JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 5, No. 3, November 2026, pp. 36-46
p-ISSN : 2803-1507 (media cetak) | e-ISSN: 2803-1531 (media online)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/175

Cybersecurity Risk Analysis on WhatsApp Application Using ISO/IEC 27001 Framework

Nining Ariati[1], Khalil Fikri*[2], Gathan Albani[3], M. Erbi Agustian[4], Mgs Andi Gantara[5], Yovi Prayoga[6]
[1,2,3,4,5,6] Program Studi Sistem Informasi, Universitas Indo Global Mandiri, Palembang, Indonesia
Jl. Jend. Sudirman Km.4 No. 62, 20 Ilir D. IV, Kec. Ilir Tim. I, Kota Palembang, Sumatera Selatan 30129
e-mail: nining@uigm.ac.id[1]

ARTICLE INFO

Article History:

Received: 23-04-2026
Revised: 29-05-2026
Accepted: 24-07-2026
Published: 28-10-2026

ABSTRACT

Cybersecurity threats continue to increase alongside the widespread use of digital communication applications such as WhatsApp in daily activities. This study aims to analyze cybersecurity risks associated with WhatsApp usage based on the ISO/IEC 27001 framework and to identify users' security awareness regarding various threats that may affect information security. The research employed a descriptive quantitative method by collecting data through a Likert-scale questionnaire distributed to 70 active WhatsApp users. The collected data were analyzed using validity testing, reliability testing, and descriptive statistical analysis to evaluate users' perceptions and security behaviors. The results indicate that the majority of respondents demonstrate a good level of cybersecurity awareness, particularly in protecting one-time password (OTP) codes, recognizing suspicious messages or links, and understanding the importance of personal data protection. The risk analysis identified several major threats that may compromise information security, including phishing attacks, OTP misuse, account hijacking, and personal data leakage. In addition, some users have not fully utilized additional security features such as two-step verification and privacy settings. Based on the security control principles of ISO/IEC 27001, improving cybersecurity literacy, optimizing the use of security features, and providing continuous user education can help reduce information security risks associated with WhatsApp usage. This study contributes to understanding user security awareness and provides recommendations for strengthening information protection against evolving cyber threats.

Keywords: *Cybersecurity, WhatsApp, ISO/IEC27001, Information Security Awareness, Risk Analysis.*

Abstrak

Ancaman keamanan siber terus meningkat seiring dengan tingginya penggunaan aplikasi komunikasi digital seperti *WhatsApp* dalam berbagai aktivitas sehari-hari. Penelitian ini bertujuan untuk menganalisis risiko keamanan siber pada penggunaan *WhatsApp* berdasarkan kerangka kerja ISO/IEC 27001 serta mengidentifikasi tingkat kesadaran keamanan pengguna terhadap berbagai ancaman yang berpotensi mengganggu keamanan informasi. Metode penelitian yang digunakan adalah kuantitatif deskriptif dengan pengumpulan data melalui kuesioner berbasis skala Likert yang disebarkan kepada 70 pengguna aktif *WhatsApp*. Data yang diperoleh dianalisis menggunakan uji validitas, uji reliabilitas, dan statistik deskriptif untuk mengevaluasi persepsi serta perilaku keamanan pengguna. Hasil penelitian menunjukkan bahwa mayoritas responden memiliki tingkat kesadaran keamanan siber yang baik, terutama dalam menjaga kerahasiaan kode OTP, mengenali pesan atau tautan mencurigakan, serta memahami pentingnya perlindungan data pribadi. Analisis risiko mengidentifikasi beberapa ancaman utama yang berpotensi memengaruhi keamanan informasi pengguna, yaitu *phishing*, penyalahgunaan kode OTP, pencurian akun, dan kebocoran data pribadi. Selain itu, masih terdapat pengguna yang belum memanfaatkan fitur keamanan

DOI: https://doi.org/10.51903/qdy0wx11

p-ISSN : 2803-1507 e-ISSN : 2803-1531

tambahan seperti verifikasi dua langkah dan pengaturan privasi secara optimal. Berdasarkan prinsip pengendalian keamanan ISO/IEC 27001, peningkatan literasi keamanan siber, pemanfaatan fitur keamanan, dan edukasi pengguna secara berkelanjutan dapat membantu mengurangi risiko keamanan informasi pada penggunaan *WhatsApp*.

Kata Kunci: Keamanan Siber*, WhatsApp,* ISO/IEC 27001*,* Kesadaran Keamanan Informasi, Analisis Risiko.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah cara individu maupun organisasi dalam bertukar informasi secara cepat dan efisien. Salah satu aplikasi komunikasi yang paling banyak digunakan saat ini adalah *WhatsApp*, yang menyediakan berbagai layanan seperti pesan instan, panggilan suara, panggilan video, serta pengiriman dokumen digital. Berdasarkan berbagai laporan keamanan siber, peningkatan penggunaan aplikasi komunikasi digital juga diikuti oleh meningkatnya ancaman keamanan informasi seperti *phishing, malware*, pencurian identitas, penyalahgunaan data pribadi, dan serangan *social engineering* [1], [2]. Kondisi tersebut menunjukkan bahwa keamanan informasi menjadi aspek penting yang harus diperhatikan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi yang diproses melalui aplikasi komunikasi digital [3], [4].

Fenomena meningkatnya ancaman keamanan siber pada aplikasi komunikasi telah menjadi perhatian berbagai pihak, baik pengguna individu maupun organisasi. Meskipun *WhatsApp* telah menerapkan mekanisme *end-to-end encryption*, berbagai penelitian menunjukkan bahwa risiko keamanan masih dapat muncul melalui faktor manusia, konfigurasi perangkat yang tidak aman, kebocoran metadata, serangan rekayasa sosial, serta kelemahan pada proses pengelolaan keamanan informasi [5], [6]. Selain itu, meningkatnya penggunaan *WhatsApp* dalam aktivitas akademik, bisnis, dan pemerintahan menjadikan aplikasi ini sebagai salah satu target yang menarik bagi pelaku kejahatan siber [7], [8]. Oleh karena itu, diperlukan pendekatan manajemen risiko yang sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko keamanan yang mungkin terjadi pada penggunaan aplikasi tersebut [9].

Salah satu standar internasional yang banyak digunakan dalam pengelolaan keamanan informasi adalah *Information Security Management System* (ISMS) ISO/IEC 27001. Standar ini menyediakan kerangka kerja yang komprehensif untuk mengidentifikasi aset informasi, mengukur tingkat risiko, menentukan kontrol keamanan, serta melakukan perbaikan berkelanjutan terhadap sistem keamanan informasi [10], [11]. Berbagai penelitian telah menerapkan ISO 27001 pada sektor pendidikan, kesehatan, pemerintahan, *e-commerce*, dan organisasi bisnis untuk meningkatkan efektivitas pengelolaan risiko keamanan informasi [12], [16]. Hasil penelitian tersebut menunjukkan bahwa penerapan kontrol keamanan berdasarkan ISO 27001 mampu membantu organisasi dalam mengurangi kemungkinan terjadinya insiden keamanan informasi dan meningkatkan kesiapan menghadapi ancaman siber [17], [18].

Penelitian terdahulu sebagian besar berfokus pada implementasi ISO 27001 pada sistem informasi organisasi, aplikasi web, laboratorium klinik, perusahaan media, maupun perusahaan teknologi finansial [19], [22]. Namun demikian, penelitian yang secara khusus mengkaji analisis risiko keamanan siber pada aplikasi *WhatsApp* dengan menggunakan kerangka kerja ISO 27001 masih relatif terbatas. Sebagian penelitian hanya membahas aspek teknis keamanan aplikasi komunikasi tanpa menghubungkannya dengan proses manajemen risiko yang terstruktur [23], [24]. Kondisi ini menunjukkan adanya *research gap* berupa keterbatasan kajian mengenai identifikasi risiko keamanan siber pada aplikasi *WhatsApp* berdasarkan kontrol keamanan yang direkomendasikan oleh ISO 27001 [4], [25], [26], [27].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk melakukan analisis risiko keamanan siber pada aplikasi *WhatsApp* menggunakan kerangka kerja ISO/IEC 27001. Analisis dilakukan dengan mengidentifikasi aset informasi, ancaman, kerentanan, dampak risiko, serta tingkat kemungkinan terjadinya risiko. Hasil analisis diharapkan mampu memberikan gambaran mengenai tingkat risiko keamanan yang terdapat pada penggunaan aplikasi *WhatsApp* serta rekomendasi pengendalian yang sesuai dengan standar ISO 27001. Kontribusi penelitian ini adalah menyediakan pendekatan analisis risiko yang terstruktur terhadap aplikasi komunikasi digital yang banyak digunakan masyarakat sehingga dapat menjadi referensi bagi pengguna maupun organisasi dalam meningkatkan keamanan informasi.

2. TINJAUAN PUSTAKA

2.1. ISO/IEC 27001 dan Manajemen Risiko Keamanan Informasi

p-ISSN : 2803-1507 e-ISSN : 2803-1531

ISO/IEC 27001 merupakan standar internasional yang digunakan untuk membangun dan mengelola *Information Security Management System* (ISMS). Standar ini menyediakan kerangka kerja untuk mengidentifikasi aset informasi, melakukan penilaian risiko, menentukan kontrol keamanan, serta melakukan evaluasi berkelanjutan terhadap efektivitas pengendalian yang diterapkan [10], [11]. Dalam konteks keamanan informasi, tujuan utama penerapan ISO 27001 adalah menjaga aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Manajemen risiko keamanan informasi merupakan proses sistematis yang mencakup identifikasi risiko, analisis risiko, evaluasi risiko, dan perlakuan risiko. Menurut berbagai penelitian, penerapan ISO 27001 mampu meningkatkan efektivitas pengelolaan keamanan informasi dengan menyediakan kontrol keamanan yang sesuai terhadap risiko yang ditemukan [12], [13], [18]. Oleh karena itu, ISO 27001 banyak digunakan sebagai acuan dalam analisis risiko keamanan siber pada berbagai jenis sistem informasi.

2.2. Risiko Keamanan Siber pada Aplikasi *WhatsApp*

WhatsApp merupakan aplikasi komunikasi berbasis internet yang digunakan untuk mengirim pesan, dokumen, gambar, suara, dan video. Meskipun telah menerapkan teknologi *end-to-end encryption*, aplikasi ini tetap menghadapi berbagai ancaman keamanan seperti phishing, pencurian akun, *malware*, kebocoran data pribadi, dan rekayasa sosial [5], [6]. Ancaman tersebut dapat berdampak pada kerahasiaan informasi pengguna serta menyebabkan kerugian finansial maupun reputasi. Dalam konteks manajemen risiko, ancaman keamanan tidak hanya berasal dari kelemahan teknis sistem, tetapi juga dari faktor manusia dan prosedur operasional yang kurang memadai. Oleh karena itu, diperlukan pendekatan analisis risiko yang mampu mengidentifikasi seluruh potensi ancaman dan menentukan tingkat risiko yang mungkin terjadi selama penggunaan aplikasi *WhatsApp*.

2.3. Penilaian Risiko Menggunakan ISO/IEC 27001

Proses penilaian risiko dalam ISO 27001 dimulai dengan identifikasi aset informasi yang akan dilindungi. Selanjutnya dilakukan identifikasi ancaman dan kerentanan yang dapat memengaruhi aset tersebut. Tingkat risiko kemudian ditentukan berdasarkan kombinasi antara kemungkinan terjadinya ancaman (*likelihood*) dan dampak yang ditimbulkan (*impact*). Rumus perhitungan risiko yang umum digunakan adalah Equation 1.

$$\text{Risk} = \text{Likelihood} \times \text{Impact} \qquad (1)$$

Dimana, *Risk* adalah nilai risiko, *Likelihood* adalah kemungkinan terjadinya ancaman, dan *Impact* meurpakan dampak yang ditimbulkan apabila ancaman terjadi. Melalui pendekatan tersebut, organisasi dapat menentukan prioritas pengendalian keamanan berdasarkan tingkat risiko yang diperoleh. Risiko dengan kategori tinggi memerlukan tindakan mitigasi segera, sedangkan risiko dengan kategori rendah dapat diterima dengan pengawasan tertentu.

3. METODOLOGI PENELITIAN

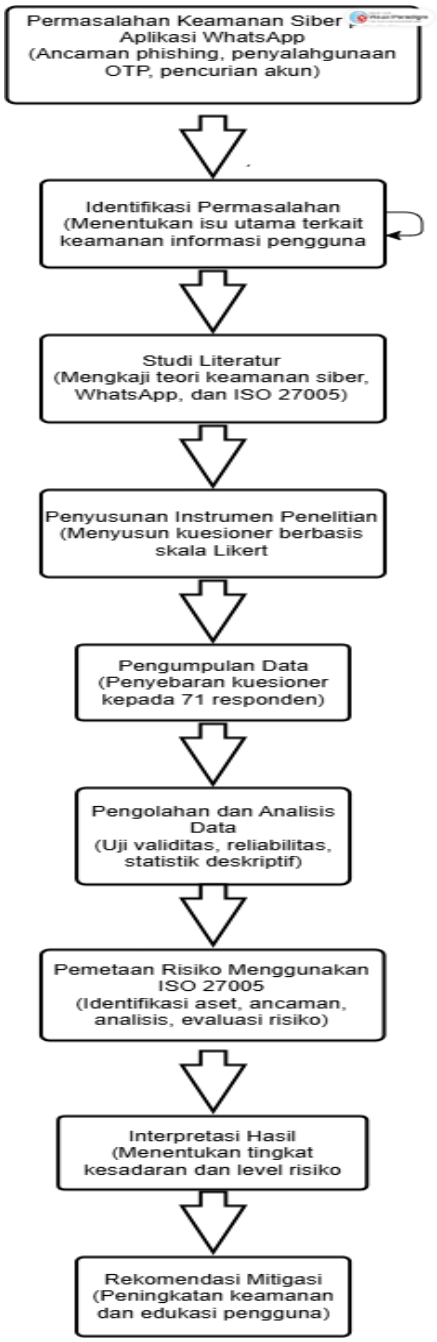
3.1. Proses Penelitian

Proses penelitian yang digunakan dalam penelitian ini ditunjukkan pada Gambar 1. Penelitian dilakukan secara sistematis untuk menganalisis risiko keamanan siber pada penggunaan *WhatsApp* berdasarkan prinsip dan kontrol keamanan informasi yang terdapat dalam ISO/IEC 27001. *Framework* ini digunakan sebagai acuan dalam mengevaluasi tingkat kesadaran keamanan pengguna serta mengidentifikasi risiko yang berpotensi mengancam kerahasiaan, integritas, dan ketersediaan informasi.

Tahap pertama penelitian adalah identifikasi permasalahan keamanan siber yang umum terjadi pada aplikasi *WhatsApp*, seperti *phishing*, penyalahgunaan kode OTP, pencurian akun, dan kebocoran data pribadi. Permasalahan tersebut menjadi dasar dalam menentukan fokus penelitian dan penyusunan instrumen penelitian. Tahap berikutnya adalah studi literatur yang bertujuan memperoleh landasan teori mengenai keamanan siber, keamanan informasi, penggunaan *WhatsApp*, serta penerapan *Information Security Management System* (ISMS) berdasarkan ISO/IEC 27001.

Literatur diperoleh dari jurnal ilmiah, buku, artikel akademik, dan dokumen resmi yang relevan dengan topik penelitian. Setelah memperoleh dasar teoritis yang memadai, dilakukan penyusunan instrumen penelitian berupa kuesioner berbasis skala Likert lima poin. Instrumen penelitian disusun untuk mengukur persepsi keamanan, pemahaman risiko, perilaku kehati-hatian, penggunaan fitur keamanan, kepercayaan terhadap sistem, pengalaman terhadap ancaman, perlindungan privasi, dan kebutuhan edukasi keamanan siber pada pengguna *WhatsApp*.

p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 1. Proses Penelitian

Tahap selanjutnya adalah pengumpulan data melalui penyebaran kuesioner secara daring menggunakan *Google Forms*. Responden penelitian merupakan pengguna aktif *WhatsApp* yang memenuhi kriteria penelitian. Sebanyak 70 responden berhasil berpartisipasi dan digunakan sebagai sampel penelitian. Data yang telah terkumpul kemudian diolah menggunakan *Microsoft Excel*. Pengolahan data dilakukan melalui analisis statistik deskriptif untuk mengetahui distribusi jawaban responden, frekuensi, persentase, nilai rata-rata (*mean*), dan tingkat kesadaran keamanan siber pengguna *WhatsApp*. Hasil analisis statistik selanjutnya dievaluasi berdasarkan kontrol keamanan yang relevan dalam ISO/IEC 27001, seperti pengendalian akses (*access control*), kesadaran keamanan informasi (*information security awareness*), keamanan operasional (*operations security*), dan perlindungan komunikasi (*communications security*). Hasil analisis kemudian dipetakan ke dalam kontrol keamanan yang relevan pada ISO/IEC 27001 untuk mengidentifikasi risiko, dampak, serta rekomendasi mitigasi yang sesuai.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Tahap akhir penelitian adalah interpretasi hasil dan penyusunan rekomendasi. Pada tahap ini, peneliti menarik kesimpulan mengenai tingkat kesadaran keamanan siber pengguna *WhatsApp* serta memberikan rekomendasi peningkatan keamanan melalui edukasi pengguna, pemanfaatan fitur keamanan tambahan, dan penerapan praktik keamanan informasi yang sesuai dengan ISO/IEC 27001.

3.2. Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh pengguna aktif aplikasi *WhatsApp* yang menggunakan aplikasi tersebut sebagai sarana komunikasi sehari-hari. Populasi dipilih karena penelitian berfokus pada tingkat kesadaran keamanan siber pengguna dalam menggunakan aplikasi *WhatsApp*. Teknik pengambilan sampel yang digunakan adalah purposive sampling, yaitu metode pemilihan sampel berdasarkan kriteria tertentu yang sesuai dengan tujuan penelitian. Adapun kriteria responden dalam penelitian ini adalah pengguna aktif *WhatsApp* yang bersedia mengisi kuesioner dan memiliki pengalaman menggunakan aplikasi tersebut. Pengumpulan data dilakukan secara daring menggunakan *Google Forms*. Berdasarkan proses pengumpulan data yang telah dilakukan, diperoleh sebanyak 70 responden yang memenuhi kriteria penelitian dan digunakan sebagai sampel penelitian. Data yang diperoleh selanjutnya digunakan untuk menganalisis tingkat kesadaran keamanan siber pengguna WhatsApp serta mengidentifikasi potensi risiko keamanan informasi berdasarkan ISO/IEC 27001.

3.3. Instrumen Penelitian

Instrumen penelitian yang digunakan dalam penelitian ini adalah kuesioner berbasis skala Likert lima poin. Skala Likert digunakan untuk mengukur tingkat persetujuan responden terhadap setiap pernyataan yang berkaitan dengan keamanan siber pada penggunaan *WhatsApp*. Skala yang digunakan terdiri dari nilai 1 sampai 5, dengan kategori 1 = Sangat Tidak Setuju, 2 = Tidak Setuju, 3 = Netral, 4 = Setuju, dan 5 = Sangat Setuju.

Tabel 1. Indikator Penelitian

No	Indikator	Deskripsi
1	Keamanan Informasi Pribadi	Mengukur persepsi responden mengenai keamanan informasi pribadi saat menggunakan *WhatsApp.*
2	Pemahaman Risiko Keamanan Siber	Mengukur tingkat pemahaman responden terhadap risiko keamanan siber yang dapat terjadi pada penggunaan *WhatsApp.*
3	Kehati-hatian terhadap Pesan atau Tautan Tidak Dikenal	Mengukur tingkat kewaspadaan responden terhadap pesan, tautan, atau nomor yang tidak dikenal.
4	Penggunaan Verifikasi Dua Langkah	Mengukur penerapan fitur keamanan verifikasi dua langkah pada akun *WhatsApp.*
5	Pembaruan Aplikasi Secara Berkala	Mengukur kebiasaan responden dalam memperbarui aplikasi untuk memperoleh perlindungan keamanan terbaru.
6	Kesadaran Menjaga Kerahasiaan Kode OTP	Mengukur kesadaran responden untuk tidak membagikan kode OTP kepada pihak lain.
7	Pengetahuan terhadap Enkripsi *End-to-End*	Mengukur tingkat pengetahuan responden terhadap fitur enkripsi yang digunakan oleh *WhatsApp.*
8	Pengalaman Menghadapi Ancaman *Phishing*	Mengukur pengalaman responden terkait penerimaan pesan atau tautan yang mengandung unsur penipuan (*phishing*).
9	Perlindungan Informasi Pribadi	Mengukur perilaku responden dalam membatasi penyebaran informasi pribadi pada aplikasi *WhatsApp.*
10	Kebutuhan Edukasi Keamanan Siber	Mengukur pandangan responden mengenai pentingnya edukasi dan peningkatan pengetahuan keamanan siber.

Kuesioner disusun berdasarkan aspek-aspek keamanan informasi yang relevan dengan penggunaan *WhatsApp*, seperti keamanan informasi pribadi, pemahaman risiko keamanan siber, kewaspadaan terhadap ancaman digital, penggunaan fitur keamanan tambahan, perlindungan data pribadi, serta kebutuhan edukasi keamanan siber. Instrumen penelitian terdiri atas 10 butir pertanyaan yang disusun untuk memperoleh gambaran mengenai tingkat kesadaran keamanan siber pengguna. Indikator penelitian yang digunakan dapat dilihat pada Tabel 1.

3.4. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah penyebaran kuesioner secara daring menggunakan *Google Forms*. Kuesioner disusun berdasarkan indikator yang berkaitan dengan keamanan siber pada penggunaan *WhatsApp*, seperti keamanan informasi pribadi, pemahaman risiko keamanan siber, kewaspadaan terhadap ancaman digital, penggunaan fitur keamanan tambahan, perlindungan data pribadi, dan kebutuhan edukasi keamanan siber. Responden dalam penelitian ini merupakan pengguna aktif *WhatsApp* yang memenuhi kriteria penelitian dan bersedia berpartisipasi secara sukarela. Kuesioner menggunakan skala Likert lima poin, yaitu Sangat Tidak Setuju (1), Tidak Setuju (2), Netral (3), Setuju (4),

p-ISSN : 2803-1507 e-ISSN : 2803-1531

dan Sangat Setuju (5). Melalui proses pengumpulan data tersebut diperoleh sebanyak 70 responden yang digunakan sebagai sampel penelitian. Data yang diperoleh dari hasil kuesioner selanjutnya digunakan untuk menganalisis tingkat kesadaran keamanan siber pengguna *WhatsApp* serta mengidentifikasi potensi risiko keamanan informasi yang relevan dengan prinsip ISO/IEC 27001

3.5. Teknik Analisis Data

Data yang telah terkumpul dianalisis menggunakan metode statistik deskriptif dengan bantuan *Microsoft Excel*. Analisis dilakukan untuk mengetahui distribusi jawaban responden, frekuensi, persentase, dan nilai rata-rata (*mean*) dari setiap indikator penelitian. Nilai rata-rata (*mean*) digunakan untuk mengetahui tingkat kecenderungan jawaban responden terhadap setiap indikator keamanan siber. Semakin tinggi nilai mean, maka semakin tinggi tingkat kesadaran keamanan siber yang dimiliki responden terhadap indikator yang diukur. Hasil analisis statistik deskriptif kemudian diinterpretasikan dan dipetakan terhadap kontrol keamanan yang relevan dalam ISO/IEC 27001. Proses ini dilakukan untuk mengidentifikasi ancaman, risiko, dampak, serta rekomendasi mitigasi yang dapat diterapkan dalam penggunaan *WhatsApp*. Risiko yang dianalisis meliputi ancaman phishing, penyalahgunaan kode OTP, kebocoran data pribadi, penggunaan fitur keamanan yang belum optimal, serta kerentanan akibat kurangnya kesadaran pengguna terhadap keamanan informasi. Selanjutnya, hasil analisis digunakan sebagai dasar dalam penyusunan rekomendasi yang bertujuan untuk meningkatkan kesadaran keamanan siber pengguna dan mendukung penerapan praktik keamanan informasi yang sesuai dengan ISO/IEC 27001

4. HASIL DAN DISKUSI

4.1. Karakteristik Responden

Karakteristik responden dalam penelitian ini digunakan untuk memberikan gambaran umum mengenai profil responden yang berpartisipasi dalam penelitian. Responden penelitian merupakan pengguna aktif *WhatsApp* yang mengisi kuesioner secara daring melalui Google Forms. Jumlah responden yang berhasil dihimpun sebanyak 70 orang.

Karakteristik responden berdasarkan jenis kelamin dapat dilihat pada Tabel 2. Berdasarkan Tabel 2, responden penelitian didominasi oleh laki-laki sebanyak 43 orang atau 61,43% dari total responden. Sementara itu, responden perempuan berjumlah 27 orang atau 38,57%. Hasil tersebut menunjukkan bahwa sebagian besar responden yang berpartisipasi dalam penelitian ini adalah pengguna *WhatsApp* berjenis kelamin laki-laki. Karakteristik responden berdasarkan usia dapat dilihat pada Tabel 3

Tabel 2. Karakteristik Responden Berdasarkan Jenis Kelamin

Jenis Kelamin	Jumlah	Persentase (%)
Laki-laki	43	61,43
Perempuan	27	38,57
Total	70	100

Berdasarkan Tabel 3, mayoritas responden berada pada rentang usia 20–25 tahun dengan jumlah 53 responden atau 75,71% dari total responden. Responden berusia di bawah 20 tahun berjumlah 2 orang (2,86%), usia 26–30 tahun berjumlah 3 orang (4,29%), dan usia di atas 30 tahun berjumlah 11 orang (15,71%). Hasil ini menunjukkan bahwa penelitian didominasi oleh kelompok usia produktif yang aktif menggunakan *WhatsApp* sebagai media komunikasi sehari-hari.

Tabel 3. Karakteristik Responden Berdasarkan Usia

Usia	J Jumlah	Persentase (%)
< 20 Tahun	2	2,86
20–25 Tahun	53	75,71
26–30 Tahun	3	4,29
> 30 Tahun	11	15,71
Tidak Terbaca	1	1,43
Total	70	100

4.2. Hasil Analisis Kuesioner

Analisis kuesioner dilakukan untuk mengetahui tingkat kesadaran keamanan siber pengguna *WhatsApp*. Data dianalisis menggunakan metode statistik deskriptif berupa frekuensi jawaban dan nilai rata-rata (*mean*) pada setiap indikator penelitian. Untuk frekuensi jawaban responden pada salah satu indikator penelitian dapat dilihat pada Tabel 4.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Tabel 4. Frekuensi Jawaban Responden

Pernyataan 1	
"Saya merasa informasi pribadi saya aman saat menggunakan *WhatsApp*"	
Skala	**Frekuensi**
1	3
2	3
3	6
4	19
5	39
Total	70

Berdasarkan Tabel 4, mayoritas responden memberikan jawaban pada kategori Setuju dan Sangat Setuju. Sebanyak 39 responden memilih kategori Sangat Setuju dan 19 responden memilih kategori Setuju terhadap pernyataan mengenai keamanan informasi pribadi saat menggunakan *WhatsApp*. Hasil ini menunjukkan bahwa sebagian besar responden memiliki tingkat kepercayaan yang cukup tinggi terhadap keamanan informasi pribadi yang mereka miliki saat menggunakan aplikasi tersebut. Meskipun demikian, masih terdapat beberapa responden yang memberikan jawaban Netral, Tidak Setuju, dan Sangat Tidak Setuju. Hal ini menunjukkan bahwa masih terdapat sebagian pengguna yang memiliki kekhawatiran terhadap keamanan informasi pribadi dalam penggunaan *WhatsApp*.

Nilai rata-rata (*mean*) setiap indikator penelitian digunakan untuk mengetahui tingkat kesadaran keamanan siber responden terhadap berbagai aspek keamanan informasi. Hasil perhitungan nilai rata-rata dapat dilihat pada Tabel 5.

Tabel 5. Nilai Rata-Rata (*Mean*) Tiap Indikator

No	**Indikator**	**Mean**
1	Keamanan Informasi Pribadi	4,26
2	Pemahaman Risiko Keamanan Siber	4,37
3	Kehati-hatian terhadap Pesan/Tautan Tidak Dikenal	4,71
4	Penggunaan Verifikasi Dua Langkah	4,47
5	Pembaruan Aplikasi Secara Berkala	4,41
6	Kesadaran Menjaga Kode OTP	4,69
7	Kepercayaan terhadap Enkripsi End-to-End	4,47
8	Pengalaman Menerima Phishing	4,49
9	Perlindungan Informasi Pribadi	4,56
10	Kebutuhan Edukasi Keamanan Siber	4,59

Berdasarkan Tabel 5, indikator kehati-hatian terhadap pesan atau tautan dari nomor yang tidak dikenal memperoleh nilai rata-rata tertinggi sebesar 4,71. Hasil ini menunjukkan bahwa sebagian besar responden memiliki tingkat kewaspadaan yang tinggi terhadap potensi ancaman keamanan siber, khususnya serangan *phishing* yang sering terjadi melalui pesan instan. Selain itu, indikator kesadaran menjaga kerahasiaan kode OTP juga memperoleh nilai rata-rata yang tinggi sebesar 4,69. Temuan ini menunjukkan bahwa mayoritas responden memahami pentingnya menjaga kerahasiaan kode OTP untuk mencegah pengambilalihan akun oleh pihak yang tidak bertanggung jawab.

Sementara itu, indikator keamanan informasi pribadi memperoleh nilai rata-rata terendah sebesar 4,26. Meskipun masih berada pada kategori tinggi, hasil tersebut menunjukkan bahwa aspek perlindungan informasi pribadi masih memerlukan perhatian lebih dibandingkan indikator lainnya. Secara keseluruhan, seluruh indikator penelitian memperoleh nilai rata-rata di atas 4,00. Hasil ini menunjukkan bahwa responden memiliki tingkat kesadaran keamanan siber yang cukup baik dalam penggunaan *WhatsApp*. Namun demikian, masih diperlukan peningkatan edukasi dan pemanfaatan fitur keamanan tambahan agar risiko keamanan informasi dapat diminimalkan secara lebih optimal.

4.3. Analisis Risiko Berdasarkan ISO/IEC 27001

Analisis risiko dilakukan dengan mengidentifikasi ancaman keamanan yang berpotensi terjadi pada penggunaan *WhatsApp* berdasarkan hasil kuesioner dan prinsip pengendalian keamanan informasi dalam ISO/IEC 27001. Analisis ini bertujuan untuk mengidentifikasi risiko yang dapat memengaruhi kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi pengguna. Hasil identifikasi risiko menunjukkan bahwa ancaman yang paling sering ditemui oleh responden adalah *phishing*, penyalahgunaan kode OTP, kebocoran data pribadi, tidak mengaktifkan verifikasi dua langkah, dan tidak melakukan pembaruan aplikasi secara berkala. Ancaman-ancaman tersebut dapat menyebabkan pengambilalihan akun, pencurian data pribadi, serta akses tidak sah terhadap informasi pengguna. Analisis risiko berdasarkan ISO/IEC 27001 dapat dilihat pada Tabel 6.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Tabel 6. Analisis Risiko Berdasarkan ISO/IEC 27001

Risiko	Ancaman	Dampak	Kontrol ISO/IEC 27001	Mitigasi
Phishing	Pesan atau tautan palsu	Pencurian data akun	*Information Security Awareness*	Edukasi keamanan siber
Penyalahgunaan OTP	*Social Engineering*	Pengambilalihan akun	*Access Control*	Tidak membagikan kode OTP
Kebocoran Data Pribadi	Penyebaran informasi berlebihan	Pelanggaran privasi	*Information Security Policy*	Membatasi informasi pribadi
Tidak Mengaktifkan Verifikasi Dua Langkah	Akses tidak sah	Kehilangan akun	*Access Control*	Aktivasi verifikasi dua langkah
Tidak Memperbarui Aplikasi	Kerentanan sistem	Eksploitasi keamanan	*Operations Security*	Pembaruan aplikasi secara berkala

Berdasarkan Tabel 6, risiko phishing merupakan salah satu ancaman yang paling sering ditemukan pada penggunaan *WhatsApp*. Serangan ini biasanya dilakukan melalui pesan atau tautan palsu yang bertujuan memperoleh informasi pribadi pengguna. Risiko lainnya adalah penyalahgunaan kode OTP yang dapat menyebabkan akun pengguna diambil alih oleh pihak yang tidak berwenang. Selain itu, kebocoran data pribadi juga menjadi risiko yang perlu diperhatikan. Risiko ini dapat terjadi akibat kurangnya kesadaran pengguna dalam membatasi informasi pribadi yang dibagikan melalui aplikasi. Hasil kuesioner juga menunjukkan bahwa masih terdapat pengguna yang belum mengaktifkan fitur verifikasi dua langkah serta belum melakukan pembaruan aplikasi secara berkala. Kondisi tersebut dapat meningkatkan peluang terjadinya insiden keamanan informasi.

Berdasarkan kontrol keamanan dalam ISO/IEC 27001, mitigasi yang dapat dilakukan meliputi peningkatan kesadaran keamanan informasi (*information security awareness*), penerapan kontrol akses (*access control*), penggunaan verifikasi dua langkah, pembatasan informasi pribadi yang dibagikan, serta pembaruan aplikasi secara rutin. Implementasi kontrol tersebut diharapkan dapat mengurangi kemungkinan terjadinya ancaman keamanan siber pada penggunaan *WhatsApp*. Berdasarkan hasil identifikasi aset, ancaman, dan kerentanan yang terdapat pada penggunaan WhatsApp, dilakukan penilaian risiko menggunakan pendekatan ISO/IEC 27001. Penilaian ini bertujuan untuk menentukan tingkat risiko yang mungkin terjadi serta tindakan mitigasi yang sesuai. Hasil analisis risiko disajikan pada Tabel 7.

Tabel 7. Analisis Risiko Keamanan Siber pada *WhatsApp* Berdasarkan ISO/IEC 27001

Aset	Ancaman	Kerentanan	Dampak	Likelihood	Risk Level	Mitigasi
Akun *WhatsApp*	*Phishing*	Pengguna kurang mampu membedakan tautan asli dan palsu	Pengambilalihan akun oleh pihak tidak berwenang	4	Tinggi (16)	Edukasi keamanan siber dan verifikasi sumber pesan
Kode OTP	Penyalahgunaan OTP	Pengguna membagikan kode OTP kepada pihak lain	Kehilangan akses akun dan pencurian identitas	5	Tinggi (20)	Tidak membagikan OTP kepada siapa pun dan mengaktifkan verifikasi dua langkah
Data Pribadi	Kebocoran data	Pengaturan privasi tidak optimal	Penyalahgunaan informasi pribadi	3	Sedang (12)	Pengaturan privasi yang lebih ketat dan pembatasan akses informasi
Riwayat Percakapan	*Malware*	Perangkat tidak memiliki perlindungan keamanan yang memadai	Kehilangan kerahasiaan informasi dan data percakapan	3	Sedang (9)	Menggunakan antivirus dan memperbarui sistem secara berkala
Daftar Kontak	*Social Engineering*	Rendahnya kesadaran pengguna terhadap modus penipuan	Penipuan dan pencurian informasi kontak	4	Tinggi (16)	Peningkatan kesadaran keamanan dan verifikasi identitas pengirim
Media dan Dokumen	Akses tidak sah	Penggunaan perangkat oleh pihak lain tanpa izin	Kebocoran dokumen dan informasi penting	3	Sedang (9)	Penggunaan kunci layar dan autentikasi perangkat

Berdasarkan Tabel 7, risiko tertinggi ditemukan pada penyalahgunaan kode OTP dan serangan phishing yang memiliki nilai risiko tinggi. Kondisi tersebut menunjukkan bahwa faktor manusia masih menjadi sumber risiko utama dalam penggunaan *WhatsApp*. Selain itu, ancaman kebocoran data pribadi, *malware*, dan *social engineering* juga berpotensi memengaruhi keamanan informasi pengguna. Oleh karena itu, penerapan kontrol

p-ISSN : 2803-1507 e-ISSN : 2803-1531

keamanan seperti verifikasi dua langkah, pengaturan privasi yang tepat, pembaruan sistem secara berkala, serta peningkatan kesadaran keamanan siber sangat diperlukan untuk mengurangi tingkat risiko yang ada sesuai dengan prinsip ISO/IEC 27001.

Diskusi

Hasil penelitian menunjukkan bahwa sebagian besar responden memiliki tingkat kesadaran keamanan siber yang baik. Hal ini terlihat dari nilai rata-rata (*mean*) seluruh indikator yang berada di atas 4,00. Tingginya nilai rata-rata tersebut menunjukkan bahwa responden telah memahami pentingnya menjaga keamanan akun dan informasi pribadi saat menggunakan *WhatsApp*. Indikator dengan nilai rata-rata tertinggi adalah kehati-hatian terhadap pesan atau tautan dari nomor yang tidak dikenal dengan nilai sebesar 4,71. Temuan ini menunjukkan bahwa mayoritas responden telah memiliki kewaspadaan yang tinggi terhadap ancaman phishing. Kesadaran untuk tidak membagikan kode OTP juga memperoleh nilai yang tinggi, yang menunjukkan bahwa responden memahami risiko pengambilalihan akun akibat penyalahgunaan kode verifikasi.

Meskipun demikian, hasil penelitian juga menunjukkan bahwa masih terdapat beberapa aspek yang perlu ditingkatkan. Sebagian responden belum memanfaatkan fitur verifikasi dua langkah secara optimal dan masih ada pengguna yang tidak melakukan pembaruan aplikasi secara berkala. Kondisi ini dapat meningkatkan risiko keamanan informasi karena pelaku kejahatan siber sering memanfaatkan kelemahan sistem yang belum diperbarui. Temuan penelitian ini sejalan dengan prinsip ISO/IEC 27001 yang menekankan pentingnya peran manusia dalam menjaga keamanan informasi. Selain aspek teknologi, keberhasilan penerapan keamanan informasi juga sangat dipengaruhi oleh tingkat kesadaran dan perilaku pengguna.

Oleh karena itu, peningkatan edukasi keamanan siber menjadi salah satu langkah penting dalam mengurangi risiko keamanan pada penggunaan *WhatsApp*. Secara keseluruhan, hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan siber pengguna *WhatsApp* berada pada kategori baik. Namun, masih diperlukan upaya berkelanjutan dalam bentuk edukasi, sosialisasi, dan pemanfaatan fitur keamanan yang tersedia agar perlindungan terhadap informasi pribadi dapat dilakukan secara lebih optimal sesuai dengan prinsip keamanan informasi dalam ISO/IEC 27001.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan terhadap 70 pengguna aktif *WhatsApp*, dapat disimpulkan bahwa pengguna menunjukkan tingkat kesadaran keamanan siber yang cukup baik. Hal ini terlihat dari mayoritas responden yang memberikan nilai 4 dan 5 pada sebagian besar indikator penelitian. Hasil tersebut menunjukkan bahwa responden memahami berbagai risiko keamanan siber, berhati-hati dalam menerima pesan atau tautan dari nomor yang tidak dikenal, serta memiliki perilaku yang baik dalam menjaga keamanan akun dan informasi pribadi. Hasil penelitian juga menunjukkan bahwa sebagian besar responden telah menerapkan praktik keamanan yang baik, seperti tidak membagikan kode OTP kepada pihak lain, membatasi informasi pribadi yang dibagikan, serta memahami pentingnya fitur keamanan yang tersedia pada aplikasi *WhatsApp*.

Selain itu, nilai rata-rata (*mean*) pada seluruh indikator penelitian berada di atas 4,00 yang menunjukkan tingkat kesadaran keamanan siber yang relatif baik. Meskipun demikian, masih ditemukan beberapa aspek yang perlu ditingkatkan. Sebagian responden belum mengaktifkan fitur verifikasi dua langkah dan belum melakukan pembaruan aplikasi secara berkala. Selain itu, banyak responden mengaku pernah menerima pesan yang mengandung unsur penipuan atau *phishing*, yang menunjukkan bahwa ancaman keamanan siber masih sering terjadi. Temuan ini mengindikasikan bahwa faktor manusia (*human factor*) masih menjadi salah satu penyebab utama munculnya risiko keamanan informasi.

Berdasarkan analisis yang mengacu pada prinsip dan kontrol keamanan dalam ISO/IEC 27001, risiko keamanan informasi pada penggunaan *WhatsApp* dapat diminimalkan melalui peningkatan kesadaran keamanan informasi, penerapan kontrol akses yang lebih baik, perlindungan data pribadi, serta pemanfaatan fitur keamanan yang tersedia. Dengan demikian, upaya peningkatan literasi keamanan siber dan penerapan praktik keamanan informasi yang baik perlu dilakukan secara berkelanjutan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi.

5.2. Saran

Berdasarkan hasil penelitian yang telah dilakukan, pengguna *WhatsApp* disarankan untuk terus meningkatkan kesadaran terhadap keamanan siber dengan memanfaatkan fitur keamanan yang tersedia, seperti verifikasi

p-ISSN : 2803-1507 e-ISSN : 2803-1531

dua langkah, pengaturan privasi akun, dan pembaruan aplikasi secara berkala. Pengguna juga perlu menjaga kerahasiaan kode OTP serta menghindari membagikan informasi pribadi kepada pihak yang tidak dikenal. Selain itu, pengguna diharapkan lebih waspada terhadap berbagai bentuk ancaman keamanan siber, seperti pesan mencurigakan, tautan tidak dikenal, maupun upaya *phishing* yang bertujuan memperoleh informasi pribadi atau mengambil alih akun pengguna. Peningkatan kewaspadaan ini penting untuk mengurangi risiko terjadinya insiden keamanan informasi.

Bagi institusi pendidikan, organisasi, maupun pihak terkait, disarankan untuk meningkatkan edukasi dan sosialisasi mengenai keamanan siber melalui pelatihan, seminar, maupun kampanye keamanan digital. Kegiatan tersebut diharapkan dapat meningkatkan pemahaman masyarakat mengenai pentingnya menjaga keamanan informasi dalam penggunaan aplikasi komunikasi digital. Untuk penelitian selanjutnya, disarankan menggunakan jumlah responden yang lebih besar dan cakupan responden yang lebih beragam agar hasil penelitian lebih representatif. Selain itu, penelitian selanjutnya dapat mengombinasikan metode kuesioner dengan wawancara atau observasi sehingga analisis yang dihasilkan menjadi lebih mendalam dan komprehensif.

DAFTAR PUSTAKA

[1] A. C. Pamungkas, W. S. Hulu, and R. Samihardjo, "Information Security Risk Management Web-Based Final Semester Summative Assessment Application Using ISO," vol. 6, no. 1, pp. 349–362, 2024, doi: 10.51519/journalisi.v6i1.668.

[2] A. Ramadhan and R. Pasla, "Pentingnya Keamanan Data Pribadi di Era Digital bagi Mahasiswa," Pijarwiyata: Jurnal Pendidikan, vol. 1, no. 1, pp. 1–5, Jul. 2026, doi: 10.31004/JIRA.V1I1.1.

[3] E. Susanto and N. Legowo, "Hasil Penilaian Risiko Keamanan Informasi pada Laboratorium Klinik Berdasarkan Kriteria Kendali Dalam Penerapan ISO 27001," vol. 12, no. 2, pp. 155–164, 2023.

[4] D. Nirwana, E. Nurjannah, C. Renta, A. Marpaung, and H. A. Wijaya, "Analisis Kebijakan Keamanan Cyber: Study Kasus Implementasi Perlindungan Data Pribadi Dalam Era Digital," JIIP - Jurnal Ilmiah Ilmu Pendidikan, vol. 7, no. 7, pp. 7364–7373, Jul. 2024, doi: 10.54371/JIIP.V7I7.4790.

[5] A. Ferdinand, K. Naristi, R. Abdillah, S. D. Walujo, and L. Dica, "Pengukuran Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Metode FMEA dan Framework ISO 27001 : 2013 pada PT . ABC," vol. 9, no. 1, pp. 23–33, 2024, doi: 10.33633/joins.v9i1.9059.

[6] A. I. Wijaya, D. I. Lestiani, Y. R. Damayanti, A. Ayu, P. Sugiono, and S. C. Huanggino, "Maturity Level Risk Assessment in Media Companies with ISO 27001 Framework," vol. 3, no. 1, pp. 1–18, 2024, doi: 10.26740/jdbim.v3i1.59169.

[7] I. Fadilla, N. Sartika, and R. Bisma, "Perancangan Sistem Informasi Manajemen Risiko berdasarkan ISO 27001 : 2013 (Sistem Manajemen Keamanan Informasi)," vol. 02, no. 03, pp. 81–86, 2021.

[8] S. Aprianti, R. P. Sari, and I. Rusi, "Manajemen Risiko Keamanan Simbada Menggunakan Metode NIST SP 800-30 Revisi 1 dan Kontrol ISO / IEC 27001 : 2013," vol. 14, no. April, pp. 50–59, 2023.

[9] H. Syahrial, "Prototype Information Security Risk Assessment Tool Berbasis Lotus Notes dalam Rangka Penerapan Sistem Manajemen Keamanan Informasi ISO 27001," vol. 2014, no. November, pp. 8–14, 2014.

[10] H. Susanto, M. N. Almunawar, and Y. C. Tuan, "A Novel Method on ISO 27001 Reviews : ISMS Compliance Readiness Level Measurement," vol. 2, no. 1, pp. 1–12, 2012.

[11] N. O. F. The and C. For, "Analysis of the user Acceptance for Implementing ISO/IEC 27001: 2005 In T Urkish," pp. 1–12, 2005.

[12] G. D. Alencar, H. P. De Moura, I. Honório, and D. F. Júnior, "An Adaptable Maturity Strategy for Information Security," vol. 13, pp. 1–12, 2018.

[13] B. S. Wibowo and R. F. Aji, "The Indonesian Journal of Computer Science," vol. 13, no. 4, pp. 6398–6410, 2024.

[14] R. Ali, "Operationalising Information Security Management : A Procedural Framework Analysis of ISO / IEC Implementation in a Financial-Technology Organisation," pp. 1–9, 2022.

[15] B. Cheung, "standard The ISO 27001 : 2022 certification process How KPMG can help Contact us," 2025.

[16] A. C. Pamungkas, W. S. Hulu, and R. Samihardjo, "Information Security Risk Management Web-Based Final Semester Summative Assessment Application Using ISO," vol. 6, no. 1, pp. 349–362, 2024, doi: 10.51519/journalisi.v6i1.668.

[17] H. Susanto, M. N. Almunawar, and Y. C. Tuan, "A Novel Method on ISO 27001 Reviews : ISMS Compliance Readiness Level Measurement," vol. 2, no. 1, pp. 1–12, 2012.

[18] I. Fadilla, N. Sartika, and R. Bisma, "Perancangan Sistem Informasi Manajemen Risiko berdasarkan

p-ISSN : 2803-1507 e-ISSN : 2803-1531

ISO 27001 : 2013 (Sistem Manajemen Keamanan Informasi),” vol. 02, no. 03, pp. 81–86, 2021.
[19] H. Susanto, M. N. Almunawar, and Y. C. Tuan, “A Novel Method on ISO 27001 Reviews : ISMS Compliance Readiness Level Measurement,” vol. 2, no. 1, pp. 1–12, 2012.
[20] R. Ali, “Operationalising Information Security Management : A Procedural Framework Analysis of ISO / IEC Implementation in a Financial-Technology Organisation,” pp. 1–9, 2022.
[21] A. C. Pamungkas, W. S. Hulu, and R. Samihardjo, “Information Security Risk Management Web-Based Final Semester Summative Assessment Application Using ISO,” vol. 6, no. 1, pp. 349–362, 2024, doi: 10.51519/journalisi.v6i1.668.
[22] E. Susanto and N. Legowo, “Hasil Penilaian Risiko Keamanan Informasi pada Laboratorium Klinik Berdasarkan Kriteria Kendali Dalam Penerapan ISO 27001,” vol. 12, no. 2, pp. 155–164, 2023.
[23] A. I. Wijaya, D. I. Lestiani, Y. R. Damayanti, A. Ayu, P. Sugiono, and S. C. Huanggino, “Maturity Level Risk Assessment in Media Companies with ISO 27001 Framework,” vol. 3, no. 1, pp. 1–18, 2024, doi: 10.26740/jdbim.v3i1.59169.
[24] B. Cheung, “standard The ISO 27001 : 2022 certification process How KPMG can help Contact us,” 2025.
[25] G. F. Michelle, N. Modami, E. E. R. Manopo, M. R. Kurniawan, D. R. Enditama, and A. T. Ayunda, “Information Security Evaluation Based on KAMI Index 5.0 (2023) at PT X,” Jurnal Ilmiah Sistem Informasi, vol. 5, no. 2, pp. 68–77, Jan. 2026, doi: 10.51903/ETG50932.
[26] M. Izzani, N. Nellatul, A. Ismatul, and A. Hamdani, “Evaluasi penerapan Kemanan Informasi Pada SIAKAD Universitas Ibrahimy Berbasis ISO/IEC 27001:2022,” Jurnal Ilmiah Sistem Informasi, vol. 5, no. 1, pp. 175–185, Jan. 2026, doi: 10.51903/D3BKTM29.
[27] D. A. Pratama, I. H. Santi, and F. Febrinita, “Android-Based Tourism Geographic Information System For Blitar Raya Utilizing Google Maps API and Kotlin,” Jurnal Ilmiah Sistem Informasi, vol. 5, no. 2, pp. 284–305, Apr. 2026, doi: 10.51903/CWE5DE68.