Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

EVALUASI MANAJEMEN RISIKO TEKNOLOGI INFORMASI BERDASARKAN FRAMEWORK NIST SP 800-30 REV.1

Yudha Yudistira[1], Andi Sofyan Anas[2], Khairan Marzuki[3]

[1,]Program Studi Teknologi Informasi, Universitas Bumigora, [23,]Program Studi Ilmu Komputer, Universitas Bumigora

Jln. Basuki Rahmat No.105 Praya Lombok Tengah 83511
[1] 2001020034@universitasbumigora.ac.id, [2] andi.sofyan@universitasbumigora.ac.id, [3] khairan.marzuki@universitasbumigora.ac.id

Abstract

The rapid advancement of information technology has brought numerous benefits to companies in enhancing operational efficiency, service quality, and data-driven decision-making. However, behind these advantages lie risks that may disrupt business continuity if not properly managed. Therefore, information technology risk management has become a crucial aspect that must be implemented systematically. This study was conducted at PT Air Minum Giri Menang to evaluate how IT risk management practices are carried out within the organization. The NIST SP 800-30 framework was employed as the primary approach to identify information assets, analyze potential threats, assess vulnerabilities, and determine the impact and likelihood of possible risks. The results of this study indicate that most risks fall into the medium category, with the most prominent threats arising from brute force attacks and human error. These findings serve as an important foundation for planning more effective and structured risk mitigation actions in the future.

Keywords : *Risk Management, Information Technologies, NIST SP 800-30*

Abstrak

Perkembangan teknologi informasi yang pesat memberikan banyak manfaat bagi perusahaan dalam meningkatkan efisiensi operasional, kualitas layanan, serta pengambilan keputusan berbasis data. Namun, di balik berbagai manfaat tersebut, terdapat risiko yang dapat mengganggu kelangsungan bisnis apabila tidak dikelola dengan baik. Oleh karena itu, manajemen risiko teknologi informasi menjadi aspek krusial yang harus diterapkan secara sistematis. Penelitian ini dilakukan di PT Air Minum Giri Menang untuk mengevaluasi bagaimana praktik manajemen risiko TI dijalankan di lingkungan perusahaan. Framework NIST SP 800-30 digunakan sebagai pendekatan utama dalam mengidentifikasi aset informasi, menganalisis potensi ancaman, mengevaluasi kerentanan, serta menilai dampak dan kemungkinan risiko yang dapat terjadi. Hasil dari penelitian ini menunjukkan bahwa sebagian besar risiko berada pada tingkat sedang (*medium*), dengan jenis ancaman yang paling menonjol berasal dari brute force attack dan kesalahan manusia (*human error*). Temuan ini menjadi dasar penting dalam perencanaan tindakan mitigasi risiko yang lebih efektif dan terstruktur ke depannya.

Kata kunci : *Manajemen Risiko, Teknologi Informasi, NIST SP 800-30*

1. PENDAHULUAN

Teknologi Informasi merupakan seperangkat alat dan sistem yang digunakan untuk mengelola data, termasuk dalam hal pengolahan, penyusunan, serta penyimpanan informasi agar dapat dimanfaatkan secara

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

optimal[1]. Informasi yang dihasilkan harus memiliki nilai penting, akurat, dan tersedia tepat waktu, sehingga teknologi ini memiliki penerapan yang luas, mencakup kehidupan sehari-hari, aktivitas bisnis, hingga sektor pemerintahan. Kemajuan teknologi informasi telah membawa pengaruh yang besar terhadap perkembangan peradaban modern[2]. Bidang-bidang seperti pendidikan, ekonomi, kesehatan, pemerintahan, dan budaya turut mengalami transformasi sebagai akibat dari kemajuan ini. Teknologi diciptakan untuk mempermudah kehidupan manusia yang dimana saat ini, teknologi informasi telah melebur menjadi elemen yang tak terpisahkan dari berbagai aktivitas rutin manusia[3].

Manajemen risiko dalam sebuah organisasi bertujuan untuk membantu dalam mengidentifikasi dan mengelola risiko yang mungkin timbul, agar proses bisnis dapat berjalan lancar dan menguntungkan[4].Ini dilakukan dengan cara mengidentifikasi potensi risiko, menilai dampaknya, mengendalikan, dan mengatasi risiko tersebut untuk meminimalkan kemungkinan terjadinya gangguan atau kerugian pada operasi organisasi[5].

PT Air Minum Giri Menang adalah entitas usaha yang berada di bawah kepemilikan pemerintah daerah bertanggung jawab menyediakan air bersih untuk masyarakat di wilayah Giri Menang. Keberadaan perusahaan ini sangat penting bagi masyarakat setempat dalam memenuhi kebutuhan air bersih. Pada bulan Juli 2020, jumlah pelanggan PT Air Minum Giri Menang tercatat sekitar 150.065 orang, yang menunjukkan adanya peningkatan signifikan. Dengan meningkatnya jumlah pelanggan, PT Air Minum Giri Menang perlu terus meningkatkan dan menjaga kualitas layanan yang diberikan.

Sebagai upaya untuk meningkatkan pelayanan kepada pelanggan, PT Air Minum Giri Menang meluncurkan aplikasi berbasis internet yang memudahkan pelanggan dalam mengakses berbagai informasi tentang perusahaan. Aplikasi ini, yang diberi nama PEPADU (Pelayanan PT Air Minum Giri Menang Terpadu), menyediakan beberapa fitur seperti informasi terkait pembayaran, pelaporan penggunaan meter, dan penanganan keluhan pelanggan, pemasangan baru, pembayaran tagihan, dan laporan pelanggan. Meskipun demikian, tidak bisa dipastikan bahwa sistem ini bebas dari risiko atau anomali yang dapat merusak atau mengganggu fungsinya, sehingga dapat memengaruhi performa sistem secara keseluruhan.

Untuk menjalankan aktivitas bisnis secara optimal dan meningkatkan layanan kepada pelanggan, PT Air Minum Giri Menang harus memastikan bahwa layanan teknologi informasi yang dikelola dapat memenuhi kebutuhan bisnis secara efisien. Ini melibatkan penyesuaian antara manajemen sumber daya TI dengan kebutuhan pelanggan, sehingga layanan yang diberikan sesuai dengan ekspektasi dan meningkatkan kepuasan pelanggan. PT Air Minum Giri Menang juga mengelola data pelanggan yang sangat penting, seperti data pribadi, informasi penggunaan air, dan rincian pembayaran. Kehilangan atau kebocoran data ini bisa merusak reputasi perusahaan serta menurunkan tingkat kepercayaan pelanggan. Dalam hal ini, NIST SP 800-30 dapat digunakan untuk mengkaji dan mengukur potensi risiko terhadap sistem yang dianalisis guna mengidentifikasi kerentanannya. Dengan demikian, diperlukan evaluasi risiko secara menyeluruh untuk mengidentifikasi serta mengantisipasi ancaman dan potensi kerugian yang mungkin terjadi di dalam sistem agar perusahaan dapat mengambil langkah pencegahan, penanganan, serta perbaikan yang tepat.

2. TINJAUAN PUSTAKA

2.1. Definisi Evaluasi

Evaluasi merupakan suatu proses yang digunakan untuk membagi masalah diuraikan ke dalam komponen-komponen yang lebih spesifik (dekomposisi) dengan tujuan untuk memberikan solusi yang lebih mudah dipahami terkait masalah tersebut[6]. Sedangkan Evaluasi data adalah proses pengumpulan dan pengorganisasian data dari berbagai sumber, seperti dokumen, wawancara, dan lainnya, secara sistematis. Dengan cara ini, data dapat diatur dengan baik, informasi penting dapat ditemukan dan dipelajari, serta kesimpulan dapat ditarik yang akan memudahkan peneliti dan pihak lain dalam memahaminya[7].

2.2. Teknologi Informasi

Teknologi informasi adalah alat utama dalam mengelola data agar dapat diubah menjadi informasi yang bermakna, dan berbagai fungsi lainnya, yang memiliki dampak besar pada masyarakat[8]. Dampak yang ditimbulkan bisa

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

bersifat positif maupun negatif, tergantung pada cara penggunaannya dan respons dari masyarakat di sekitar[9]. Perkembangan teknologi informasi berawal dari kemajuan dalam bidang komputerisasi. Pada awalnya, komputer hanya berfungsi dalam pembuatan dokumen, grafik, ilustrasi, sekaligus penyimpanan data[10]. Komputer pun berkembang dari sekadar alat pengolah data menjadi perangkat komunikasi yang terhubung dengan jaringan global seiring waktu. Perkembangan ini dipengaruhi oleh kebutuhan manusia untuk berkomunikasi, mengingat bahwa interaksi sosial adalah bagian alami dari kehidupan manusia. Kemajuan teknologi memungkinkan komunikasi dapat menjangkau berbagai kelompok masyarakat di seluruh dunia. Internet, menjadi media yang merupakan hasil dari perkembangan teknologi, selain sebagai alat pengenalan budaya daerah lain, teknologi juga mengalami perkembangan yang pesat dalam berbagai aspek. Pesatnya kemajuan teknologi informasi dan komunikasi telah memberikan pengaruh yang signifikan terhadap budaya serta lingkungan sosial masyarakat, baik dalam bentuk manfaat maupun tantangan. Salah satu dampak yang terlihat adalah pergeseran budaya dan lingkungan masyarakat yang terjadi seiring dengan perkembangan tersebut[11].

2.3. Manajemen Risiko Teknologi Informasi

Risiko adalah kemungkinan suatu peristiwa di masa depan yang dapat menyebabkan kerugian.[12]. Manajemen risiko adalah serangkaian kegiatan yang terkoordinasi untuk mengidentifikasi, menilai, dan mengelola risiko yang dihadapi oleh organisasi. Tujuan dari prosedur manajemen risiko adalah untuk mengelola dan mengoptimalkan risiko tersebut, sehingga organisasi atau perusahaan dapat meminimalkan kerugian dan memaksimalkan peluang yang ada[13].

Manajemen risiko teknologi informasi merupakan suatu proses yang mencakup kegiatan identifikasi, analisis, serta pengendalian terhadap risiko-risiko yang terkait dengan sistem informasi dan teknologi dalam operasi bisnis[14]. Proses ini bertujuan untuk mengurangi atau menghilangkan risiko yang dapat mengancam kelancaran operasional organisasi. Aktivitas dalam manajemen risiko TI mencakup identifikasi informasi yang perlu dilindungi, penilaian risiko yang ada, identifikasi kelemahan atau anomali dalam sistem, analisis dampak terhadap bisnis, serta penilaian terhadap tingkat risiko yang dapat diterima[15].

2.4. National Institute of Standart and Technology (NIST) SP 800-30

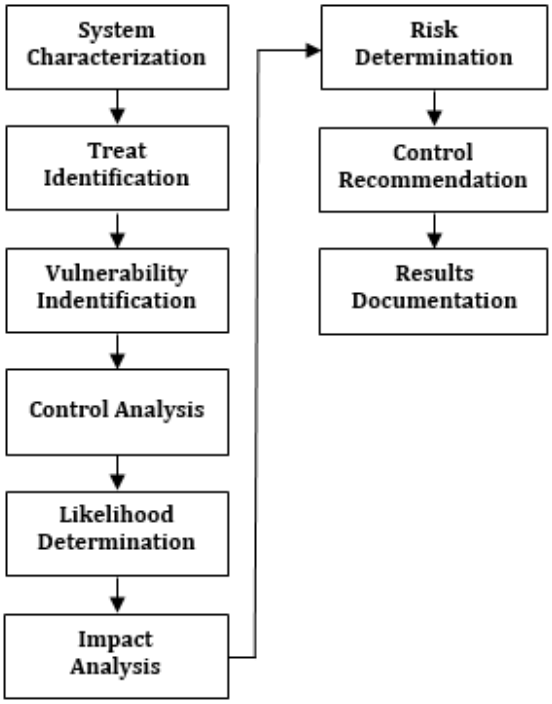
NIST SP 800-30 merupakan salah satu publikasi standar yang diterbitkan oleh *National Institute of Standards and Technology* (NIST). Standar ini merupakan bagian dari implementasi tanggung jawab hukum yang diatur oleh Undang-Undang Keamanan Data tahun 1987 dan Undang-Undang Reformasi Manajemen Teknologi Informasi tahun 1996. NIST menyusun publikasi khusus bernomor 800-30, yang dikenal dengan *Risk Management Guide for Information Technology Systems*, yang mencakup tiga langkah utama dalam manajemen risiko: penilaian risiko, mitigasi risiko, dan evaluasi risiko[16].

Menurut (Putro, 2021), NIST menyarankan pendekatan sistematis untuk mengidentifikasi, menilai, dan mengurangi potensi ancaman yang dapat merugikan sistem informasi[17]. Penilaian risiko, mitigasi risiko, dan evaluasi risiko merupakan tahapan yang saling terkait, yang bertujuan untuk memberikan panduan komprehensif mengenai bagaimana cara menilai tingkat risiko yang dihadapi, mengurangi kemungkinan terjadinya kerusakan, serta mengevaluasi efektivitas langkah mitigasi yang telah diambil. Proses-proses ini berfokus pada penyusunan rekomendasi yang dapat membantu organisasi dalam memitigasi potensi risiko yang mungkin timbul dalam operasional sistem informasi yang mereka kelola[18].

3. METODOLOGI PENELITIAN

Tahapan yang ada dalam NIST SP 800-30 Rev.1 dapat ditemukan pada Gambar 1 berikut ini.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi



Gambar 1. *Risk Assesment Flowchart*

3.1. System Characterization

Tahapan ini dilakukan dengan meninjau berbagai aspek teknis yang membentuk sistem informasi secara keseluruhan, termasuk di dalamnya perangkat keras (*hardware*), perangkat lunak (*software*), antarmuka pengguna (*interface*), struktur dan isi data yang digunakan, serta karakteristik jaringan yang menghubungkan sistem. Semua komponen ini dianalisis untuk mengidentifikasi potensi kerentanan dan ancaman yang dapat berdampak pada keamanan serta keandalan sistem informasi.

3.2. Treat Identification

Tahapan ini berfokus pada identifikasi berbagai sumber potensial yang dapat menimbulkan gangguan terhadap sistem. Dalam proses ini, dilakukan pengenalan terhadap jenis-jenis ancaman yang mungkin terjadi, baik yang berasal dari faktor internal maupun eksternal, dengan tujuan untuk memahami sejauh mana ancaman tersebut dapat memengaruhi keamanan dan keberlangsungan operasional sistem informasi.

3.3. Vulnerability Identification

Pada tahapan ini, dilakukan proses identifikasi terhadap berbagai kelemahan atau kekurangan yang ada dalam sistem, baik dari sisi teknis maupun non-teknis. Kelemahan-kelemahan tersebut dapat menjadi celah yang memungkinkan terjadinya gangguan atau serangan terhadap sistem. Dengan mengetahui titik-titik lemah ini sejak awal, organisasi dapat lebih siap dalam mengantisipasi dan mengelola risiko yang mungkin timbul, sehingga sistem dapat berjalan dengan lebih aman dan andal.

3.4. Control Analysis

Tahap ini memiliki tujuan utama untuk mengevaluasi dan menganalisis berbagai kontrol atau mekanisme pengamanan yang sudah diterapkan maupun yang direncanakan akan diterapkan dalam sistem. Analisis ini dilakukan guna mengetahui sejauh mana efektivitas kontrol tersebut dalam mengurangi atau meminimalkan kemungkinan terjadinya ancaman yang dapat mengganggu kinerja dan keamanan sistem informasi. Dengan memahami peran masing-masing kontrol, organisasi dapat menentukan langkah-langkah penguatan yang lebih tepat dan strategis.

3.5. Likelihood Determination

Pada tahapan ini, dilakukan penilaian terhadap kemungkinan suatu kelemahan dalam sistem dimanfaatkan oleh pihak yang mengancam. Tujuannya adalah untuk mengukur tingkat kecenderungan terjadinya insiden yang dapat berdampak pada sistem informasi. Hasil dari proses ini menjadi dasar penting dalam menentukan prioritas penanganan terhadap risiko yang telah teridentifikasi.

3.6. Impact Analysis

Pada tahapan ini, dilakukan penilaian terhadap besarnya dampak yang mungkin ditimbulkan apabila suatu ancaman benar-benar terjadi dan berhasil mengeksploitasi kelemahan sistem. Penilaian dampak ini dilakukan berdasarkan hasil analisis kemungkinan risiko yang telah diidentifikasi sebelumnya. Tujuannya adalah untuk memahami sejauh mana gangguan tersebut dapat memengaruhi keberlangsungan operasional sistem informasi, termasuk potensi kerugian terhadap aset, layanan, maupun reputasi organisasi.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

3.7. Risk Determination

Pada tahapan ini, dilakukan penentuan tingkat risiko secara menyeluruh terhadap sistem informasi dengan mengacu pada dua aspek utama, yaitu kemungkinan terjadinya risiko (*likelihood determination*) dan besarnya dampak yang dapat ditimbulkan (*impact analysis*). Tujuan dari proses ini adalah untuk menghasilkan nilai risiko yang dapat digunakan sebagai dasar dalam menetapkan prioritas penanganan serta strategi mitigasi yang sesuai. Dengan menilai kedua komponen tersebut secara bersamaan, organisasi dapat memperoleh pemahaman yang lebih jelas mengenai risiko mana yang paling mendesak untuk ditangani guna menjaga keamanan dan keberlangsungan sistem. Untuk sistem penilaian risiko dapat dilihat pada tabel berikut ini.

Tabel 1. Rumus Penilaian Risiko

Nilai Kemungkinan	Analisa Dampak		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low (10)	Medium (50)	High (100)
Medium (0.5)	Low (0.5)	Medium (25)	Medium (50)
Low (0.1)	Low (0.1)	Low (5)	Low (10)

3.8. Control Recommendation

Tujuan dari rekomendasi kontrol adalah untuk memberikan hasil dari proses penilaian risiko yang telah dilakukan, serta memberikan masukan yang berguna untuk langkah-langkah mitigasi risiko selanjutnya. Pada tahap ini, kontrol keamanan, baik yang bersifat teknis maupun prosedural, yang telah direkomendasikan akan dievaluasi secara cermat, diprioritaskan berdasarkan tingkat urgensinya, dan kemudian diimplementasikan untuk mengurangi potensi risiko yang dapat mengancam sistem. Proses ini memastikan bahwa langkah-langkah pengamanan yang diterapkan efektif dan sesuai dengan kebutuhan untuk melindungi sistem informasi dari ancaman yang teridentifikasi.

3.9. Result Documentation

Tahapan ini berfokus pada dokumentasi atau penyusunan laporan yang mencakup seluruh rangkaian kegiatan yang telah dilakukan, mulai dari tahap identifikasi karakteristik sistem hingga rekomendasi kontrol yang diberikan. Proses ini bertujuan untuk menyusun catatan yang komprehensif dan terperinci, yang dapat digunakan sebagai referensi atau dasar untuk pengambilan keputusan lebih lanjut terkait manajemen risiko dan upaya mitigasi yang perlu dilakukan.

4. HASIL DAN PEMBAHASAN

Bagian ini membahas hasil analisis serta uraian mengenai langkah-langkah yang dilakukan selama proses penilaian risiko keamanan informasi menerapkan metode framework NIST SP 800-30. Penilaian ini diterapkan pada lingkungan operasional PT Air Minum Giri Menang (PTAM) di Mataram. Setiap tahapan dijelaskan secara rinci untuk memberikan gambaran menyeluruh tentang bagaimana proses manajemen risiko dijalankan dalam organisasi tersebut.

4.1. System Characterization

Berdasarkan hasil wawancara dengan Asisten Manajer Perangkat Keras dan Jaringan di PT Air Minum Giri Menang, sistem yang dimiliki oleh instansi ini terdiri atas empat jenis aset utama, termasuk hardware, software, informasi, dan sumber daya manusia. Aset-aset dalam kategori perangkat keras mencakup komputer, server, dan UPS. Untuk perangkat lunak, yang termasuk di dalamnya adalah sistem operasi seperti Windows dan Ubuntu, serta aplikasi layanan pelanggan bernama PEPADU. Sementara itu, aset informasi meliputi data pelanggan, yang rinciannya disajikan dalam Tabel 1 di bawah ini.

Tabel 2. System Characterization

No	Kelompok	Aset	Keterangan
1	Informasi	Data Informasi Pelanggan	Informasi pribadi pelanggan meliputi nama, alamat, dan kontak.
		Data Informasi Pegawai	Informasi pribadi karyawan meliputi nama, jabatan, dan ID.
2	Perangkat Keras	Server	Digunakan untuk pengelolaan serta penyimpanan data, termasuk email, berkas, dan aplikasi.
		Komputer	Perangkat yang

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

			berfungsi untuk membuka data, menyusun dokumen, serta menjalankan berbagai aplikasi.
		Access Point	Perangkat Wi-Fi yang memungkinkan koneksi perangkat lain ke jaringan.
		UPS	Sumber daya listrik cadangan yang menjaga perangkat tetap beroperasi saat terjadi pemadaman listrik.
3	Perangkat Lunak	Windows	Sistem operasi komputer yang banyak digunakan untuk menjalankan aplikasi dan mengelola berkas.
		Ubuntu	Sistem operasi komputer yang bersifat open-source dan dapat digunakan secara gratis.
		Aplikasi PEPADU	Aplikasi yang dikembangkan oleh PT Air Minum Giri Menang untuk memudahkan pelanggan dalam melakukan permintaan pasang baru, cek tagihan, pengaduan, dan layanan lainnya.
		Microsoft Office	Perangkat lunak pengolah dokumen yang banyak digunakan, seperti Word, Excel, dan PowerPoint.
4	Manusia	Karyawan	Karyawan di PT Air Minum Giri Menang yang memiliki peran dan tanggung jawab spesifik.

4.2. Treat Identification

Sebelum melakukan penilaian risiko, perlu dilakukan identifikasi terhadap ancaman yang berpotensi mengganggu keamanan aset informasi Sistem PT Air Minum Giri Menang. Ancaman ini bisa berasal dari faktor internal maupun eksternal, seperti bencana alam, kerusakan fasilitas, masalah sosial, dan masalah operasional. Interval nilai tertentu digunakan untuk menilai.

Daftar ancaman dan kelemahan diperoleh melalui wawancara dengan Manajer IT, khususnya terkait software dan jaringan. Rinciannya disajikan pada Tabel 2 berikut ini.

Tabel 3. Treat Identification

No	Sumber Ancaman	Motivasi	Keterangan
1	Virus	Ketidak sengajaan, dan ingin merusak software (*ego*).	Kerusakan pada fungsi perangkat lunak yang diakibatkan oleh virus komputer.
2	SQL Injection	Ketidak sengajaan, dan rasa ingin tahu.	Penyerangan dengan menyisipkan perintah SQL berbahaya ke dalam sistem yang memiliki celah keamanan.
3	Brute Force	Rasa ingin tahu, masuk ke sistem secara ilegal, dan merubah atau mencuri data.	Serangan yang mencoba menebak kunci sistem keamanan dengan cara mencoba setiap kemungkinan untuk mendapatkan akses.
4	Bencana Alam		Bencana alam yang berisiko merusak aset, seperti gempa, banjir, petir, atau angin kencang.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

5	Kebakaran	Ketidak sengajaan, dan merusak aset.	Kebakaran akibat konsleting listrik atau tindakan individu yang sengaja merusak aset.
6	Human Error	Ketidak sengajaan	Masih banyak karyawan yang tidak memiliki pemahaman atau pengetahuan terkait teknologi informasi.

4.3. Vulnerability Identification

Identifikasi kerentanan pada Sistem PT Air Minum Giri Menang dilakukan dengan menganalisis kelemahan sistem informasi berdasarkan sumber-sumber ancaman yang ada secara daring, serta potensi yang mungkin terjadi di masa mendatang. Hasil analisis ditampilkan pada Tabel 3 berikut ini.

Tabel 4. Vulnerability Identification

No	Sumber Ancaman	Aset yang terdampak	Kerentanan
1	Virus	Komputer, server, dan software	Penggunaan media penyimpanan eksternal (*flashdisk*) tanpa pengendalian.
			Antivirus jarang diperbarui dan digunakan, sehingga meningkatkan risiko keamanan.
			Melakukan unduhan file dari sumber yang tidak terpercaya.
2	SQL Injection	Server, dan software.	Input validasi yang lemah saat penetration test.
			Kesalahan dalam proses pengujian penetrasi sistem.
3	Brute Force	Data informasi pelanggan, data informasi pegawai, server, dan software.	Absennya sistem pemantauan terhadap aktivitas login yang mencurigakan.
			Belum diterapkannya mekanisme autentikasi multi-faktor (*MFA*).
4	Kebakaran	Semua aset	Terjadinya hubungan pendek arus listrik (*korsleting*).
			Kemungkinan terkena sambaran petir (bencana alam).
5	Human Error	Karyawan	Rendahnya kesadaran akan keamanan.
			Manajemen yang kurang konsisten dalam menerapkan disiplin.
			Kurangnya keterampilan dan pengalaman yang diperlukan.

4.4. Control Analysis

Pada tahap ini, tujuan yang dicapai adalah mengidentifikasi langkah-langkah pengendalian yang diterapkan terhadap risiko yang telah diidentifikasi pada tahap sebelumnya. Setiap aset memiliki potensi ancaman yang perlu dikelola, dan setiap ancaman tersebut akan ditangani dengan langkah-langkah pengendalian yang sesuai. Untuk penjelasan lebih rinci, berikut adalah penanganan potensi ancaman pada sistem PT Air Minum Giri Menang yang dapat dilihat pada Tabel 4 berikut ini.

Tabel 5. Control Analysis

No	Sumber Ancaman	Kerentanan	Penerapan kontrol
1	SQL Injection	Input validasi yang lemah saat	Dilakukan maintenance.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

		penetration test.	
		Kesalahan dalam proses pengujian penetrasi sistem.	Dilakukan maintenance.
2	Brute Force	Absennya sistem pemantauan terhadap aktivitas login yang mencurigakan.	Pemberitahuan melalui email ketika terdeteksi adanya serangan pada sistem.
		Belum diterapkannya mekanisme autentikasi multi-faktor (*MFA*).	Sistem otomatis yang memblokir IP setelah beberapa kali percobaan akses yang gagal.
3	Human Error	Rendahnya kesadaran akan keamanan.	Mulai menerapkan dokumentasi manajemen risiko
		Manajemen yang kurang konsisten dalam menerapkan disiplin.	Pemberian teguran terhadap kesalahan yang dianggap serius dalam operasional.
		Kurangnya keterampilan dan pengalaman yang diperlukan.	Menyediakan panduan atau orientasi singkat untuk pegawai baru yang masuk ke dalam organisasi.

4.5. Likelihood Determnination

Tahapan *Likelihood Determination* (LD) ini bertujuan untuk mengevaluasi sejauh mana kelemahan dapat dimanfaatkan dalam menciptakan ancaman, serta sejauh mana sumber ancaman dapat mendeteksi kelemahan tersebut. Hasil evaluasi ini kemudian dikelompokkan dalam tingkat tinggi, menengah, atau rendah, seperti yang tercantum dalam tabel 5 di bawah ini.

Tabel 6. Likelihood Determination (LD)

No	Sumber Ancaman	ID LD	Kerentanan	Tingkat LD
1	Virus	LDV-01	Penggunaan media penyimpanan eksternal (*flashdisk*) tanpa pengendalian.	Medium
		LDV-02	Antivirus jarang diperbarui dan digunakan, sehingga meningkatkan risiko keamanan.	High
		LDV-03	Melakukan unduhan file dari sumber yang tidak terpercaya.	Low
2	SQL Injection	LDS-01	Input validasi yang lemah saat penetration test.	Medium
		LDS-02	Kesalahan dalam proses pengujian penetrasi sistem.	low
3	Brute Force	LDB-01	Absennya sistem pemantauan terhadap aktivitas login yang mencurigakan.	Low
		LDB-02	Belum diterapkannya mekanisme autentikasi multi-faktor (*MFA*).	Medium
4	Kebakaran	LDK-01	Terjadinya hubungan pendek arus listrik (*korsleting*).	Low
		LDK-02	Kemungkinan terkena sambaran petir (bencana alam).	Low
5	Human Error	LDH-01	Rendahnya kesadaran akan keamanan.	Medium
		LDH-02	Manajemen yang kurang konsisten dalam menerapkan disiplin.	Medium
		LDH-03	Kurangnya keterampilan dan pengalaman yang	Medium

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

			diperlukan.	

4.6. Impact Analysis

Langkah selanjutnya, *Impact Analysis* (IA) diperuntukkan dalam menilai tingkat risiko adalah menentukan sejauh mana dampak yang dapat ditimbulkan oleh ancaman terhadap kelemahan tersebut, yang dapat dilihat pada tabel 6 di bawah ini.

Tabel 7. Impact Analysis

No	Sumber Ancaman	ID IA	Dampak	Tingkat IA
1	Virus	IAV-01	Kehilangan aset atau data yang bersifat vital.	Medium
		IAV-02	Akses terhadap perangkat lunak menjadi tidak tersedia.	High
		IAV-03	Kerusakan atau kehilangan informasi yang penting.	Medium
2	SQL Injection	IAS-01	Masuknya data asing atau tidak valid ke dalam sistem.	Medium
		IAS-02	Sistem mengalami gangguan sehingga tidak dapat dioperasikan.	High
3	Brute Force	IAB-01	Data dapat dimodifikasi atau dihapus oleh pihak yang tidak berwenang.	High
		IAB-02	Kehilangan hak akses terhadap sistem informasi.	High
4	Kebakaran	IAK-01	Kerusakan media penyimpanan dan hilangnya informasi yang tersimpan.	High
		IAK-02	Kerusakan pada perangkat keras serta infrastruktur pendukung lainnya.	High
5	Human Error	IAH-01	Laporan yang dihasilkan menjadi tidak akurat atau tidak sesuai.	Medium
		IAH-02	Keputusan bisnis yang diambil menjadi kurang tepat karena informasi yang keliru.	Medium
		IAH-03	Gangguan dalam proses operasional perusahaan.	Medium

4.7. Risk Determination

Tahapan ini bertujuan untuk menilai tingkat risiko terhadap sistem informasi di PT Air Minum Giri Menang. Penentuan risiko didasarkan pada kemungkinan ancaman yang ada, untuk menilai dampaknya terhadap sistem informasi. Dampak yang menyerang suatu sistem dalam instansi perlu diminimalisir atau dicegah segera mungkin agar risiko tidak berkembang menjadi besar dan merugikan instansi. Selain itu, langkah pencegahan juga perlu dilakukan agar risiko serupa tidak terulang, yang dapat dilihat pada tabel 7 di bawah ini.

Tabel 8. Risk Determination

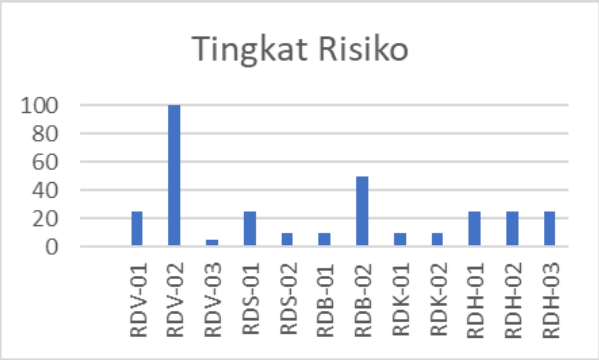
No	Sumber Ancaman	ID RD	ID LD	ID IA	Tingkat LD	Tingkat IA	Tingkat Risiko
1	Virus	RDV-01	LDV-01	IAV-01	Medium (0.5)	Medium (50)	Medium (25)
		RDV-02	LDV-02	IAV-02	High (1.0)	High (100)	High (100)
		RDV-03	LDV-03	IAV-03	Low (0.1)	Medium (50)	Low (5)
2	SQL Injection	RDS-01	LDS-01	IAS-01	Medium (0.5)	Medium (50)	Medium (25)
		RDS-02	LDS-02	IAS-02	Low (0.1)	High (100)	Low (10)
3	Brute Force	RDB-01	LDB-01	IAB-01	Low (0.1)	High (100)	Low (10)
		RDB-02	LDB-02	IAB-02	Medium (0.5)	High (100)	Medium (50)
4	Kebakaran	RDK-	LDK-	IAK-	Low (0.1)	High (100)	Low (10)

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

		01	01	01			
		RDK-02	LDK-02	IAK-02	Low (0.1)	High (100)	Low (10)
5	Human Error	RDH-01	LDH-01	IAH-01	Medium (0.5)	Medium (50)	Medium (25)
		RDH-02	LDH-02	IAH-02	Medium (0.5)	Medium (50)	Medium (25)
		RDH-03	LDH-03	IAH-03	Medium (0.5)	Medium (50)	Medium (25)

Berikut ini juga disajikan penilaian tingkat risiko dalam bentuk grafik yang dapat dilihat pada gambar 2 dibawah ini.

Gambar 2. Grafik Tingkat Risiko



4.8. Risk Recommendation

Tahap ini bertujuan untuk memberikan rekomendasi pengendalian risiko yang dapat mengurangi atau menghilangkan risiko yang telah diidentifikasi sebelumnya, sesuai dengan framework NIST SP 800-53, yang dapat dilihat pada tabel 8 di bawah ini.

Tabel 9. Risk Recommendation

No	Sumber Ancaman	ID RD	Tingkat Risiko	Rekomendasi Kontrol
1	Virus	RDV-01	Medium (25)	Batasi penggunaan USB hanya pada perangkat yang telah terdaftar, serta nonaktifkan fitur autorun.
		RDV-02	High (100)	Aktifkan pembaruan otomatis pada perangkat lunak antivirus.
		RDV-03	Low (5)	Blokir akses pengguna ke situs web yang menyediakan unduhan ilegal.
2	SQL Injection	RDS-01	Medium (25)	Berikan pelatihan keamanan aplikasi dan manajemen risiko TI kepada para pengembang sistem.
		RDS-02	Low (10)	Terapkan penggunaan *parameterized queries* dan validasi input secara ketat.
3	Brute Force	RDB-01	Low (10)	Gunakan sistem monitoring yang mampu mendeteksi pola serangan dan aktivitas login mencurigakan.
		RDB-02	Medium (50)	Terapkan otentikasi multi-faktor (MFA) untuk akun yang memiliki akses kritis.
4	Kebakaran	RDK-01	Low (10)	Gunakan sistem pemadam kebakaran otomatis serta pemantauan terhadap kondisi kelistrikan.
		RDK-02	Low (10)	Pasang penangkal petir, *surge protector*, dan gunakan UPS untuk melindungi perangkat dari gangguan listrik.
5	Human Error	RDH-01	Medium (25)	Wajibkan pelatihan keamanan berkala dan evaluasi kesadaran

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 2, Juni 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

		pegawai.
RDH-02	Medium (25)	Implementasikan kebijakan dan prosedur standar operasional secara konsisten.
RDH-03	Medium (25)	Wajibkan pelatihan rutin serta sertifikasi kompetensi bagi seluruh staf terkait.

5. KESIMPULAN DAN SARAN

Penilaian risiko berdasarkan framework NIST SP 800-30 berhasil mengidentifikasi sejumlah ancaman yang berpotensi mengganggu kelangsungan sistem informasi di perusahaan. Risiko tertinggi berasal dari ancaman virus akibat antivirus yang tidak diperbarui, dengan nilai risiko sebesar 100 (kategori tinggi). Risiko lain seperti human error, brute force, SQL injection, dan kebakaran juga ditemukan, meskipun sebagian besar memiliki tingkat kemungkinan yang rendah hingga sedang.

Sebagai langkah mitigasi, disarankan agar perusahaan memperbarui sistem keamanan secara berkala, menerapkan autentikasi multi-faktor, meningkatkan kesadaran karyawan terkait keamanan informasi, serta memperkuat kontrol operasional dan dokumentasi. Dengan perbaikan tersebut, perusahaan diharapkan dapat meningkatkan efektivitas pengelolaan risiko TI dan menjaga stabilitas operasional di masa mendatang. Keberhasilan mitigasi risiko dapat diukur melalui indikator seperti penurunan jumlah insiden keamanan, peningkatan kepatuhan terhadap kebijakan TI, dan hasil audit internal yang lebih baik setelah implementasi kontrol.

Berdasarkan hasil penelitian, berikut beberapa saran yang dapat dipertimbangkan:

1. Memanfaatkan framework lain seperti NIST SP 800-30, NIST CSF, COBIT, atau kerangka serupa dalam mengevaluasi keamanan teknologi informasi.
2. Menggabungkan beberapa framework untuk meningkatkan efektivitas dalam penilaian dan pengelolaan keamanan informasi.

6. UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada PT Air Minum Giri Menang Mataram atas izin, dukungan, dan kesempatan yang telah diberikan sehingga penelitian ini dapat dilaksanakan. Penghargaan yang tulus juga diberikan kepada Kepala Bidang Teknologi Informasi beserta seluruh jajaran yang telah memberikan data, informasi, serta waktu selama proses wawancara dan diskusi, yang sangat membantu dalam memperoleh pemahaman mengenai sistem informasi dan pengelolaan risikonya. Kontribusi dan kerja sama yang diberikan oleh seluruh pihak terkait menjadi bagian penting dalam kelancaran dan penyelesaian penelitian ini.

DAFTAR PUSTAKA:

[1] C. A. Cholik, "PERKEMBANGAN TEKNOLOGI INFORMASI KOMUNIKASI / ICT DALAM BERBAGAI BIDANG," *J. Bus. Theory Pract.*, vol. 10, no. 2, p. 6, 2021, [Online]. Available: http://www.theseus.fi/handle/10024/341553%0Ahttps://jptam.org/index.php/jptam/article/view/1958%0Ahttp://ejurnal.undana.ac.id/index.php/glory/article/view/4816%0Ahttps://dspace.uii.ac.id/bitstream/handle/123456789/23790/17211077 Tarita Syavira Alicia.pdf?

[2] S. Nurul, S. Anggrainy, and S. Aprelyani, "FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI : KEAMANAN INFORMASI , TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM)," *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022.

[3] A. W. Darwin Effendi, "PEMANFAATAN TEKNOLOGI DALAM PROSES PEMBELAJARAN MENUJU," *Pros. Semin. Nas. Pendidik. Progr. Pascasarj. Univ. PGRI PALEMBANG*, pp. 125–129, 2019.

[4] C. R. Prilly Peshaulia Thenu, Agustinus Fritz Wijaya, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 5 (STUDI KASUS : PT GLOBAL INFOTECH)," *J. Bina Komput.*, pp. 1–13, 2020.

[5] A. D. M. Sukma Arta Atmojo, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office," *J. Tek. Inform. dan Sist. Inf.*,

vol. 7, no. 3, pp. 546–558, 2020.

[6] A. S. Millah, Apriyani, D. Arobiah, E. S. Febriani, and E. Ramdhani, "Analisis Data dalam Penelitian Tindakan Kelas," *J. Kreat. Mhs.*, vol. 1, no. 2, pp. 140–153, 2023.

[7] I. A. Siregar, "Analisis Dan Interpretasi Data Kuantitatif," *ALACRITY J. Educ.*, vol. 1, no. 2, pp. 39–48, 2021, doi: 10.52121/alacrity.v1i2.25.

[8] M. D. Ria and A. Budiman, "Perancangan sistem informasi tata kelola teknologi informasi perpustakaan," *J. Inform. dan Rekayasa Perangkat Lunak*, vol. 2, no. 1, pp. 122–133, 2021.

[9] T. Makmur, "TEKNOLOGI INFORMASI," *Info Bibl. J. Perpust. dan Ilmu Inf.*, p. null, 2019, doi: 10.24036/ib.v1i1.12.

[10] L. S. S. Paul Eduard Sudjiman, "KOMPUTER DALAM PROSES PENGAMBILAN KEPUTUSAN Paul Eduard Sudjiman dan Lorina Siregar Sudjiman COMPUTER BASED MANAGEMENT INFORMATION SYSTEM," *J. TeIKa*, 2018.

[11] N. Yona Sidratul Munti and D. Asril Syaifuddin, "Analisa Dampak Perkembangan Teknologi Informasi Dan Komunikasi Dalam Bidang Pendidikan," *J. Pendidik. Tambusai*, vol. 4, no. 2, pp. 1799–1805, 2020.

[12] H. E. N. E. S. S. N. I. M. R. I. I. H. M. L. P. G. S. A. B. M. A. H. L. N. L. A. & F. S. P. M. Akbar, *Manajemen Risiko*. 2021.

[13] I. P. A. E. Pratama and M. T. S. Pratika, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018," *J. Telemat.*, vol. 15, no. 2, pp. 63–70, 2021, doi: 10.61769/telematika.v15i2.333.

[14] J. Ecleas and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Software PEGA Menggunakan ISO 31000," *J. Tek. Inform. dan Sist. Inf.*, vol. 8, no. 1, 2021.

[15] J. N. Utamajaya and 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, 2021.

[16] D. I. Izatri, N. I. Rohmah, and R. S. Dewi, "Identifikasi Risiko pada Perpustakaan Daerah Gresik dengan NIST SP 800-30," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 50, 2020, doi: 10.30865/jurikom.v7i1.1756.

[17] A. A. Putro, A. Ambarwati, and E. Setiawan, "Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1," *J. Teknol. dan Inf.*, vol. 11, no. 2, pp. 125–136, 2021, doi: 10.34010/jati.v11i2.5314.

[18] M. H. Alifian and D. Priharsari, "Penyusunan Disaster Recovery Plan (DRP) menggunakan framework NIST SP 800-34 (Studi Kasus pada Perusahaan IT Nasional)," vol. 5, no. 10, pp. 4673–4679, 2021, [Online]. Available: http://j-ptiik.ub.ac.id.