http://univ45sby.ac.id/ejournal/index.php/industri/index ISSN 1412 – 2146 (Cetak)
Vol. 27 No.1, Hal. 28-41(2024) ISSN 2721 – 5431 (Online

Analisis Manajemen Risiko Aset Teknologi Informasi dan Pemeliharaan Aset Menggunakan *Quantitative Risk Analysis* WH-TGR

Boriski Sinaga[1], Rr. Rochmoeljati[2]
[1.2]Program Studi Teknik Industri - UPN "Veteran" Jawa Timur
Email: [1]20032010154@student.upnjatim.ac.id, [2]rochmoeljati@upnjatim.ac.id

ABSTRAK

Penelitian ini memiliki tujuan untuk melakukan analisis manajemen risiko terhadap aset Teknologi Informasi (TI) dengan menerapkan metode *Quantitative Risk Analysis* (Analisis Risiko Kuantitatif). Fokus penelitian mencakup identifikasi risiko terkait aset TI dan pemeliharaan aset dalam konteks manajemen risiko. Metodologi *Quantitative Risk Analysis* digunakan untuk mengukur risiko secara kuantitatif dengan mempertimbangkan nilai ekonomi dan dampak finansial terhadap aset TI. Proses identifikasi risiko melibatkan penilaian dan analisis potensi ancaman serta kerentanannya terhadap aset TI. Selanjutnya, penelitian mengevaluasi dampak finansial dari setiap risiko yang teridentifikasi. Pentingnya pemeliharaan aset dalam konteks manajemen risiko juga dibahas secara rinci. Pendekatan kuantitatif digunakan untuk mengukur efektivitas pemeliharaan terhadap mitigasi risiko yang telah diidentifikasi. Analisis ini memberikan dasar bagi organisasi untuk menentukan alokasi sumber daya yang tepat untuk pemeliharaan aset dan memahami dampak finansial yang mungkin timbul dari risiko yang ada. Hasil dari penelitian ini diharapkan dapat memberikan pandangan yang komprehensif terkait risiko dan pemeliharaan aset TI, memungkinkan organisasi untuk mengambil keputusan yang lebih baik dalam manajemen risiko dan menjaga keamanan serta ketersediaan aset TI mereka.

Kata Kunci : ***Manajemen Resiko, Aset Teknologi Informasi, Pemeliharaan Aset***

PENDAHULUAN

Peran Teknologi Informasi (TI) dalam konteks perusahaan memiliki kepentingan yang sangat vital dan beragam, membentuk fondasi untuk mencapai efisiensi, produktivitas, dan inovasi. TI tidak hanya berperan sebagai sarana pendukung, melainkan menjadi unsur kunci dalam menjalankan operasional dan strategi perusahaan *modern*. Melalui TI, otomatisasi berbagai proses bisnis dapat terwujud, mengurangi ketergantungan pada pekerjaan manual, dan meningkatkan efisiensi operasional secara menyeluruh. Sistem manajemen perusahaan, seperti *Enterprise Resource Planning* (ERP), turut berkontribusi dalam mengintegrasikan berbagai fungsi perusahaan.

TI menciptakan saluran komunikasi yang efisien melalui email, video konferensi, dan platform kolaborasi, memfasilitasi kerjasama tim yang lebih baik tanpa terbatas oleh lokasi fisik anggota tim. Sistem *Business Intelligence* (BI) dan analitika data memungkinkan perusahaan melakukan analisis mendalam terhadap data, mendukung

pengambilan keputusan berbasis bukti, dan merespons perubahan pasar atau situasi internal perusahaan dengan cepat. Perlindungan dan manajemen keamanan informasi menjadi fokus utama perusahaan, dengan sistem keamanan TI yang membantu melindungi data sensitif, mengatasi ancaman siber, dan memastikan kepatuhan terhadap regulasi terkait privasi dan keamanan.

Menurut [1], risiko adalah kemungkinan terjadinya suatu peristiwa yang dapat menimbulkan kerugian bagi suatu perusahaan atau instansi. Karena risiko selalu ada, penggunaan manajemen risiko yang tepat untuk meminimalkan potensi kerugian menjadi suatu kebutuhan yang sangat penting [2]. Risiko dapat menyebabkan kerugian terhadap kelangsungan proses bisnis dengan tingkat dampak yang beragam, baik dalam jangka pendek maupun jangka panjang [3]. Tingkat risiko dipengaruhi oleh berbagai faktor, termasuk tingkat paparan, lokasi, pengguna, kuantitas, dan kerentanan barang [4].

Menurut [5], manajemen risiko adalah pengambilan risiko secara rasional sepanjang proses manajemen risiko, termasuk penilaian risiko, pengembangan opsi dan langkah-langkah implementasi, dan manajemen risiko. Menurut [6] Manajemen risiko merupakan bagian terpadu dari proses manajemen berkelanjutan yang dirancang untuk mengurangi kerugian dan meningkatkan peluang.

Berdasarkan pengertian di atas, kita dapat menyimpulkan bahwa hakikat manajemen risiko adalah suatu metode, pendekatan, atau disiplin ilmu yang mempelajari berbagai jenis risiko. Ini mencakup pemahaman tentang bagaimana risiko muncul, strategi untuk menghindarinya dengan fokus pada tujuan penghindaran kerugian, upaya efektif dalam penggunaan sumber daya untuk mencapai tujuan, dan cara mencapai tujuan yang diinginkan dengan efektif dan efisien. Manajemen risiko melibatkan usaha proaktif untuk menangani potensi kerugian dengan cara yang rasional, sehingga tujuan dapat tercapai.

Manajemen risiko adalah suatu pendekatan strategis yang diterapkan oleh organisasi untuk mengenali, menilai, dan mengelola risiko-risiko yang dapat berdampak pada pencapaian tujuan mereka. Manajemen risiko juga merupakan proses memprediksi risiko agar suatu organisasi atau perusahaan tidak mengalami kerugian[7]. Tujuan utama dari manajemen risiko adalah mengurangi ketidakpastian dan memaksimalkan peluang yang mungkin muncul dalam suatu kegiatan atau proyek. Hal ini melibatkan serangkaian proses, termasuk identifikasi risiko, analisis risiko, pengembangan strategi mitigasi, dan pemantauan risiko secara berkelanjutan. Manajemen risiko memiliki peran penting dalam membantu organisasi merencanakan langkah-langkah proaktif untuk menghadapi dan mengatasi risiko yang dapat mempengaruhi keberhasilan mereka. Dalam konteks bisnis, manajemen risiko dapat melibatkan aspek keuangan, operasional, hukum, teknologi, dan reputasi.

Menurut [8], analisis risiko melibatkan dua pendekatan utama: Analisis Kualitatif, yang menggunakan penilaian deskriptif tingkat tinggi, sedang, dan rendah, serta Analisis Kuantitatif, yang menggambarkan dampak dan reliabilitas secara numerik. Terdapat pula metode campuran, dikenal sebagai metode *Hybrid*, yang menggabungkan kedua pendekatan sebelumnya.

TINJAUAN PUSTAKA

Penelitian terkait dengan topik manajemen resiko terhadap pemeliharaan TI, pernah dilakukan sebelumnya oleh [9], pada penelitian yang dilakukan oleh [9], mengindikasikan adanya pemeliharaan dan manajemen aset TI dengan optimal yang dilakukan oleh PT. HMS., Sumber daya TI yang diperiksa melibatkan banyak perangkat keras, seperti perangkat seluler (*Tab, iPhone, iPad*), *notebook*, *desktop*, dan monitor, yang semuanya disimpan di satu gudang.

Administrator bertujuan untuk mengenali faktor risiko yang harus diberi prioritas perawatan dan menentukan sumber daya TI mana yang memerlukan perhatian khusus, sesuai dengan kebutuhan yang ada. Hasil dari penelitian yang dilakukan memunculkan bukti bahwasannya untuk memenuhi persyaratan tersebut, analisis manajemen risiko TI menggunakan teknik analisis risiko kuantitatif (QRA) untuk mengidentifikasi dan mengukur aset TI serta secara efektif dan efisien mengidentifikasi aspek dan faktor yang memerlukan perhatian khusus. Penelitian yang dilakukan oleh [9], Rekomendasi kepada manajer adalah untuk mengutamakan perawatan laptop dengan fokus pada risiko kesalahan acak, seperti kegagalan perangkat keras kritis, kerusakan akibat kejadian luar biasa, dan potensi kehilangan data mendadak. Tindakan pengendalian lebih lanjut dapat melibatkan implementasi kebijakan backup secara teratur, pemantauan kesehatan perangkat keras secara berkala, dan memberikan pelatihan kepada pengguna guna menghindari kesalahan yang dapat mengakibatkan kerugian data.

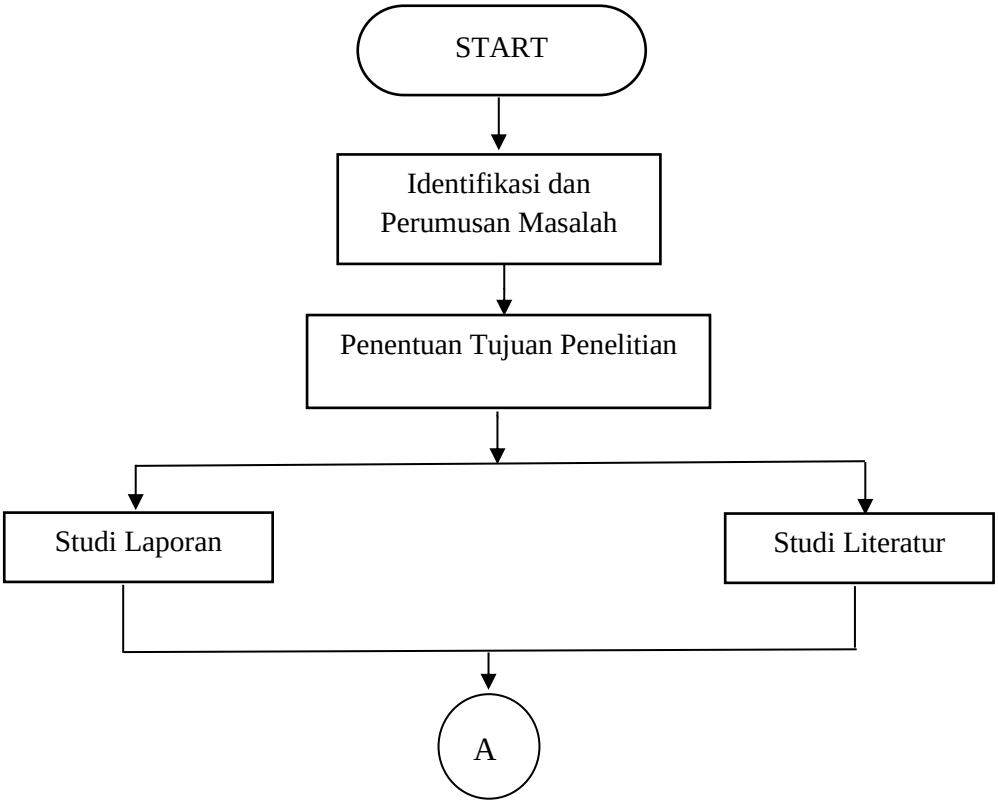
Penelitian yang sama juga dilakukan oleh peneliti lainnya pada bidang atau objek yang berbeda. Penelitian yang dilakukan oleh [10] berbasis metode Analisis Risiko Kualitatif dan Kuantitatif dilakukan dengan merujuk pada petunjuk dari NIST SP 800-30, mengindikasikan hasil penelitian berupa tingginya tingkat risiko yang diteliti, dapat ditentukan dengan mengklasifikasikan sumber ancaman. Setelah semua hasil analisis risiko disajikan, rekomendasi risiko diberikan dan diteruskan ke manajemen atau fasilitas TI. Temuan dari penelitian ini akan menjadi landasan bagi manajemen senior dalam proses pengambilan keputusan terkait kebijakan, prosedur, anggaran, operasi sistem, dan manajemen perubahan. Analisis Risiko Kuantitatif adalah pendekatan untuk merinci dan memahami estimasi risiko dengan mengintegrasikan perkiraan frekuensi serta potensi hasil dari insiden. [11]

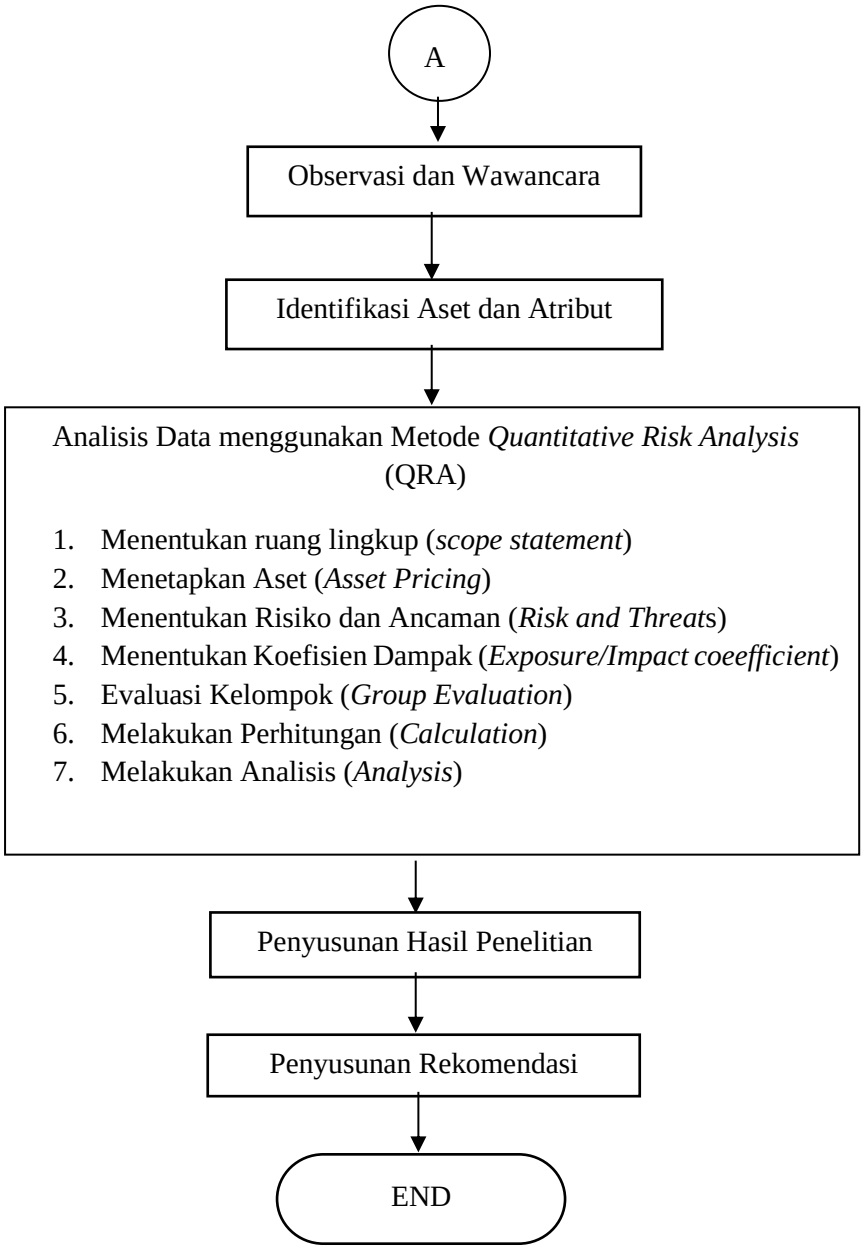
Penelitian lainnya dilakukan oleh [12], dimana dalam penelitiannya Syaputra menjelaskan bahwa Tata kelola dari TI adalah perwujudan kompleks dari struktur hubungan proses yang memandu dan mengendalikan organisasi untuk mencapai visi dan misinya dengan menciptakan nilai yang menyeimbangkan risiko TI dan prosesnya. Hasil penelitian yang dilakukan oleh [12], mengindikasikan bahwasannya jika dilihat dari sisi risiko, dengan potensi kerugian terbesar timbul dari sumber daya manusia internal yang berperan sebagai administrator server. Penilaian manajemen risiko kualitatif menentukan bahwa sumber ancaman berisiko tinggi adalah sumber daya manusia internal dan sistem infrastruktur TI.

Ketiga penelitian yang telah dipaparkan sebelumnya kemudian diperkuat dengan adanya temuan yang sama, dari penelitian yang dilakukan oleh [13]. Penelitian ini dilaksanakan pada Diskominfo Pemerintah Provinsi Riau. Penelitian yang dilakukan oleh [13], selaras dengan hal yang dikemukakan oleh [12] dimana dijelaskan

bahwasannya Teknologi informasi (TI) merupakan salah satu aspek penting dalam suatu perusahaan yang menunjang seluruh aktivitas bisnisnya. [13] juga menyebutkan bahwa kebemanfaatan Teknologi Informasi (TI) berperan penting dalam mendorong perubahan dalam proses bisnis, mengurangi biaya operasional, meningkatkan kualitas layanan kepada konsumen, dan pada akhirnya, mendukung peningkatan kinerja bisnis. Fungsinya tidak hanya sebagai alat pendukung aktivitas bisnis, melainkan juga memainkan peran kunci dalam pencapaian tujuan manajemen perusahaan. Pencapaian tujuan tersebut harus didukung dengan pengelolaan TI yang tepat. Metode yang digunakan oleh [13] memiliki perbedaan dengan metode yang diterapkan oleh [9] dan [10]. Dimana penelitian yang dilakukan oleh [13] memanfaatkan sebuah metode. Namun, diantara banyaknya penelitian yang selaras dengan penggunaan metode maupun hasil penelitian, terdapat pula penelitian yang menunjukkan perbedaan hasil, dimana perbedaan hasil ini juga berlandaskan pada
metode pendekatan atau metode penelitian yang berbeda.

METODE PENELITIAN





Gambar 1. *Flowchart* Penelitian

Penelitian ini menggunakan pendekatan *Quantitative Risk Analysis* (QRA) yang terdiri dari tujuh tahapan, yakni:

1. Menetapkan Ruang Lingkup (*Scope Statement*): Mengidentifikasi dan menentukan batasan serta ruang lingkup penelitian untuk memberikan panduan dalam proses analisis risiko.
2. Menetapkan Aset (*Asset Pricing*): Menilai dan menentukan nilai aset yang terlibat dalam risiko, membantu dalam penilaian dampak finansial dari potensi kerugian.
3. Resiko dan Ancaman (*Risks and Threats*): Identifikasi risiko dan ancaman yang mungkin terjadi terhadap aset TI, membentuk dasar analisis lebih lanjut.
4. Menentukan Koefisien Dampak (*Exposure*/*Impact coefficient*): Menetapkan faktor dampak atau koefisien dampak terhadap nilai aset, digunakan dalam perhitungan risiko.
5. Evaluasi Kelompok (*Group Evaluation*): Mengelompokkan risiko dan ancaman ke dalam kategori tertentu untuk memfasilitasi analisis lebih terfokus.
6. Melakukan Penghitungan (*Calculation*): Melakukan perhitungan kuantitatif berdasarkan data yang terkumpul, termasuk estimasi nilai dampak dan probabilitas terjadinya risiko.
7. Melakukan Analisis (*Analysis*): Menyusun evaluasi hasil perhitungan dan memberikan pemahaman mendalam terhadap tingkat risiko serta potensi dampaknya.

Pendekatan ini memberikan landasan struktural untuk mengidentifikasi, mengukur, dan menganalisis risiko secara kuantitatif dalam konteks pemeliharaan aset TI.

Pembuatan pernyataan ruang lingkup (*scope statement*) perlu memperhitungkan tiga faktor utama. Pertama, adalah penetapan obyek evaluasi secara spesifik, yang mencakup lokasi dan jumlah aset TI yang akan dianalisis. Lokasi yang relevan untuk evaluasi ini adalah gudang WH-TGR. Jumlah aset TI yang akan dievaluasi mencakup aset TI selama periode dari bulan Agustus hingga Desember 2023, dengan tipe dan model yang melibatkan Komputer, Laptop, Monitor, *Scanner*, *Printer*, serta CCTV (Kamera *Outdoor*). Berikutnya adalah penentuan metode analisa risiko, yaitu *Quantitative Risk Analysis* (QRA). Terakhir melakukan kalkulasi analisis untuk menentukan aspek yang perlu untuk dilakukan pengendalian.

Menentukan penilaian harga aset (*asset pricing*) melibatkan penetapan nilai yang sesuai dengan kategori dan model aset Teknologi Informasi (TI) yang tengah dianalisis, berdasarkan informasi dari sumber basis data Aset TI perusahaan, yang direpresentasikan oleh *platform Service-Now*. Tugas mengidentifikasi dan mengevaluasi risiko, bersama dengan ancaman, bertujuan untuk mengenali potensi dari sumber ancaman. Hal ini melibatkan penyusunan daftar yang merinci ancaman yang dapat muncul dari sumber-sumber tersebut. Tujuannya adalah untuk menerapkan informasi yang diperoleh dalam manajemen aset TI yang sedang dievaluasi. Sumber ancaman dalam konteks ini diartikan sebagai kondisi atau peristiwa yang berpotensi merusak sistem pemeliharaan aset TI.

Proses penilaian Risiko dan Ancaman dilakukan melalui pemberian nilai *Annualized Rate Occurrence* (ARO) pada setiap jenis ancaman (dapat dilihat pada Tabel 1). Nilai ARO diperoleh dari persentase potensi kemunculan setiap ancaman untuk setiap aset TI dalam kurun waktu satu tahun.

HASIL DAN PEMBAHASAN

Aset Teknologi Informasi yang dianalisis mencakup periode dari bulan Agustus 2023 hingga Desember 2023 dan melibatkan berbagai kategori dan jenis, seperti Komputer, Laptop, Monitor, Scanner, Printer, dan CCTV (Kamera *Outdoor*). Penelitian ini terfokus pada aset TI yang tergolong dalam kategori peralatan dan memiliki nilai yang dapat diukur.

Tabel 1. Penetapan Harga Aset Teknologi Informasi (*Asset Pricing*)

Jenis Aset	Detail Aset	Jumlah	Harga	Total
Desktop/PC		2	Rp6.150.000	Rp12.300.000
Laptop	Laptop (Toshiba)	16	Rp5.500.000	Rp124.300.000
	Laptop (Lenovo)	3	Rp5.500.000	
	Laptop (Dell)	4	Rp4.950.000	
Monitor	Sharp TV LED 50 Inch	5	Rp5.050.000	Rp25.200.000
Scanner		68	Rp900.000	Rp61.200.000
Printer	Printer (Canon Printer Ink)	2	Rp150.000	Rp36.190.000
	Printer (HP Laserjet M107w)	2	Rp850.000	
	Printer (Zebra Printer Barcode)	13	Rp2.630.000	
CCTV (*Outdoor Camera*)		132	Rp350.000	Rp46.200.000

Tabel 2. Ancaman (1 Tahun)

Ancaman (*Threat*)	ARO
Kekurangan Daya (*Power loss*)	2
Kesalahan tidak disengaja (*Accidental Errors*)	2
Pencurian atau penghancuran aset TI (*Theft or Destruction of Computing Resource*)	0.72
Kehilangan Komunikasi (*Communication Loss*)	0.68
Bencana Alam (*Natural disasters*)	0.4
Virus Komputer (*Computer Virus*)	0.29
Penyalahgunaan Hak Akses Karyawan (*Abuse of Access Privileges by Employees*)	0.24
Pihak luar yang berhasil akses ke sistem (*Successful Unauthorized System Access by Outsider*)	0.08
Penghentian tanpa bencana (*Non-disaster downtime*)	0.06
Kebakaran (*Fire*)	0.01

Proses penghitungan dilakukan dalam dua langkah. Langkah pertama melibatkan pembuatan spreadsheet dengan memasukkan nilai aset TI pada sumbu vertikal, yang diperoleh dari Tabel 1 Penetapan Harga Aset TI (Pricing Asset). Selanjutnya, nilai threat dimasukkan pada sumbu horizontal, diambil dari Tabel 2 Ancaman dalam satu tahun. Kemudian, nilai koefisien dampak (EF) untuk setiap aset TI seperti Komputer, Laptop, Monitor, Scanner, Printer, dan CCTV (Kamera Outdoor) juga dimasukkan.

Langkah kedua melibatkan pembuatan spreadsheet terpisah, di mana nilai di setiap sel dihasilkan melalui perkalian antara nilai aset TI, nilai threat, dan nilai koefisien dampak. Hasil perhitungan ini disajikan dalam Tabel 3, yang mencakup Nilai Threat dan Nilai Koefisien Dampak. Selanjutnya, Tabel 4 menggambarkan Kalkulasi Nilai Koefisien Dampak dalam bentuk nilai Finansial (Rupiah) berdasarkan perhitungan tersebut.

Tabel 3. Nilai Aset TI, Nilai Threat dan Nilai Koefisien Dampak

	Tipe Aset TI	**Komputer**	**Laptop**	**Monitor**	**Scanner**	**Printer**	**CCTV (*Outdoor Camera*)**
	Nilai Aset TI	Rp12.300.000	Rp116.800.000	Rp25.250.000	Rp61.200.000	Rp36.190.000	Rp46.200.000
Ancaman	**Risiko**						
Kehilangan Daya (*Power loss*)	2	0,1	0,1	0,1	0,2	0,1	0,2
Kesalahan tidak disengaja (*Accidental Errors*)	2	0,1	0,1	0	0,1	0,1	0,1
Pencurian atau penghancuran aset TI (*Theft or Destruction of Computing Resource*)	0,72	0,5	0,5	0,5	0,2	0,1	0,2
Kehilangan Komunikasi (*Communication Loss*)	0,68	0,1	0,1	0	0,3	0,1	0,3
Bencana Alam (*Natural disasters*)	0,4	0,2	0,2	0	0,1	0,1	0,1
Virus Komputer (*Computer Virus*)	0,29	0,5	0,5	0,5	0,5	0,5	0,5
Penyelewengan Hak Akses Karyawan (Misappropriation of Employee Access Rights)	0,24	1,0	1,0	1	1	1,0	1
Pembobonlan sistem oleh pihak luar (*Unauthorized System Access by External Parties*)	0,08	0,7	0,7	0,5	0,3	0,2	0,3
Pengestopan tanpa bencana (*Stop a downtime*)	0,06	0,2	0,2	0,2	0,2	0,1	0,2
Kebakaran (*Fire*)	0,01	0,5	0,5	0,5	0,3	0,3	0,3

Tabel 4. Perhitungan nilai koefisien dampak pada aspek finansial (dalam mata uang Rupiah).

Tipe Aset TI	**Komputer**	**Laptop**	**Monitor**	**Scanner**	**Printer**	**CCTV (*Outdoor Camera*)**	**Total**
Ancaman							
Kehilangan Daya (*Power loss*)	Rp2.460.000	Rp24.860.000	Rp5.050.000	Rp24.480.000	Rp7.238.000	Rp18.480.000	**Rp82.568.000**

Tipe Aset TI	Komputer	Laptop	Monitor	Scanner	Printer	CCTV (*Outdoor Camera*)	Total
Ancaman							
Kesalahan tidak disengaja (*Accidental Errors*)	Rp2.460.000	Rp24.860.000	Rp0	Rp12.240.000	Rp7.238.000	Rp9.240.000	**Rp56.038.000**
Pencurian atau Penghancuran Aset TI (Theft or Destruction of IT Assets)	Rp4.428.000	Rp44.748.000	Rp9.090.000	Rp8.812.800	Rp2.605.680	Rp6.652.800	**Rp76.337.280**
Kehilangan Komunikasi (*Communication Loss*)	Rp836.400	Rp8.452.400	Rp0	Rp12.484.800	Rp1.230.460	Rp9.424.800	**Rp32.428.860**
Bencana Alam (*Natural disasters*)	Rp984.000	Rp9.944.000	Rp0	Rp2.448.000	Rp1.447.600	Rp1.848.000	**Rp16.671.600**
Virus Komputer (*Computer Virus*)	Rp1.783.500	Rp18.023.500	Rp3.661.250	Rp8.874.000	Rp5.247.550	Rp6.699.000	**Rp44.288.800**
Penyelewengan Hak Akses Karyawan (Misappropriation of Employee Access Rights)	Rp2.952.000	Rp29.832.000	Rp6.060.000	Rp14.688.000	Rp8.685.600	Rp11.088.000	**Rp73.305.600**
Pembobonlan sistem oleh pihak luar (*Unauthorized System Access by External Parties*)	Rp688.800	Rp6.960.800	Rp1.010.000	Rp1.468.800	Rp434.280	Rp1.108.800	**Rp11.671.480**
Pengestopan tanpa bencana (*Stop a downtime*)	Rp147.600	Rp1.491.600	Rp303.000	Rp734.400	Rp108.570	Rp554.400	**Rp3.339.570**
Kebakaran (*Fire*)	Rp61.500	Rp621.500	Rp126.250	Rp183.600	Rp108.570	Rp138.600	**Rp1.240.020**
Total	**Rp16.801.800**	**Rp169.793.800**	**Rp25.300.500**	**Rp86.414.400**	**Rp34.344.310**	**Rp65.234.400**	

Untuk menetapkan aset TI yang memerlukan pengendalian, dilakukan Analisis *Across* Aset dengan mengumpulkan dan menilai peringkat nilai *Single Loss* Expectancy (SLE) pada masing-masing aset TI terhadap seluruh ancaman. Proses ini mengacu pada langkah-langkah kalkulasi yang dicontohkan dalam Tabel 4 sebagai panduan. Hasilnya digunakan sebagai dasar untuk menentukan peringkat jenis aset TI, disusun dari nilai dampak SLE tertinggi hingga terendah dalam bentuk nilai Finansial

(Rupiah) pada Tabel 4. SLE (*Single Loss Expectancy*) merujuk pada jumlah kerugian finansial pada setiap aset TI yang timbul akibat masing-masing ancaman.

Tabel 5. Ranking dan Nilai *Across Asset*

Ranking dan Nilai *Across Aset*	
Laptop	Rp169.793.800
Scanner	Rp86.414.400
CCTV	Rp65.234.400
Printer	Rp34.344.310
Monitor	Rp25.300.500
Komputer	Rp16.801.800

Untuk mengidentifikasi jenis ancaman atau risiko yang memerlukan pengendalian, dilakukan *Analysis Across Risk* secara komprehensif dengan mengakumulasi dan meranking nilai *Single Loss Expectancy* (SLE) dari setiap ancaman terhadap seluruh aset TI. Hasil tersebut menjadi dasar untuk menetapkan peringkat jenis ancaman atau risiko, disusun berdasarkan dampak SLE mulai dari yang terbesar hingga terkecil dalam nilai finansial (Rupiah). Informasi ini terdokumentasi dalam Tabel 6 Peringkat dan Nilai Risiko Secara Keseluruhan.

Tabel 6. Ranking dan Nilai *Across Risk*

Ranking dan Nilai *Across Aset*	
Kehilangan Daya (*Power loss*)	Rp82.568.000
Pencurian atau penghancuran aset TI (*Theft or Destruction of Computing Resource*)	Rp76.337.280
Penyalahgunaan Hak Akses Karyawan (*Abuse of Access Privileges by Employees*)	Rp73.305.600
Kesalahan tidak disengaja (*Accidental Errors*)	Rp56.038.000
Virus Komputer (*Computer Virus*)	Rp44.288.800
Kehilangan Komunikasi (*Communication Loss*)	Rp32.428.860
Bencana Alam (Natural disasters)	Rp16.671.600

Ranking dan Nilai *Across Aset*	
Pihak luar yang berhasil akses ke sistem (*Successful Unauthorized System Access by Outsider*)	Rp11.671.480
Penghentian tanpa bencana (*Non-disaster downtime*)	Rp3.339.570
Kebakaran (*Fire*)	Rp1.240.020

Berdasarkan data pada Tabel 5, terlihat bahwa Laptop menjadi aset TI dengan dampak kerugian paling tinggi, mencapai Rp169.793.800, sedangkan Komputer memiliki dampak terendah dalam menghadapi ancaman dan risiko. Melalui Analisis Komprehensif Aset, dapat diidentifikasi aset TI yang seharusnya diberikan prioritas dalam penerapan pengendalian, terutama menghadapi berbagai potensi ancaman dan risiko.

Pada Tabel 6, terlihat bahwa Risiko Kehilangan Daya memiliki dampak kerugian paling signifikan, yaitu sebesar Rp82.568.000, sedangkan Risiko Kebakaran memiliki dampak paling rendah. Analisis Aset Menyeluruh membantu menentukan prioritas pengendalian risiko untuk aset TI berdasarkan dampak finansial, dengan total dampak mencapai Rp397.889.210.

Rekomendasi dari analisis tersebut adalah memberikan tindakan pengendalian risiko terutama pada aset TI jenis Laptop yang memiliki potensi kerugian terbesar. Selain itu, ancaman Kehilangan Daya perlu mendapatkan perhatian khusus karena memiliki dampak kerugian tertinggi di antara risiko lainnya.

KESIMPULAN DAN SARAN

Penelitian mengenai evaluasi risiko manajemen dalam pemeliharaan aset Teknologi Informasi dengan menerapkan metode *Quantitative Risk Analysis* (QRA) berhasil mengenali faktor risiko yang membutuhkan prioritas perawatan pada aset TI. Nilai potensi kerugian tertinggi tercatat pada aset TI berupa Laptop, mencapai Rp169.793.800, sedangkan risiko Kehilangan Daya mencapai Rp82.568.000. Hasil analisis memberikan dasar yang kuat untuk pengambilan keputusan strategis dalam merancang mitigasi risiko yang efektif.

Melalui *Quantitative Risk Analysis*, perusahaan dapat memperoleh pemahaman yang matang terhadap risiko dan merancang rencana manajemen risiko yang adaptif dan efisien. Implementasi langkah-langkah yang diusulkan diharapkan dapat meningkatkan ketahanan operasional dan memastikan integritas serta ketersediaan aset TI dalam jangka panjang.

Saran untuk pemeliharaan aset *warehouse* adalah sebagai berikut:

1. Pengembangan Jadwal Pemeliharaan Teratur: Implementasikan jadwal pemeliharaan rutin dan terencana untuk setiap jenis aset, mencegah kegagalan yang tidak terduga, dan memaksimalkan umur pakai aset.

2. Penerapan Kriteria Prioritas Pemeliharaan: Buat kriteria prioritas untuk pemeliharaan aset, memfokuskan perhatian pada aset yang kritis untuk operasional dan keberlanjutan organisasi.
3. Pelatihan dan Kesadaran Pengguna: Selenggarakan program pelatihan rutin untuk meningkatkan kesadaran keamanan di kalangan pengguna, mengurangi risiko yang dapat disebabkan oleh kelalaian atau tindakan tidak sengaja.

.

DAFTAR PUSTAKA

[1] R. Bisma, "Manajemen Risiko Aset Teknologi Informasi: Studi kasus Implementasi Manajemen Risiko SPBE Dinas Komunikasi dan Informatika Pemerintah Kota Balikpapan," 2022.

[2] P. P. Thenu, A. F. Wijaya, C. Rudianto, U. Kristen, and S. Wacana, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 5 (STUDI KASUS: PT GLOBAL INFOTECH)," 2020.

[3] A. F. Rohman, A. Ambarwati, and E. Setiawan, "ANALISIS MANAJEMEN RISIKO IT DAN KEAMANAN ASET MENGGUNAKAN METODE OCTAVE-S IT RISK MANAGEMENT ANALYSIS AND ASSET SECURITY USING OCTAVE-S METHOD," *Journal of Information Technology and Computer Science (INTECOMS)*, vol. 3, no. 2, 2020.

[4] J. N. Utamajaya, A. Afrina, and A. N. Fitriah, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA PERUSAHAAN TOKO UJUNG PANDANG GROSIR PENAJAM PASER UTARA MENGGUNAKAN FRAMEWORK ISO 31000:2018," *Sebatik*, vol. 25, no. 2, pp. 326–334, Dec. 2021, doi: 10.46984/sebatik.v25i2.1430.

[5] Z. Arifin, *Dasar-Dasar Manajemen Bank Syariah*. Jakarta: Pustaka Alfabet, 2005.

[6] T. L. Ahmad and H. Fitria, "ANALISIS DAMPAK MANAJEMEN RANTAI PASOK PADA KEUNGGULAN BERSAING DAN KINERJA PERUSAHAAN (STUDI PADA UMKM KLASTER BANDENG PRESTO SEMARANG)," *Jurnal Aplikasi Ilmu Teknik Industri*, vol. 2, no. 2, pp. 1–9, 2021.

[7] D. Pratiwi and B. Kurniawan, "Pengaruh Penrapan Manajemen Resiko Terhadap Kinerja Keuangan …," 2017.

[8] J. W. Merrit, "A Method for Quantitative Risk Analysis," *CISSP. Wang Global. Virginia*, 2000.

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

[10] A. G. R. Padang, "Penilaian Manajemen Risiko TI Menggunakan Quantitative dan Qualitative Risk Analysis," *Sistemasi: Jurnal Sistem Informasi* , vol. 10, no. 3, pp. 527–537, 2021.

[11] A. Anindyta, I. Eko Julianto, and A. Nugroho, "Analisis Risiko Kebocoran Gas pada Sistem Perpipaan Recycle Gas Hydrofinishing Plant dengan Menggunakan Metode Quantitative Risk Analysis (QRA) (Studi Kasus : Perusahaan Produksi Pelumas)," 2017.

[12] A. Syaputra, "Penilaian IT Governance dalam Manajemen Risiko IT Menggunakan Metode Quantitative dan Qualitative Risk Analysis," *Jurnal Manajemen Informatika (JAMIKA)* , vol. 3, no. 2, pp. 63–73, 2022.

[13] M. S. Zulvi, "Manajemen Risiko Teknologi Informasi menggunakan Metode FMEA (Studi Kasus: Diskominfo Pemprov Riau)," *Jurnal Komputer Terapan* , vol. 8, no. 2, pp. 381–390, 2022.