distribusi penggunaan data	k4.2
SDM - Eksternal	Penyebarluasan data/informasi penting dari pihak eksternal	a.7- 1	Tidak ada unit hukum untuk menangani ancaman eksternal	k5.1
	Perusakan dan Pencurian Aset TI pada Instalasi IT	a.7- 2	Tidak ada manajemen tambahan aset TI	k5.2
	Hacker	a.7- 3	Tidak ada tambahan keamanan pada sistem	k5.3
Sistem dan infrastruktur IT	*Server Down*	a.8- 1	Tidak ada cadangan host lain	k6.1
	Kerusakan sistem dan aplikasi	a.8- 2	Penundaan update sistem dari staff	k6.2
	Server kelebihan kapasitas	a.8- 3	Tidak adanya batasan pada akses orang ke server database.	k6.3
	Pencadangan data yang gagal	a.8- 4	Tidak ada jadwal *backup* server reguler	k6.4
	Pembaruan perangkat lunak gagal	a.8- 5	Staf TI menunda pembaruan *Software*	k6.5
	Kurang *update* pada sistem ataupun perangkat IT *(out of date)*	a.8- 6	Unit Pelayanan IT Tidak Memiliki Rencana *Update* Teknologi Baru	k6.6

Langkah selanjutnya adalah identifikasi resiko. Tujuan dari fase ini adalah untuk menentukan nilai tingkat resiko suatu sistem TI. Identifikasi resiko untuk kerentanan dan ancaman dapat dinyatakan dalam

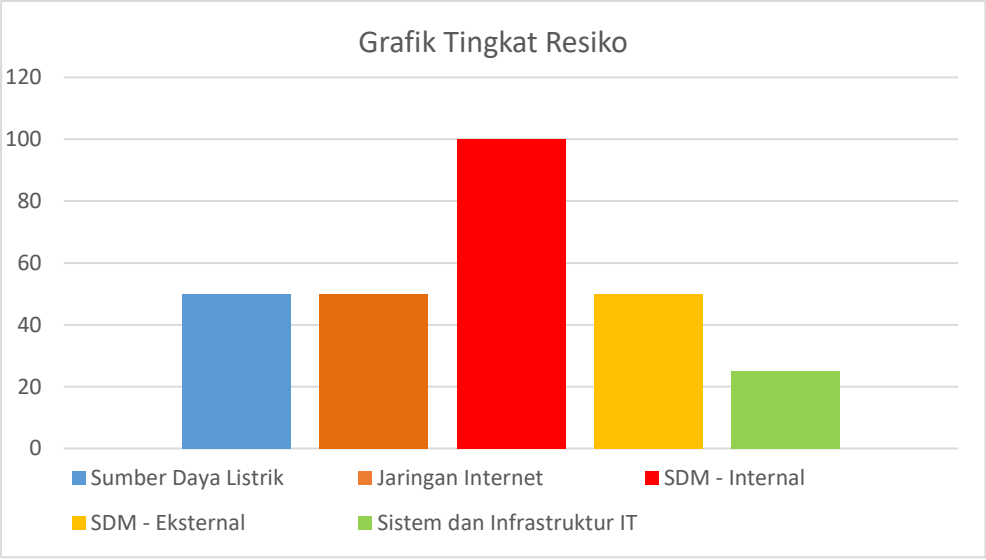
besaran dampak jika sumber ancaman dapat diperbaiki dan kerentanan dapat mengurangi atau menghilangkan resiko tersebut. Untuk mengukur skor resiko, skala resiko dan matriks resiko ditunjukkan pada Tabel 7. Hasil akhir pengukuran resiko diperoleh dengan menghitung skor yang ditentukan oleh kemungkinan terjadinya suatu ancaman *(likelihood of the threat)* dan dampak dari ancaman *(impact).*

Tabel 7: Matriks Tingkat Resiko

Probabilitas Ancaman	*IMPACT*		
	Low (10)	*Medium* (50)	*High* (100)
High (0. 1)	Low 10 × 0. 1 =10	Medium 50 × 1. 0 = 50	High 100 × 1. 0 = 100
Medium (0. 5)	Low 10 × 0. 5 = 5	Medium 50 × 0. 5 = 25	Medium 50 × 0. 5 = 25
Low (0. 1)	Low 10 × 0. 1 = 1	Low 50 × 0. 1 = 5	Low 100 × 0. 1 = 10

Jenis Ancaman	Tingkat Probabilitas Ancaman	Nilai Dampak	Nilai Ancaman	Tingkat Ancaman
Sumber Daya Listrik	Tinggi (1)	Sedang (50)	50	Sedang
Jaringan Internet	Tinggi (1)	Sedang (50)	50	Sedang
SDM - Internal	Tinggi (1)	Tinggi (100)	100	Tinggi
SDM - Eksternal	Sedang (0. 5)	Tinggi (100)	50	Sedang
Sistem dan Infrastruktur IT	Sedang (0.5)	Sedang (50)	25	Sedang

Tabel 8: Penentuan Resiko



Gambar 2. Grafik Tingkat Resiko

Tabel 9: Kontrol Yang Direkomendasikan

Jenis Ancaman	Tingkat Ancaman	Rekomendasi
Sumber Daya Listrik	Sedang	Meminta Tambahan Unit UPS Tambahan untuk di Bagian *Server* Menyiapkan generator untuk respons yang lebih cepat Periksa tanggal servis AC secara berkala.

		Menyiapkan VSAT Untuk cadangan sumber daya internet tambahan *Backup* data diperbarui dengan menejemen yang baik
Jaringan I*nternet*	Sedang	Konfigurasi *backup* Jaringan
SDM - I*nternal*	Tinggi	Regulasi SDM semakin disosialisasikan. Jadwalkan pemeriksaan log berkala tambahan Pelatihan keterampilan dan sosialisasi staf
SDM - *Eksternal*	Sedang	Pembaruan Sistem Keamanan mrnggunskan Pengawasan cctv Mengirim data ke *server cloud* lebih cepat dan terjamin keamanan data Keamanan *Server* yang Ditingkatkan dengan penambahan *software* ataupun *hardware*
Sistem dan Infrastruktur IT	Sedang	Jadwalkan restart sistem secara berkala Siapkan *backup server host/cloud* Memberi Batasan orang yang bisa akses Manajemen *backup* data Persiapan pencadangan *software* yang rentan akan virus Membuat pengajuan pembelian *Hardware* dengan teknologi terbaru

4. PENUTUP

Analisis resiko dan menejemen resiko IT berdasarkan dua metode analisis *Quantitative* dan *Qualitative* memberikan hasil pedoman yang nantinya akan digunakan sebagai tindak lanjut dalam menghindari resiko yang akan dihadapi. Melakukan penilaian resiko TI menggunakan analisis resiko kuantitatif mengemukakan Aset TI yang berjumlah lebih dari KRW 50 juta adalah *server, router*, dan komputer dan laptop, sehingga proses manajemen resiko TI berfokus pada empat jenis aset TI. Ancaman dengan total nilai aset lebih dari Rp 50 juta termasuk kehilangan jaringan *(network error)*, kerusakan sumber daya listrik, bencana alam, kehilangan aset infrastruktur TI yang dicuri dan pelanggaran hak akses. Hasil analisis resiko kualitatif menunjukkan bahwa resiko tinggi terletak pada SDM Internal (sumber daya manusia internal) dan resiko rata-rata pada Sumber daya listrik, jaringan internet dan infrastruktur TI. Melalui manajemen resiko TI dan analisis resiko, yang hasilnya akan memberikan pedoman pengelolaan resiko TI untuk SDM internal dan eksternal serta untuk aset, sistem, dan infrastruktur TI. Pencadangan dan pemeliharaan aset, sistem, dan infrastruktur TI harus dilakukan dan didokumentasikan secara berkala untuk mencegah resiko yang berkelanjutan. Unit Pelayanan Dinas XYZ perlu lebih memperhatikan SDM internalnya dan mengamankan insfrastruktur TI jangka panjang dalam bentuk pelatihan berdasarkan keterampilan yang dibutuhkan terlebih dahulu.

DAFTAR PUSTAKA

[1] D. Antoni, A. Syaputra, And M. Nasir, "A Literature Review Of Infrastructure Capabilities In Shared E-Government Concept," In *2019 International Conference On Electrical Engineering And Computer Science (Icecos)*, 2019, Pp. 117–121.

[2] J. Jonny And C. Darujati, "Penilaian Resiko Data Sistem Informasi Manajemen Puskesmas Dan Aset Menggunakan Iso 27005," *Sist. J. Sist. Inf.*, Vol. 10, No. 1, Pp. 1–12, 2021.

[3] A. Yulianto, A. Ambarwati, And C. Darujati, "Analisis Manajemen Resiko Ti Pemeliharaan Aset Menggunakan Quantitative Risk Analysis (Qra) Pada Pt. Hms," In *Prosiding Seminar Nasional Teknologi Dan Rekayasa Informasi (Sentrin) 2016*, 2016, Pp. 45–51.

[4] B. Muslim, "Quantitative Risk Analysis Of Asset Information Technology At Stt Pagaralam," *Pros. Stta Yogyakarta (Senatik 2018), Stta*, Pp. 501–509, 2018.

[5] M. Anhar And S. U. Kalsum, "Penerapan Metode Service Quality & Quality Function Deployment (Qfd) Dalam Upaya Peningkatan Pelayanan Kepada Mahasiswa Politeknik Ketapang," *J. Sist. Tek. Ind.*, Vol. 18, No. 2, Pp. 75–83, 2016.

[6] A. G. R. Padang, A. Ambarwati, And E. Setiawan, "Penilaian Manajemen Resiko Ti Menggunakan Quantitative Dan Qualitative Risk Analysis," *Sist. J. Sist. Inf.*, Vol. 10, No. 3, Pp. 527–537, 2021.

[7] S. Susilo, "Analisa Tingkat Resiko Tata Kelola Teknologi Informasi Perguruan Tinggi Menggunakan Model Framework National Institute Of Standards & Technology (Nist) Special Publication 800-30 Dan It General Control Questionnaire (Itgcq)," *J. Ind. Serv.*, Vol. 3, No. 1c, 2017.

[8] D. Pasha, A. Thyo Priandika, And Y. Indonesian, "Analisis Tata Kelola It Dengan Domain Dss Pada Instansi Xyz Menggunakan Cobit 5," *J. Ilm. Infrastruktur Teknol. Inf.*, Vol. 1, No. 1, Pp. 7–12, 2020.

[9] A. Syaputra, "Aplikasi E-Kelurahan Untuk Peningkatan Pelayanan Administrasi Dalam Mendukung

Penerapan E-Government," *Matrik J. Manajemen, Tek. Inform. Dan Rekayasa Komput.*, Vol. 20, No. 2, Pp. 379–388, 2021.

[10] C. M. Sufyana And E. Suharto, "Analisis Pengukuran Tingkat Kematangan Sistem Informasi Akademik Menggunakan Cobit 5.0 Di Politeknik X," *J. E-Komtek*, Vol. 2, No. 2, Pp. 101–116, 2018.

[11] M. A. Dewi, A. Ambarwati, And C. Darujati, "Analisis Resiko Kuantitatif Aset Ti Pada Blc E-Gov Dinkominfo Surabaya," In *Prosiding Semnas Inotek (Seminar Nasional Inovasi Teknologi)*, 2018, Vol. 2, No. 1, Pp. 7–12.

[12] A. Ramdhani, R. Hardian, And A. Maulana Fajar, "Pembuatan Motion Graphic Pengenalan Desain Komunikasi Visual Untuk Siswa Sma-Smk." Politeknik Harapan Bersama, 2021.

[13] A. Asrofi And D. S. Hadmoko, "Strategi Adaptasi Masyarakat Pesisir Dalam Penanganan Bencana Banjir Rob Dan Implikasinya Terhadap Ketahanan Wilayah (Studi Di Desa Bedono Kecamatan Sayung Kabupaten Demak Jawa Tengah)," *J. Ketahanan Nas.*, Vol. 23, No. 2, Pp. 125–144, 2017.

[14] A. Elanda And R. L. Buana, "Analisis Manajemen Resiko Infrastruktur Dengan Metode Nist (National Institute Of Standards And Technology) Sp 800-30 (Studi Kasus: Stmik Rosma)," *Elkom J. Elektron. Dan Komput.*, Vol. 14, No. 1, Pp. 141–151, 2021.

[15] R. S. Aranov, D. Witarsyah, And L. Abdurrahman, "Perancangan Tata Kelola Manajemen Teknologi Informasi Smk N 4 Bandung Menggunakan Framework Cobit 5 Domain Evaluate, Direct And Monitor (Edm) & Build, Acquire And Implement (Bai)," *Eproceedings Eng.*, Vol. 5, No. 2, 2018.

[16] S. O. D. Ningsih And S. W. Hati, "Analisis Resiko Keselamatan Dan Kesehatan Kerja (K3) Dengan Menggunakan Metode Hazard And Operability Study (Hazop) Pada Bagian Hydrotest Manual Di Pt. Cladtek Bi Metal Manufacturing," *J. Appl. Bus. Adm.*, Vol. 3, No. 1, Pp. 29–39, 2019.

[17] M. Muhaemin, "Mengembangkan Busines Continuity Planning (Bcp) Dengan Pendekatan Kuantitatif Studi Kasus: Siak-Ditjen Adminduk Kemendagri," *Just It J. Sist. Informasi, Teknol. Inf. Dan Komput.*, Vol. 9, No. 1, Pp. 1–11, 2018.