Jurnal Manajemen Informatika (JAMIKA)
Volume 12 Nomor 1 Edisi April 2022
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Penilaian IT Governance dalam Manajemen Risiko IT Menggunakan Metode *Quantitative* dan *Qualitative Risk Analysis*

Assessment of IT Governance in IT Risk Management Using Quantitative Methods and Qualitative Risk Analysis

Asep Syaputra
Institut Teknologi Pagar Alam, Kota Pagar Alam, Indonesia,
Program Studi Teknik Informatika, Institut Teknologi Pagar Alam, Pagar Alam, Indonesia
*E-mail: asepsyaputra68@sttpagaralam.ac.id

Abstrak

Tata Kelola IT adalah struktur hubungan proses yang memandu dan mengendalikan suatu organisasi untuk mencapai visi dan misi dengan menambahkan nilai yang akan menyeimbangkan risiko dengan IT dan prosesnya. Metode analisis yang digunakan dalam penelitian ini adalah analisis risiko kuantitatif dan kualitatif. Pendekatan Quantitative Risk Analysis (QRA) berfokus pada analisis pemeliharaan sumber daya IT untuk menemukan faktor risiko yang perlu mendapat pertimbangan dan penanganan yang serius. Untuk metode analisis risiko kualitatif, NIST SP 800-30 digunakan untuk menganalisis berbagai atribut ancaman dan risiko untuk memberikan pedoman pengelolaan instalasi IT di Kampus XYZ. Berdasarkan penilaian risiko QRA, SDM Internal yang memiliki akses ke server dihitung sebagai potensi kerugian kampus yang paling tinggi. Hal ini terlihat pada aspek risiko dimana kerugian yang disebabkan oleh SDM Internal yang memainkan peran sebagai admin server memiliki potensi kerugian yang paling besar. Penilaian kualitatif manajemen risiko menemukan sumber ancaman dengan risiko tinggi adalah SDM Internal dan Sistem Insfrastruktur IT. Tingkat risiko ini dapat dideteksi selama proses klasifikasi sumber bahaya. Penyajian seluruh hasil analisis risiko dapat memberikan hasil rekomendasi risiko yang akan dikomunikasikan bersama manajemen IT kampus. Untuk kemudian dapat membantu pihak kampus dalam membuat sebuah keputusan yang memuat tentang kebijakan, prosedur, anggaran, operasi sistem, dan manajemen perubahan.

Kata kunci: *Assessment IT Governance, qualitative risk analysis, nist sp 800-30.*

Abstract

IT Governance is the structure of process relationships that guide and control an organization to achieve its vision and mission by adding value that will balance risks with IT and its processes. The analytical method used in this research is quantitative and qualitative risk analysis. The Quantitative Risk Analysis (QRA) approach focuses on analyzing the maintenance of IT resources to find risk factors that need serious consideration and treatment. For the qualitative risk analysis method, NIST SP 800-30 is used to analyze the various threat and risk attributes to provide guidelines for managing IT installations at XYZ Campus. Based on the QRA risk assessment, Internal HR who has access to the server is calculated as the highest potential campus loss. This can be seen in the risk aspect where losses caused by Internal HR who play the role of server admins have the greatest potential for losses. Qualitative assessment of risk management finds sources of threats with high risk are Internal HR and IT Infrastructure Systems. This level of risk can be detected during the hazard source classification process. The presentation of all risk analysis results can provide risk recommendations that will be communicated to campus IT management. To then be able to assist the campus in making a decision that includes policies, procedures, budgets, system operations, and change management.

Keywords: *Assessment IT Governance, qualitative risk analysis, nist sp 800-30.*

Naskah diterima 15 Mar. 2022; direvisi 8 Apr. 2022; dipublikasikan 9 Apr. 2022.

I. PENDAHULUAN

Dengan pesatnya perkembangan *Information Technology (IT)* saat ini, hal itu berpengaruh besar terhadap peran dalam berbagai bidang kegiatan organisasi dan perusahaan. Bahkan sangat berperan penting dalam menjaga proses bisnis tetap efisien dan efektif terhadap organisasi dan perusahaan [1]. Terlebih pada masa pandemi saat ini, peran IT sangat penting karena semua pekerjaan dan bisnis yang dilakukan membutuhkan proses *paperless* dan *online*, seperti halnya kampus-kampus yang mulai menjalankannya menjadi proses layanan dan bisnis bagi perusahaan [2]. Keberhasilan tata kelola perusahaan saat ini tergantung pada ruang lingkup pengelolaan IT.

Tata kelola pada bagian IT adalah bagian dari tata kelola instansi atau perusahaan. Beberapa hal utama yang diperhatikan dengan tata kelola perusahaan adalah tata kelola IT, terkait dengan bagaimana manajemen senior memastikan bahwa manajer sistem informasi (CIO) dan organisasi TI dapat memberikan nilai kepada organisasi dalam hal nilai [3]. Kegiatan utama dalam bidang pendidikan tinggi, sesuai dengan fungsi utamanya, yaitu pendidikan, adalah pelayanan akademik [4]. Dalam mengimplementasikan layanan akademik ini, sangat penting untuk menggunakan IT yang dapat menjaga kecepatan, kenyamanan dan kemudahan dalam layanan akademik untuk memberikan mahasiswa layanan akademik berkualitas tinggi [5].

Penggunaan IT dalam semua proses penyampaian layanan akademik di Kampus tentunya dapat terjadi berbagai ancaman dan hambatan terhadap risiko IT yang akan mempengaruhi kualitas layanan dan berujung pada tingkat kepercayaan masyarakat terhadap kualitas layanan yang disediakan kampus. Seberapa besar risiko yang ditimbulkan dalam penggunaan IT dan belum pernah dilakukan penelitian [6]. Penelitian ini melakukan proses penilaian (referensi NIST 800-30) lanjut. Manajemen harus menyadari berbagai ancaman IT yang terjadi atau mungkin timbul dilingkungan kampus dan mengembangkan strategi untuk mengelola risiko yang berbeda ini. Instalasi IT adalah unit di Kampus XYZ dengan tugas mengatur dan mengelola penggunaan IT di Kampus. Departemen instalasi IT ini memainkan peran penting dalam mengelola semua aktivitas atau layanan bisnis yang didukung IT, tetapi tidak memiliki identifikasi ancaman IT di kampus yang teratur dan terperinci. Manajemen sumber daya IT yang tidak memadai dapat menimbulkan berbagai risiko bagi IT.

Dari penelitian yang telah dilakukan oleh Adhie Thyo Priandika [7] dengan judul Analisis Tata Kelola IT Dengan Domain Dss Pada Instansi Xyz Menggunakan Cobit 5, pada penelitian ini Model kematangan *(Maturity Level)* digunakan untuk pengelolaan dan kontrol pada proses teknologi informasi didasarkan pada metode evaluasi organisasi, sehingga dapat mengevaluasi sendiri dari level tidak ada (0) hingga optimis. Model kematangan dimaksudkan untuk mengetahui keberadaan persoalan yang ada dan bagaimana menentukan prioritas peningkatan. Analisis tata kelola IT dengan menggunakan sub domain DSS.01, DSS.02, DSS.03, DSS.04, DSS.05, dan DSS.06 dengan hasil evaluasi tingkat kematangan *(maturity level)* dengan tingkat kematangan yang berada pada level 5 *(Optimised)* yang berarti penerapan teknologi informasi telah memiliki ukuran dan dijadikan sebagai sasaran kinerja perusahaan. Sehingga dalam menerapkan tata kelola TI, yaitu pada proses pengarsipan dokumen secara umum tingkat kematangan perusahaan dalam mengelola teknologi informasi sudah mengacu pada *level bast practice.*

Penelitian selanjutnya dilakukan oleh Susilo yang membahas tentang Analisa Tingkat Risiko 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)*, dalam penelitian ini Model Framework NIST dengan cara mengintegrasikan konsep *IT Risk Management* melalui kegiatan penilaian *(assesment)* dan rekomendasi strategi mitigasi risiko dapat mengukur tingkat probabilitas ancaman serta tingkat dampaknya bagi institusi. Dengan melakukan perhitungan *(Calculation) impact analysis* (perhitungan terhadap dampak dari kejadian gangguan keamanan) berupa *single loss expectancy (SLE)* dan *Annualized loss expectancy (ALE*), *Annualized loss expectancy (ALE)*, yaitu nilai moneter yang akan hilang karena gangguan keamanan terhadap asset, pada jangka waktu satu tahun. Dimana: SLE adalah *Single loss expectancy*, merupakan nilai kerugian secara financial pada setiap asset TI yang diakibatkan oleh setiap threat. *ARO* adalah *Annualized rate occurrence*, merupakan nilai prosentase potensi setiap *threat* untuk setiap asset IT dalam 1 tahun. Yang kemudian, melalui kegiatan wawancara mendalam dengan Pihak Pengelola TIK menggunakan dokumen *IT General Questionnaire* serta *review* dokumen operasional ditemukan hasil analisa risiko yang dirangkum dalam bentuk rencana penerapan perlindungan yang mampu mengurangi tingkat risiko tata kelola teknologi informasi PTS. XYZ. Semakin banyak kegiatan pengelolaan TIK yang belum memiliki pengendalian, maka semakin tinggi tingkat risiko pengelolaan TIK. Dari beberapa penelitian yang telah dilakukan sebelumnya, peneliti menemukan permasalahan pada tata kelola IT dibagian manajemen risiko IT yang sangat rentan akan terjadi permasalahan, dengan beberapa metode sehingga hasil akhir dapat ditemukan sebuah pedoman yanag akan menemukan titik risiko yang paling tinggi dan solusi yang paling tepat [8].

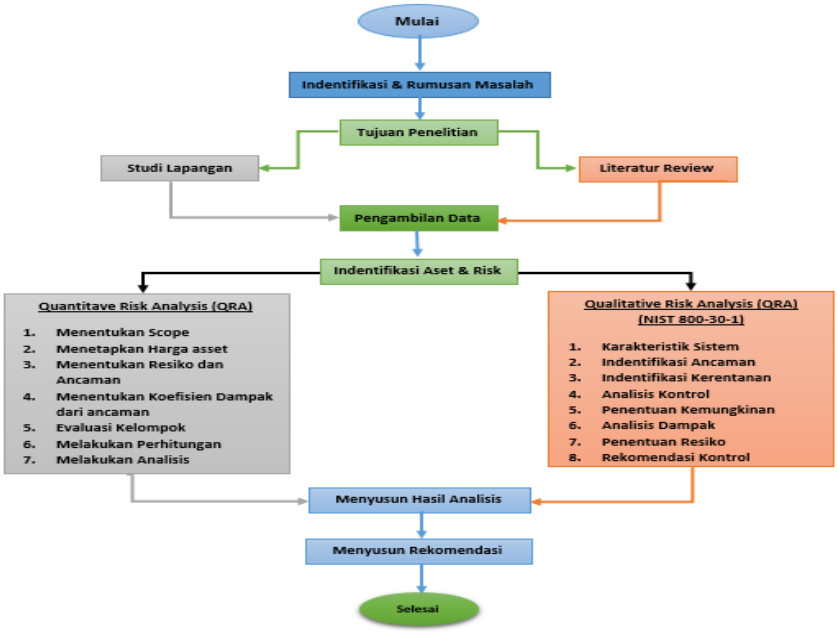
Berdasarkan wawancara dengan manajer instalasi IT di Kampus XYZ, beberapa masalah muncul di Kampus XYZ. Kerusakan komputer yang tidak menyala pada jam kerja karena kurangnya perawatan secara berkala, membuat pelayanan Kampus, mahasiswa dan Layanan akademik menjadi sulit dan sistem tidak dapat mengakses dan menampilkan data. Tim penyiapan IT kampus XYZ tidak melakukan penilaian risiko IT reguler untuk mencegah terulangnya insiden ini dan ancaman IT lainnya, Penilaian Manajemen Risiko IT harus dilakukan di Kampus XYZ. Tujuan dari penelitian ini adalah untuk menganalisis pemeliharaan aset IT melalui analisis risiko kuantitatif, menganalisis berbagai risiko dan ancaman, dan memperoleh rencana mitigasi risiko yang dapat mencegah tantangan dan ancaman serta kerugian pada infrastruktur *backbone IT* melalui analisis risiko kualitatif. Penggunaan analisis risiko kuantitatif dan analisis risiko kualitatif diharapkan memberikan

Jurnal Manajemen Informatika (JAMIKA)
Volume 12 Nomor 1 Edisi April 2022
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

rekomendasi manajemen risiko IT kuantitatif dan kualitatif yang lebih komprehensif kepada instalasi IT di kampus XYZ. Hasil penelitian ini bermanfaat bagi instansi IT kampus XYZ sebagai inventarisasi risiko pada aset IT, berdasarkan mitigasi risiko sebagai dasar analisis risiko kuantitatif dan kualitatif.

II. METODE PENELITIAN

Adopsi IT untuk penggunaan IT harus disertai dengan tata kelola yang ditargetkan untuk meminimalkan gangguan lebih lanjut terhadap proses bisnis [9]. Penelitian terdahulu mengungkapkan dua ancaman utama terhadap aset IT sepanjang tahun. Salah satunya adalah hilangnya Koneksi *internet*, yang lain adalah hilangnya daya listrik. Perhitungan *Financial Value Impact Factor (Rs)* menunjukkan bahwa risiko kesalahan yang tidak disengaja merupakan potensi kerugian terbesar bagi perusahaan. Penelitian ini tidak memberikan manajemen risiko atau analisis manajemen yang akurat untuk mengurangi potensi biaya kerugian aset IT perusahaan. Anda juga tidak perlu memberikan panduan tentang cara menangani risiko yang terkait dengan aset IT masa depan [10].



Gambar 1. Alur Penelitian

Penelitian selanjutnya, Kebutuhan akan stabilitas sistem menjadi semakin penting karena penyediaan layanan IT yang dibutuhkan oleh mahasiswa dan tantangan yang ditimbulkan oleh layanan IT salah satunya adalah SIAKAD (Sistem Informasi Akademik) Kampus XYZ mengenai kerentanan keamanan informasi. Jika masalah ini tidak dapat diatasi secara berkelanjutan, konsekuensinya adalah membahayakan atau membahayakan keberlanjutan sistem (terutama akademisi). Alur pada penelitian dapat dilihat pada gambar 1.

Pada penelitian ini dimulai dengan mengindentifikasi masalah yang terjadi, lalu ditemukan sebuah rumusan masalah yang menyatakan bahwa belum adanya pedoman yang dapat mengantisipasi risiko dalam manajemen IT pada Kampus XYZ, kemudian diindentifikasi risiko dari asset insfrastruktur yang akan digunakan menggunakan *Quantitative* dan *Qualitative Risk Analysis.* Diantaranya menggunakan NIST SP 800-30, NIST SP 800-30 menyediakan pembuat keputusan dengan informasi keamanan yang terbukti komprehensif dan konsisten, pemodelan sumber daya yang terstruktur untuk mengidentifikasi ancaman, dan analisis keamanan informasi dari berbagai pemangku kepentingan yang dapat diidentifikasi Menyediakan fitur lainnya. Dalam penelitian ini, peneliti menggunakan NIST SP800-26 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. Menetapkan kontrol sangat diperlukan karena dapat meminimalisir tingkat risiko pada data ke tingkat yang lebih dapat kontrol secara terstruktur. Kemudian akan dilajutkan ke langkah berikutnya, yaitu mitigasi dan penilaian risiko [11].

Analisis risiko kuantitatif adalah teknik menganalisis risiko dengan angka untuk mewakili efektivitas dan probabilitas. Jika nilai risiko kuantitatif yang diharapkan berlaku untuk penerapan pengukuran numerik biaya sumber daya yang dinyatakan dalam jumlah, bersama dengan probabilitas kerugian, jumlah kasus, dan

nilai frekuensi kejadian serta ancaman kerentanan, metode ini memperoleh hasil ke dalam bentuk indikator [12]. *Fase QRA (Quantitative Risk Analysis)* terdiri dari tujuh fase penting berikut ini. (1) Mengidentifikasi aspek survey, (2) Mengidentifikasi harga setiap aset IT sesuai dengan fungsi IT, (3) Mengidentifikasi ancaman dan risiko dari sumber daya yang dievaluasi, penyebab potensi ancaman dan penyebab risiko Mengidentifikasi dan mencantumkannya, (4) Upaya yang dilakukan untuk mengidentifikasi faktor-faktor yang berpengaruh dengan mengidentifikasi kerentanan aset IT terhadap risiko tertentu dan dengan menganalisis kerentanan aset TI untuk mengidentifikasi faktor eksposur (EF) meningkat, (5) Evaluasi kelompok, (6) perhitungan, (7) evaluasi akhir dianalisis dengan memasukan nilai yang telah diperoleh dalam *spreadsheet* [13].

Dengan menggunakan pedoman NIST SP80030 pada Metode analisis risiko kualitatif, panduan ini dapat digunakan nanti di fase untuk menemukan rekomendasi ancaman dan risiko untuk unit IT. Penelitian sebelumnya memanfaatkan metode ini untuk menganalisi risiko. Pada penelitian ini menerapkan dua metode, analisis risiko kuantitatif dan analisis risiko kualitatif, untuk menemukan hasil dari analisis penilaian risiko yang lebih baik dan mengintegrasikan kekurangan masing-masing ke dalam analisis penilaian risiko. Menganalisis secara kuantitatif digunakan untuk menemukan unsur-unsur *maintenance* aset TI, Analisis kualitatif, disisi lain, lebih banyak digunakan untuk menemukan ancaman dan risiko yang dihadapi oleh instalasi TI di suatu kampus XYZ.

Data kualitatif dan kuantitatif adalah dasar dari penelitian ini. Gambar 1 menunjukan alur penelitian. Objek penelitian ini berfokus pada instalasi IT yang ada pada salah satu kampus yang berada di kawasan Kota Pagar Alam. Data penelitian didapatkan dari pengelola instalasi IT serta dari teknisi IT pada Kampus tempat penelitian dilakukan. Nama kampus tempat penelitian dilakukan bersifat rahasia karena penelitian ini difokuskan pada pembahasan risiko TI terhadap aset IT dikampus dan instalasi IT itu sendiri.

Sebagian besar data penelitian merupakan data yang *up-to-date*, reliabel dan bisa dihitung hasilnya. Sumber data yang digunakan adalah primer, data diambil dari lokasi instalasi IT kampus XYZ melalui wawancara pribadi dengan kepala bagian IT. Data sekunder didapatkan pada luar instalasi IT Kampus XYZ. Penelitian ini menggunakan beberapa metode pengumpulan data, seperti survei manajer IT dan teknisi infrastruktur IT di kampus XYZ, tentang masalah sumber daya IT dan manajemen risiko. Wawancara dengan *installer* IT Kampus XYZ dan beberapa profesional IT Kampus XYZ menggunakan media *online* dalam format *WhatsApp* dan *email* dan Terakhir dengan metode observasi.

Bagian analisis risiko adalah penilaian risiko yang berbentuk sebuah portofolio. Proses penilaian pada bagian risiko bisa dilakukan secara kuantitatif dan kualitatif [14]. Analisis menggunakan dua metode, yaitu analisis risiko kuantitatif *(QRA)*, yang terdiri dari analisis risiko tujuh langkah [15]. Metode NIST SP 80030 digunakan sebagai analisis risiko kualitatif, NIST SP 80030 juga memiliki langkah analisis yang akan menemukan masalah yang dilanjutkan dengan membuat rekomendasi penyelesaian risiko pada insfrastruktur IT di kampus XYZ.

Identifikasi Aset dan Risiko

Dalam penelitian ini, manajer aset TI (*chief installation engineer),* memberikan spesifikasi IT dan jumlah aset IT pada kampus XYZ. Beberapa jenis aset IT yang dianggap sebagai asset yang paling berpengaruh penting *server, router, monitor, laptop, printer* dan Genset, seperti pada Tabel 1 dibawah. Tahap pertama analisis untuk menentukan volume, yaitu instalasi teknologi informasi yang berada pada salah satu kampus di kota Pagar Alam. Penelitian ini berjalan September 2020 hingga Agustus 2021 dan mencakup jenis aset TI termasuk *server, router, monitor*, laptop, printer, dan generator.

Quantitative Risk Analysis

Langkah selanjutnya adalah menentukan harga sumber daya IT. Tabel 1 meneunjukan biaya sumber daya IT yang telah disurvei dengan melihat harga pembelian awal aset IT tersebut. Langkah selanjutnya adalah menetapkan nilai *Annualize Rate Occurrence (ARO)* untuk mengidentifikasi risiko dan ancaman dan mencari nilai total *Annualized Loss Expectancy (ALE)* yang dihitung adalah kerugian moneter untuk suatu aset karena risiko selama periode satu tahun. *ARO* dihitung dengan menghitung persentase ancaman yang dihadapi dalam satu tahun saat IT kampus XYZ dipasang yang bisa dilihat pada Tabel 2, dan Tabel 3 menunjukan nilai *Impact Factor* (factor ancaman) untuk setiap sumber daya IT. Penjumlahan dengan cara perhitungan rumit mulai terjadi karena pada tahapan ini harus menghitung satu nilai Faktor Dampak untuk setiap bagian jenis aset IT.

Jurnal Manajemen Informatika (JAMIKA)
Volume 12 Nomor 1 Edisi April 2022
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

TABEL 1
DAFTAR HARGA ASET IT

Asset Type	Jumlah	Harga Per-Satuan	Total Harga
Server	1	115,000,000	115,000,000
Router	5	13,000,000	65,000,000
Laptop	3	9,000,000	27,000,000
Printer	3	1,200,000	3,600,000
Monitor	5	600,000	3,000,000
Genset	1	15,000,000	15,000,000
	Jumlah		228,600,000

TABEL 2
ANCAMAN (1 TAHUN)

No	Ancaman	ARO
1.	Hilangnya energi listrik / kehilangan daya	1. 2
2.	Lost Contact / kehilangan jaringan	1. 2
3.	Kesalahan secara tidak sengaja *(Accidental Error)*	0
4.	Virus pada Komputer	0. 2
5.	Pelanggaran hak akses	0. 3
6.	Bencana alam	0. 2
7.	Pencurian dan Perusakan Aset IT	0. 1
8.	Pemaksaan akses ke sistem dari pihak eksternal / *Hack*	0
9.	Penghentian sistem untuk perangkat TI non-darurat	0
10.	Bencana Kebakaran	0. 01
11.	Bencana Alam Gempa	0. 01

Pada tabel 1 dapat dilihat nilai aset adalah nilai finansial setiap aset IT yang nilainya ditentukan pada langkah penetapan harga aset [12]. Sedangkan pada tabel 2 menampilkan *Eksposur Factor (EF)* yang terdapat nilai Persentase kerugian karena ancaman terhadap sumber daya IT, pada EF memiliki jarak rentang nilai antara 0 dan 1 dalam rumus (2), *Annualized Rate Occurrence (ARO),* persentase potensi ancaman terhadap aset IT dalam setahun [13].

TABEL 3
KOEFISIEN DAMPAK SUMBER DAYA TI

No	Ancaman	EF				
		Server	Router	Laptop	Printer	Monitor
1	Kehilangan energi listrik / kehilangan daya	0,3	0,3	0,5	0,3	0,3
2	Kehilangan komunikasi / kehilangan jaringan	0,3	0,0	0,0	0,0	0,0
3	Kesalahan tidak sengaja *(Accidental Error)*	0,5	0,3	0,3	0,5	0,5
4	Komputer Virus	0,0	0,0	0,3	0,0	0,0
5	Pelanggaran hak akses	0,3	0,3	0,3	0,0	0,0
6	Bencana alam	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
8	Akses eksternal paksa ke sistem/ *Hack*	0,3	0,0	0,5	0,0	0,3
9	Penghentian proses perangkat TI diluar bencana	0,3	0,3	0,3	0,3	0,3
10	Bencana Kebakaran	1	1	1	1	1
11	Bencana Alam Gempa Bumi	1	1	1	1	1

III. HASIL DAN PEMBAHASAN

Setelah semuanya dihitung, hasilnya bisa digunakan dalam mengetahui aset IT yang dianggap memiliki potensi kerugian pada finansial paling besar, serta dilakukan *Across Asset Analysis* dengan memeringkatkan jumlah total perhitungan *ALE* pada pengurutan masing-masing jenis aset IT dari terbesar hingga paling kecil.

Jurnal JAMIKA Manajemen Informatika
Jurnal Manajemen Informatika (JAMIKA)
Volume 12 Nomor 1 Edisi April 2022
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Sebaliknya, untuk mengetahui ancaman mana yang berbahaya bagi perusahaan, yang harus dilakukan adalah memberi peringkat jumlah total nilai ALE yang dihitung berdasarkan setiap ancaman *(Across Risk)* [18]. Dari Tabel 4 dapat diketahui bahwa Nilai Lintas Aset paling tinggi, yaitu *Server* Rp. 129,950,000, dan Nilai Aset Terendah adalah *Monitor*

Dengan nilai Rp. 2.040.000. Nilai kumulatif risiko tertinggi, yaitu padamnya listrik *(power loss)* dengan nilai Rp. 83.376.000, selanjutnya kehilangan jaringan komunikasi (*loss of network communication loss)* dengan nilai Rp. 41.400.000. Ada 4 ancaman yang memiliki nilai risiko 0, yaitu ketidaksengajaan kesalahan, virus pada komputer, 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)	Monitor (Rp)
1	Kehilangan energi listrik / kehilangan daya	41,400,000	23,400,000	16,200,000	1,296,000	1,080,000
2	Kehilangan komunikasi / kehilangan jaringan	41,400,000	0	0	0	0
3	Kesalahan tidak sengaja *(Accidental Error)*	0	0	0	0	0
4	Komputer Virus	0	0	1,620,000	0	0
5	Pelanggaran hak akses	10,350,000	5,850,000	2,430,000	0	0
6	Bencana alam	23,000,000	13,000,000	5,400,000	720,000	600,000
7	Penghancuran dan pencurian Aset IT	11,500,000	6,500,000	2,700,000	360,000	300,000
8	Akses eksternal paksa ke sistem/ Hack	0	0	0	0	0
9	Penghentian proses perangkat TI diluar bencana	0	0	0	0	0
10	Bencana Kebakaran	1,150,000	650,000	270,000	36,000	30,000
11	Bencana Alam Gempa Bumi	1,150,000	650,000	270,000	36,000	30,000
	Total	129,950,000	50,050,000	28,890,000	2,448,000	2,040,000

Qualitative Risk Analysis

Metode NIST SP 800-30 digunakan sebagai metode analisis risiko kualitatif. Metode NIST SP 800-30 selama tahap analisis risiko dapat memberikan rekomendasi untuk pengendalian. Tahap awal dalam NIST SP 800-30 adalah karakterisasi sistem atau *system characterization* mendefinisikan lingkup penilaian rIsiko, mendefinisikan batas otorisasi (atau persetujuan), dan menyediakan informasi (contohnya, informasi tentang *Hardware*, *Software*, komunikasi sistem, manajer departemen, atau personel pendukung). [19]. Tabel 5 menunjukkan identifikasi ancaman *(Threat Identification).*

TABEL 5
INDENTIFIKASI ANCAMAN TERHADAP INSTALASI IT

Ancaman Utama	Keterangan	Kode
Bencana Banjir	Kegagalan proses pada sistem, kehilangan data, dan infrastruktur IT yang rusak	a.1- 1
Bencana Gempa	Kegagalan proses pada sistem, kehilangan data, dan infrastruktur IT yang rusak	a.2- 1
Sumber Daya Listrik	*Server down* karena Kehilangan daya listrik	a.3- 1
	Tidak optimalnya tegangan listrik (Kekurangan Daya)	a.3- 2
	AC di ruang instalasi rusak/mati	a.3- 3
	kehilangan daya pada *Modem* dan *Router*	a.3- 4
	Kerusakan sistem dan kehilangan data	a.3- 5
Kebakaran	Kebakaran pada Gedung tempat insfratruktur IT	a.4- 1

Jurnal Manajemen Informatika (JAMIKA)
Volume 12 Nomor 1 Edisi April 2022
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Jaringan Internet	Gangguan jaringan Internet atau terputusnya koneksi	a.5- 1
SDM -Internal	Penyalahgunaan data internal	a.6- 1
	Kesalahan entri data *(Human Error)*	a.6- 2
	Hak akses internal yang disalahgunakan	a.6- 3
SDM - Eksternal	Penyalahgunaan data internal	a.6- 1
	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	a.8- 2
	Server kelebihan kapasitas	a.8- 3
	Pencadangan data yang gagal	a.8- 4
	Pembaruan perangkat lunak gagal	a.8- 5
	Teknologi ketinggalan zaman *(out of date)*	a.8- 6

Selanjutnya ke tahap pembuatan daftar identifikasi kerentanan rIsiko dan sumber ancaman dengan responden, kemudian diskusikan hasil dari identifikasi kerentanan berdasarkan apa yang telah terjadi dilapangan. Tabel 6 menunjukkan hasil pembahasan tentang kerentanan yang muncul ketika ancaman tersebut ada.

Tahap selanjutnya adalah *Control Analysis*, hasil pengamatan terhadap implementasi kontrol analisis yang nantinya akan meminimalisir terjadinya ancaman [20]. Daftar periksa pemindaian dari aturan manajemen baru dan lama yang mencakup jika ada kerentanan dalam instalasi TI kampus XYZ. Misalnya: Pelatihan dan sosialisasi TI dan sistem informasi, manajemen cadangan, pedoman baru tentang prosedur operasi standar (SOP) dalam pengelolaan ancaman dunia maya. Langkah kelima adalah penentuan probabilitas, setelah diketahui hasil analisis risiko yang terpenuhi, hal ini dapat digunakan sebagai acuan untuk menentukan risiko yang mungkin terjadi. Ada 3 kategori tingkatan, yaitu Rendah (0.1), Sedang (0.5), Tinggi (1). Penentuan prediksi kemungkinan ini terdiri dari penentuan tingkat kemungkinan yang terjadi dalam menghadapi risiko yang teridentifikasi.

TABEL 6
INDENTIFIKASI ANCAMAN INSTALASI INSFRASTRUKTUR IT

Ancaman Utama	Keterangan Ancaman	*Threat code*	Kerentanan	Kode Kerentanan
Tenaga Listrik	Server computer Mati Kehilangan daya listrik	a.3- 1	Unit sistem kapasitas terbatas 'UPS'	k1.1
	Gangguan Daya listrik (Kekurangan Daya)	a.3- 2	Adanya kerusakan pada MCB pada pemakaian listrik secara tidak beraturan	k1.2
	AC di ruang instalasi rusak/mati	a.3- 3	Generator/genset tidak segera memulai (respons lambat)	k1.3
	Modem dan Router kehilangan daya	a.3- 4	Tidak ada backup jaringan internet	k1.4
	Sistem rusak dan kehilangan data	a.3- 5	Tidak ada pemulihan data pada sistem.	k1.5
Bencana Kebakaran	Kebakaran pada Gedung Aset Insfratruktur IT	a.4- 1	Kurangnya pelatihan tentang SOP keselamatan Aset pada saat terjadi kebakaran kebakaran	k2.1
Jaringan Internet	Koneksi Internet Terputus	a.5- 1	Tidak ada backup jaringan internet	k3.1
SDM - Internal	Penyalahgunaan data dari pihak internal	a.6- 1	Aturan untuk petugas kurang detail dan lebih mudah dipahami.	k4.1
	Kesalahan entri data *(Human Eror)*	a.6- 2	Kurangnya pelatihan atau distribusi penggunaan data	k4.2
	Hak akses dari pihak internal yang disalahgunakan	a.6- 3	Log akses tidak diperiksa secara teratur.	k4.3

Jurnal JAMIKA Manajemen Informatika
Jurnal Manajemen Informatika (JAMIKA)
Volume 12 Nomor 1 Edisi April 2022
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Ancaman Utama	Keterangan Ancaman	*Threat code*	Kerentanan	Kode Kerentanan
SDM - Eksternal	Kesalahan entri data *(Human Eror)*	a.6- 2	Kurangnya pelatihan atau distribusi penggunaan data	k4.2
	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	a.8- 2	Staf TI menunda pembaruan sistem	k6.2
	Server kelebihan kapasitas	a.8- 3	Tidak ada batasan pada akses orang ke *server database*.	k6.3
	Pencadangan data yang gagal	a.8- 4	Tidak ada jadwal pencadangan *server reguler*	k6.4
	Pembaruan perangkat lunak gagal	a.8- 5	Staf TI menunda pembaruan perangkat lunak	k6.5
	Teknologi ketinggalan zaman *(out of date)*	a.8- 6	Manajemen Kampus Tidak Memiliki Rencana Pengeluaran Teknologi Baru	k6.6

Langkah selanjutnya adalah identifikasi risiko. Tujuan dari tahapan ini, yaitu untuk mengetahui nilai tingkat risiko suatu sistem IT. Identifikasi risiko untuk kerentanan dan ancaman dapat dinyatakan dengan besarnya dampak jika sumber ancaman dapat diperbaiki kerentanan dapat mengurangi atau menghilangkan dari risiko tersebut [21]. Untuk mengukur nilai dari risiko, skala risiko dan matriks risiko disajikan pada Tabel 7. Hasil akhir dari ukuran risiko dilakukan dengan menghitung penilaian yang ditentukan oleh kemungkinan terjadinya ancaman. *(likelihood of the threat)* dan dampak dari ancaman *(impact).*

TABEL 7
MATRIKS TINGKAT RISIKO

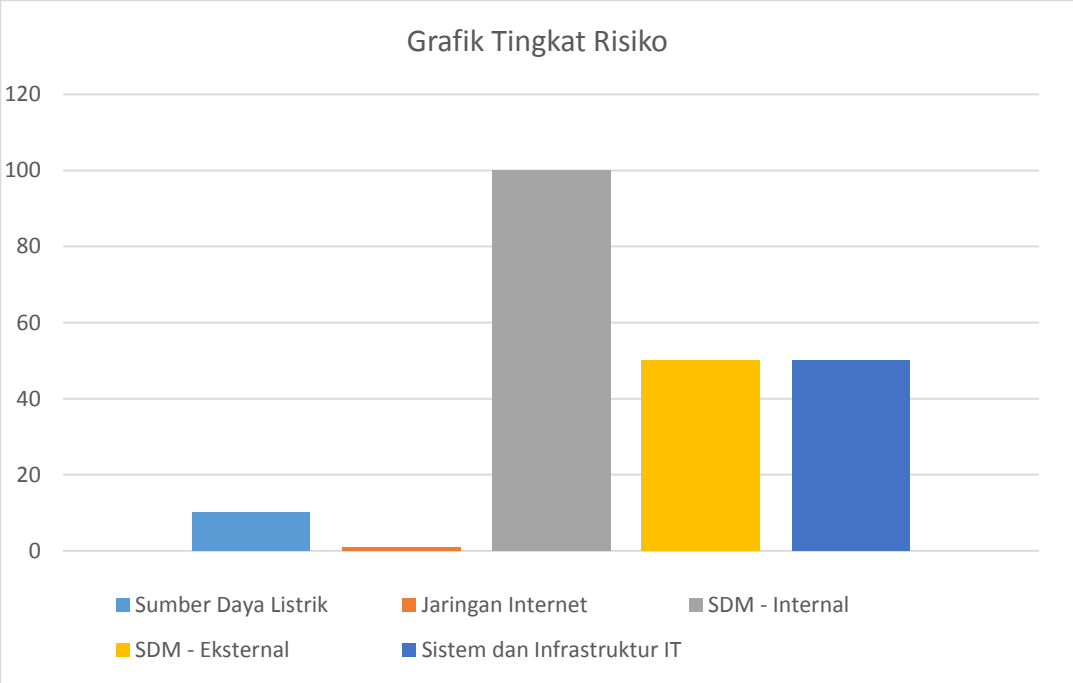
Probabilitas Ancaman	*IMPACT*		
	Low (10)	*Medium (50)*	*High (100)*
High (0. 1)	*Low* 10 × 0. 1 =10	*Medium* 50 × 1. 0 = 50	*High* 100 × 1. 0 = 100
Medium (0. 5)	*Low* 10 × 0. 5 = 5	*Medium* 50 × 0. 5 = 25	*Medium* 50 × 0. 5 = 25
Low (0. 1)	*Low* 10 × 0. 1 = 1	*Low* 50 × 0. 1 = 5	*Low* 100 × 0. 1 =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

Pada tabel 8 dan gambar 2 menunjukan tingkat risiko yang sudah dihitung sebelumnya kemudian didapatkan jenis ancaman yang paling tinggi, sedang dan rendah, dari hasil penentuan risiko ini nantinya akan dibuat pemetaan untuk rekomendasi penanganan yang paling tepat dan akurat untuk ancaman tersebut.

Jurnal Manajemen Informatika (JAMIKA)
Volume 12 Nomor 1 Edisi April 2022
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

TABEL 8
PENENTUAN RISIKO

Jenis Ancaman	Tingkat Probabilitas Ancaman	Nilai Dampak	Nilai Ancaman	Tingkat Ancaman
Sumber Daya 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 - Eksternal	Sedang (0. 5)	Tinggi (100)	50	Sedang
Sistem dan Infrastruktur IT	Sedang (0.5)	Tinggi (100)	50	Sedang



Gambar 2. Grafik Tingkat Risiko

Pengklasifikasian risiko ini bertujuan untuk tingkat risiko yang dinilai pada suatu sistem dengan mengacu pada kemungkinan dan dampak risiko yan terindetifikasi dalam hal mengevaluasi tingkat risiko tersebut. Tabel 9 dapat dilihat Identifikasi Risiko yang didefinisikan dalam Rekomendasi Kontrol *(Control Recommendations)* Berdasarkan langkah-langkah sebelumnya, kontrol pada langkah ini dapat mengurangi atau menghilangkan risiko yang teridentifikasi, tergantung pada keinginan IT. Kontrol yang direkomendasikan selama implementasi bertujuan mengurangi risiko kehilangan ataupun kerusakan terhadap sistem IT dan datanya, yang nantinya bisa sampai ke tingkat yang bisa diproses, seperti yang ditunjukkan pada Tabel 9.

TABEL 9
KONTROL YANG DIREKOMENDASIKAN

Jenis Ancaman	Tingkat Ancaman	Rekomendasi
Sumber Daya Listrik	Rendah	Meminta Unit UPS Tambahan di Bagian *Server* Generator siap untuk respons yang lebih cepat Periksa tanggal servis AC Anda secara berkala. Beli VSAT Untuk cadangan sbumber daya bagi internet Cadangan Data Diperbarui dengan menejemen yang baik
Jaringan Internet	Rendah	Konfigurasi backup Jaringan
SDM - Internal	Tinggi	Regulasi SDM semakin disosialisasikan.

SDM - Eksternal	Sedang	Jadwalkan pemeriksaan log berkala tambahan Pelatihan keterampilan dan sosialisasi staf Pembaruan Sistem Keamanan Pengawasan cctv Mengirim data ke *server cloud* lebih cepat dan terjamin keamanan data Keamanan Server yang Ditingkatkan
Sistem dan Infrastruktur IT	Sedang	Jadwalkan restart sistem secara berkala Siapkan Cadangan *server host/cloud* Memberi Batasan orang yang bisa akses Manajemen Cadangan data Persiapan pencadangan perangkat lunak Membuat pengajuan pembelian perangkat keras baru ke pihak Kampus

IV. KESIMPULAN

Penilaian risiko IT di fasilitas IT Kampus XYZ di Kota Pagar Alam, yang mengacu pada dua metode analisis risiko kuantitatif dan analisis risiko kualitatif, memberikan hasil tambahan. Penilaian risiko IT menggunakan analisis risiko kuantitatif. Aset IT dengan total aset melebihi KRW 50 juta, yaitu *server, router*, dan *prosesor*, sehingga proses manajemen risiko IT terfokus pada tiga jenis aset IT. Ancaman dengan total nilai aset melebihi Rp. 50 juta termasuk hilangnya daya listrik *(power loss)*, hilangnya jaringan *(network loss)*, terjadi bencana alam, aset insfratruktur IT yang hilang dicuri, dan pelanggaran hak akses. Hasil dari analisis risiko kualitatif, ditemukan bahwa tingkat risiko yang tinggi adalah SDM Internal (Sumber Daya Manusia Internal), dan tingkat risiko rata-rata adalah SDM – Eksternal (sumber daya manusia eksternal) dan sistem dan infrastruktur IT. Ini memberikan pedoman manajemen risiko IT untuk karyawan internal dan eksternal serta aset IT, sistem dan infrastruktur IT. Keamanan dan pemeliharaan aset IT, sistem dan infrastruktur IT harus dilakukan dan didokumentasikan secara teratur. Manajemen kampus XYZ yang berada di Kota Pagar Alam harus lebih memperhatikan staf internalnya dan memastikan investasi jangka panjang dalam bentuk pelatihan berdasarkan keterampilan prioritas yang dibutuhkan.

UCAPAN TERIMA KASIH

Terima kasih kepada kedua orang tua saya yang selalu memberikan motivasi yang tidak saya dapatkan dari manusia lain, Terima kasih kepada ITPA (Institut Teknologi Pagar Alam) yang telah mendukung penelitian ini baik dari segi moril dan materil.

DAFTAR PUSTAKA

[1] 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.

[2] F. Febrianty *et al.*, *Manajemen Perubahan Perusahaan Di Era Transformasi Digital*. Yayasan Kita Menulis, 2020.

[3] 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.

[4] 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.

[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, 2018.

[6] B. Muslim, "Analisis Sistem Informasi (SI) Terintegrasi di Perguruan Tinggi (PT)(Studi Kasus: STT Pagar Alam)," *J. Teknol. Inf. MURA*, vol. 10, no. 2, pp. 83–91, 2018.

[7] 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.

[8] S. Susilo, "Analisa Tingkat Risiko 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, 2019.
[9] J. Simarmata *et al.*, *Teknologi Informasi: Aplikasi dan Penerapannya*. Yayasan Kita Menulis, 2020.
[10] H. C. Chotimah, "Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]," *J. Polit. Din. Masal. Polit. Dalam Negeri dan Hub. Int.*, vol. 10, no. 2, pp. 113–128, 2019.
[11] A. Elanda and R. L. Buana, "Analisis Manajemen Risiko 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.
[12] B. Muslim, "Quantitative Risk Analysis of Asset Information Technology at STT Pagaralam," *Pros. STTA Yogyakarta (Senatik 2018), STTA*, pp. 501–509, 2018.
[13] L. Maulida, "Analisis risiko aset teknologi informasi menggunakan metode quantitative risk analys (QRA)." UIN Sunan Ampel Surabaya, 2021.
[14] J. Jonny and C. Darujati, "Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005," *Sist. J. Sist. Inf.*, vol. 10, no. 1, pp. 1–12, 2021.
[15] S. O. D. Ningsih and S. W. Hati, "Analisis Risiko 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.
[16] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," *J. Inform. J. Pengemb. IT*, vol. 2, no. 2, pp. 1–8, 2020.
[17] A. G. R. Padang, A. Ambarwati, and E. Setiawan, "Penilaian Manajemen Risiko TI Menggunakan Quantitative dan Qualitative Risk Analysis," *Sist. J. Sist. Inf.*, vol. 10, no. 3, pp. 527–537, 2021.
[18] M. A. Dewi, A. Ambarwati, And C. Darujati, "Analisis Risiko 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.
[19] K. Ahdieh Sadat, "An enhanced risk identification and assessment model to improve software risk management/Ahdieh Sadat Khatavakhotan." University of Malaya, 2021.
[20] B. L. Mahersmi, F. A. Muqtadiroh, and B. C. Hidayanto, "Analisis Risiko Keamanan Informasi Dengan Menggunakan Metode Octave Dan Kontrol Iso 27001 Pada Dishubkominfo Kabupaten Tulungagung," *SESINDO 2020*, vol. 2020, 2020.
[21] 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, 2019.