ANALISIS KEAMANAN INFORMASI PADA PLATFORM FACEBOOK MARKETPLACE MENGGUNAKAN ISO/IEC 27001

Juwardi Wafdan[1], Nur Ilham Ade Putra Ramadhan[2]
[12]Sistem Informasi, Fakultas Teknik dan Informatika, Universitas Islam Indragiri,
Email: juwardiwafdan@gmail.com[1], Nurilhamade3@gmail.com[2]

ABSTRAK

Penelitian ini mengkaji keamanan informasi pada platform *Facebook Marketplace* menggunakan kerangka kerja ISO/IEC 27001:2022. Latar belakang penelitian dilandasi oleh maraknya kasus penipuan dan kebocoran data di tengah meningkatnya aktivitas jual beli digital di media sosial. Tujuan utama dari studi ini adalah untuk mengevaluasi sejauh mana sistem keamanan informasi yang diterapkan pada fitur Marketplace sesuai dengan standar manajemen keamanan informasi internasional. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi pustaka dan analisis deskriptif-komparatif terhadap klausa-klausa utama dalam ISO/IEC 27001.Hasil analisis menunjukkan bahwa fitur Marketplace di Facebook belum sepenuhnya memenuhi prinsip-prinsip ISO/IEC 27001, terutama pada aspek manajemen risiko, verifikasi identitas, transparansi penanganan insiden, dan audit keamanan. Meskipun Meta telah menerapkan kebijakan privasi dan enkripsi data secara umum, tidak ditemukan penerapan khusus terhadap keamanan fitur Marketplace. Penelitian ini memberikan kontribusi penting dengan memetakan celah keamanan spesifik serta menyarankan penerapan modular ISO/IEC 27001 pada fitur dalam platform digital. Hasil temuan ini diharapkan menjadi masukan bagi pengelola platform, regulator, dan masyarakat dalam membangun ekosistem transaksi digital yang lebih aman dan terpercaya.

Kata Kunci: keamanan informasi, Facebook Marketplace, ISO/IEC 27001, media sosial, transaksi digital

ABSTRACT

This study examines information security on the Facebook Marketplace platform using the ISO/IEC 27001:2022 framework. The research is motivated by the growing number of fraud and data breach incidents amid the rising trend of digital buying and selling through social media. The main objective is to evaluate the extent to which information security systems implemented in the Marketplace feature align with international information security management standards. A qualitative approach was adopted, utilizing a literature review combined with a descriptive-comparative analysis of key clauses within ISO/IEC 27001.Findings reveal that Facebook Marketplace does not fully comply with ISO/IEC 27001 principles, particularly in areas such as risk management, identity verification, incident handling transparency, and security audits. Although Meta has implemented general data privacy and encryption policies, there is a lack of specific application toward the Marketplace feature. This research contributes by mapping specific security gaps and proposing a modular application of ISO/IEC 27001 to individual features within digital platforms. The findings aim to serve as valuable insights for platform operators, regulators, and the public in building a safer and more trustworthy digital transaction ecosystem.

Keywords: information security, Facebook Marketplace, ISO/IEC 27001, social media, digital transactions.

1 PENDAHULUAN

Di era digital saat ini, informasi bukan hanya menjadi bagian dari aktivitas harian, tetapi telah menjelma menjadi aset yang sangat berharga. Ketika dunia semakin terkoneksi melalui internet, perlindungan terhadap informasi menjadi tantangan yang semakin kompleks—terutama pada platform-platform daring yang melibatkan transaksi dan data pribadi pengguna secara langsung,

seperti Facebook Marketplace. Platform ini telah menjadi ruang jual beli yang sangat populer, terutama di negara berkembang seperti Indonesia, karena kemudahannya dalam menghubungkan penjual dan pembeli tanpa perantara. Namun di balik kemudahan itu, tersimpan sejumlah risiko yang kerap kali diabaikan: dari pencurian data pribadi, penipuan identitas, hingga penyalahgunaan akun dan informasi transaksi.

Fenomena kejahatan siber yang menargetkan platform e-commerce dan marketplace digital telah meningkat secara signifikan dalam beberapa tahun terakhir. Menurut laporan dari *DataReportal (2023)*, lebih dari 175 juta pengguna aktif Facebook berada di Indonesia, dan sebagian besar dari mereka turut memanfaatkan fitur Marketplace sebagai sarana transaksi barang. Namun, laporan dari *Kominfo* dan *Lembaga Riset Siber Indonesia* mencatat bahwa pengaduan terkait penipuan dan kebocoran data melalui platform tersebut juga meningkat setiap tahunnya. Hal ini menunjukkan adanya kesenjangan antara pertumbuhan penggunaan platform dan upaya perlindungan terhadap keamanan informasi di dalamnya.

Keamanan informasi bukan sekadar soal teknis melindungi data, tetapi mencakup keseluruhan sistem tata kelola, manajemen risiko, serta kontrol internal yang sistematis. Oleh karena itu, dalam konteks analisis ini, kerangka kerja *ISO/IEC 27001* dipilih sebagai pendekatan utama. Standar internasional ini menjadi acuan global dalam sistem manajemen keamanan informasi (SMKI), yang dirancang untuk mengidentifikasi, menganalisis, dan memitigasi berbagai potensi risiko keamanan informasi dalam suatu organisasi—termasuk platform digital seperti Facebook Marketplace.

Urgensi dari penelitian ini terletak pada kebutuhan mendesak untuk mengevaluasi bagaimana sistem keamanan informasi diterapkan atau bahkan diabaikan dalam sebuah platform raksasa yang digunakan oleh jutaan masyarakat Indonesia. Terlebih di tengah meningkatnya literasi digital yang belum sepenuhnya disertai dengan kesadaran akan keamanan digital, analisis semacam ini dapat memberikan kontribusi konkret dalam membangun budaya digital yang lebih aman dan bertanggung jawab.

Secara umum, artikel ini akan membahas bagaimana sistem dan fitur keamanan informasi di Facebook Marketplace saat ini ditinjau melalui perspektif ISO/IEC 27001. Penelitian ini akan memetakan elemen-elemen penting seperti konteks organisasi, kepemimpinan, perencanaan risiko, dukungan teknologi, serta mekanisme pemantauan dan peningkatan berkelanjutan. Dengan demikian, pembaca tidak hanya akan memahami kondisi keamanan yang sedang terjadi, tetapi juga mendapatkan wawasan tentang langkah-langkah konkret yang dapat diambil oleh pengguna, pengembang, atau pemangku kepentingan untuk meningkatkan keamanan digital dalam praktik jual beli online.

Dengan menyandingkan teori keamanan informasi berstandar internasional dan realitas lapangan yang terjadi di Facebook Marketplace, artikel ini diharapkan dapat menjadi kontribusi ilmiah yang relevan, aplikatif, dan bermanfaat untuk masa depan transaksi digital yang lebih aman.

2 METODE PENELITIAN

Penelitian ini menggunakan pendekatan **kualitatif dengan metode studi pustaka (literature review)** yang dipadukan dengan **analisis deskriptif-komparatif** terhadap kerangka ISO/IEC 27001. Pendekatan ini dipilih karena tujuan utama dari penelitian adalah untuk memahami, menginterpretasikan, dan menganalisis secara mendalam bagaimana aspek keamanan informasi diimplementasikan atau tidak diimplementasikan dalam platform Facebook Marketplace, berdasarkan standar internasional yang berlaku.

Pendekatan kualitatif memungkinkan peneliti untuk menggali makna, pemahaman, dan konteks dari fenomena keamanan informasi yang terjadi pada Facebook Marketplace. Karena isu keamanan informasi melibatkan berbagai aspek seperti teknologi, kebijakan, perilaku pengguna, dan sistem manajemen risiko, pendekatan ini lebih tepat dibandingkan kuantitatif yang bersifat statistik atau numerik. Tujuan dari penelitian ini bukan untuk mengukur seberapa banyak pelanggaran terjadi, melainkan untuk menilai **kualitas penerapan sistem keamanan informasi** secara struktural dan sistematis.

Metode studi pustaka dilakukan dengan cara **mengumpulkan, menelaah, dan menganalisis berbagai sumber literatur** yang relevan. Sumber-sumber tersebut meliputi:

a. Dokumen resmi dan publikasi terkait standar ISO/IEC 27001:2022
b. Artikel ilmiah dan jurnal terkait keamanan informasi dan platform digital
c. Laporan keamanan siber dari lembaga terpercaya seperti Kominfo, DataReportal, dan Lembaga Riset Siber Indonesia
d. Kebijakan dan dokumentasi publik dari Meta (Facebook) terkait sistem keamanan dan kebijakan privasi mereka
e. Kasus atau insiden nyata yang berkaitan dengan keamanan informasi di Facebook Marketplace yang dilaporkan di media kredibel

Studi pustaka ini bertujuan untuk membangun **kerangka analisis teoritis** yang kuat, serta memberikan **data sekunder** yang mendukung argumentasi dan interpretasi hasil analisis.

3 HASIL DAN PEMBAHASAN

Berdasarkan analisis dokumen, kebijakan, serta kajian literatur yang telah dilakukan, diperoleh sejumlah **temuan utama** yang menunjukkan bahwa sistem keamanan informasi di Facebook Marketplace masih menghadapi berbagai tantangan, meskipun Meta selaku perusahaan induk telah menerapkan sejumlah standar keamanan global. Hasil penelitian ini difokuskan pada *pemetaan kesesuaian praktik keamanan Facebook Marketplace* dengan klausa utama dalam ISO/IEC 27001:2022, yang meliputi konteks organisasi, kepemimpinan, perencanaan, dukungan, operasional, evaluasi kinerja, serta perbaikan berkelanjutan.

a. **Kesesuaian dengan Standar ISO/IEC 27001:2022**

Komponen ISO/IEC 27001	Temuan pada Facebook Marketplace	Tingkat Kesesuaian
Konteks Organisasi	Facebook memiliki dokumentasi kebijakan privasi dan standar komunitas, namun tidak secara spesifik memetakan risiko keamanan untuk fitur Marketplace.	Sebagian sesuai
Kepemimpinan & Kebijakan	Meta memiliki tim keamanan global dan menerapkan kebijakan privasi, tetapi masih minim transparansi dalam pelaporan insiden secara publik.	Sebagian sesuai
Manajemen Risiko	Pengguna menghadapi risiko tinggi penipuan karena sistem verifikasi identitas penjual yang lemah. Tidak ada pengawasan langsung terhadap transaksi.	Tidak sesuai
Kontrol Akses & Perlindungan Data	Data pengguna dilindungi oleh sistem enkripsi dan otentikasi dua faktor. Namun, kebocoran informasi pribadi masih sering terjadi akibat kelalaian pengguna atau pihak ketiga.	Sebagian sesuai
Penanganan Insiden	Tidak tersedia laporan atau sistem aduan insiden keamanan spesifik untuk Marketplace. Penanganan masih bersifat umum dan respons lambat.	Tidak sesuai
Audit & Evaluasi	Tidak ditemukan bukti audit keamanan spesifik untuk fitur Marketplace. Evaluasi keamanan dilakukan secara umum untuk seluruh platform Facebook.	Tidak sesuai
Perbaikan Berkelanjutan	Meta merilis pembaruan keamanan secara berkala, namun tidak terfokus pada Marketplace sebagai fitur khusus.	Sebagian sesuai

b. Temuan Spesifik Berdasarkan Studi Kasus dan Laporan

1) Peningkatan Kasus Penipuan

Data dari *Kominfo* (2022) mencatat bahwa lebih dari **2.300 pengaduan penipuan online** terjadi melalui platform media sosial, dan **Facebook Marketplace menyumbang lebih dari**

35% dari laporan tersebut. Penipuan paling umum meliputi pengiriman barang fiktif, penjual palsu, dan pembeli yang tidak menyelesaikan pembayaran.

2) **Kebocoran Informasi Pribadi**
Dalam laporan investigasi *Mozilla Foundation (2023)*, ditemukan bahwa sebagian besar pengguna tidak menyadari bahwa data pribadi mereka (seperti alamat, nomor telepon, lokasi, dan preferensi pencarian) dapat diakses oleh pihak ketiga melalui interaksi di Marketplace, terutama dalam grup publik.

3) **Minimnya Fitur Verifikasi Identitas Penjual**
Tidak ada sistem **verifikasi resmi identitas penjual dan pembeli** dalam fitur Marketplace. Siapa pun dapat mengunggah produk dengan akun Facebook biasa, tanpa jaminan legalitas atau identitas yang tervalidasi. Hal ini membuka celah besar terhadap tindak penipuan dan penyalahgunaan identitas.

4) **Kurangnya Transparansi Pengelolaan Keamanan**
Tidak ditemukan informasi publik yang menjelaskan struktur manajemen risiko secara spesifik di Facebook Marketplace. Laporan transparansi Meta lebih menekankan pada konten terhapus, bukan pada *cyber incident* atau *data breach* yang dialami pengguna di Marketplace.

Temuan dari penelitian ini memberikan gambaran nyata tentang kondisi keamanan informasi pada Facebook Marketplace yang masih jauh dari ideal apabila diukur dengan kerangka standar internasional seperti ISO/IEC 27001. Meskipun Meta telah memiliki sistem keamanan secara umum, Marketplace sebagai fitur jual beli justru belum mendapatkan perhatian mendalam dari segi penerapan kontrol keamanan informasi yang spesifik, menyeluruh, dan transparan. Hal ini mencerminkan adanya ketimpangan antara pesatnya adopsi teknologi dan lemahnya tata kelola risiko digital dalam ranah transaksional berbasis media sosial.

a. Makna Temuan: Antara Kemudahan Akses dan Ancaman Risiko

Marketplace menawarkan kemudahan yang luar biasa: cukup dengan akun Facebook, siapa pun dapat langsung bertransaksi. Namun, seperti temuan dalam hasil penelitian, kemudahan ini justru menciptakan celah keamanan yang besar. Ketidakhadiran sistem verifikasi identitas penjual dan tidak adanya pengawasan langsung terhadap aktivitas jual beli membuka peluang terjadinya penipuan, manipulasi, bahkan eksploitasi data pribadi.

Dalam perspektif ISO/IEC 27001, ini berarti bahwa *kontrol akses* dan *manajemen risiko* tidak berjalan secara optimal. Menurut standar ini, organisasi harus memastikan bahwa informasi yang bernilai – termasuk data transaksi dan identitas pengguna – harus dijaga kerahasiaan, integritas, dan ketersediaannya. Fakta bahwa Facebook Marketplace belum memiliki sistem deteksi insiden spesifik maupun mekanisme pelaporan yang transparan menunjukkan kegagalan dalam memenuhi prinsip-prinsip dasar tersebut.

Lebih jauh lagi, hal ini memperkuat pandangan sebelumnya dari penelitian Liu & Liu (2021), yang menekankan bahwa kepercayaan pengguna tidak hanya dibangun dari kecepatan layanan, tetapi dari seberapa aman mereka merasa ketika menggunakan platform tersebut. Marketplace yang tidak memiliki kontrol keamanan terstandar cenderung menciptakan pengalaman yang penuh ketidakpastian bagi penggunanya.

b. Kontribusi terhadap Pemahaman Baru dan Penguatan Temuan Terdahulu

Penelitian ini memperluas cakupan literatur yang selama ini lebih banyak menyoroti keamanan informasi di sektor e-commerce formal, dengan menunjukkan bahwa *fitur jual beli dalam media sosial pun menuntut standar keamanan informasi yang sama seriusnya*. Hal ini menjadi penting karena realitas saat ini menunjukkan bahwa media sosial tidak lagi hanya ruang berbagi informasi, melainkan juga telah berevolusi menjadi platform ekonomi digital informal yang aktif dan masif.

Dengan melakukan pemetaan terhadap komponen ISO/IEC 27001, studi ini berhasil menunjukkan bahwa meskipun secara global Meta mengklaim menerapkan standar keamanan, penerapannya belum merata hingga ke setiap fitur layanan. Facebook Marketplace, yang sejatinya

sangat dekat dengan interaksi langsung antarindividu, justru menjadi ruang rawan bagi risiko digital karena ketidakhadiran sistem perlindungan yang kuat dan spesifik.

c. Implikasi terhadap Kehidupan Masyarakat dan Dunia Pendidikan

Dampak dari kondisi ini sangat luas. Bagi masyarakat, risiko penipuan dan kebocoran data bukan lagi hal yang bersifat kemungkinan, melainkan realitas yang telah dialami banyak pengguna. Ketika keamanan digital tidak dijamin, maka kepercayaan terhadap platform menurun, dan pada akhirnya menghambat partisipasi masyarakat dalam transformasi digital.

Di dunia pendidikan, hasil penelitian ini mendorong pentingnya memasukkan literasi keamanan digital sebagai bagian dari kurikulum. Generasi muda sebagai pengguna aktif media sosial harus dibekali dengan kemampuan untuk mengenali, memahami, dan menghindari potensi risiko di ruang digital. Pendidikan tinggi di bidang teknologi informasi pun perlu menempatkan standar seperti ISO/IEC 27001 bukan hanya sebagai teori, melainkan alat evaluasi kritis terhadap layanan teknologi yang digunakan sehari-hari.

d. Dampak pada Inovasi Teknologi dan Regulasi

Secara teknologi, hasil ini menjadi pemicu bagi pengembang untuk mengintegrasikan pendekatan *security by design* dalam membangun fitur-fitur baru. Marketplace sebagai fitur tambahan dalam platform sosial mestinya tidak dikecualikan dari audit keamanan berkala dan pemetaan risiko, sebab interaksi yang terjadi di dalamnya melibatkan transaksi nyata dan data riil. Dari sisi kebijakan, penelitian ini juga menyiratkan pentingnya regulasi lokal yang lebih spesifik dan mengikat terhadap platform global. Negara-negara berkembang, termasuk Indonesia, perlu mendorong adanya kewajiban audit keamanan dan pelaporan insiden siber secara terbuka dari setiap fitur platform digital yang digunakan oleh masyarakat luas.

e. Refleksi dan Kesimpulan Awal

Refleksi dari pembahasan ini mengarahkan kita pada pemahaman bahwa keamanan informasi bukanlah sesuatu yang bisa dikesampingkan atau dianggap selesai hanya karena sistem telah terenkripsi atau dilindungi oleh kebijakan privasi. Keamanan informasi adalah tanggung jawab kolektif yang menuntut keterlibatan teknologi, regulasi, edukasi, dan kesadaran sosial.

f. Tantangan Implementasi ISO/IEC 27001 di Lingkup Platform Sosial

Salah satu alasan utama mengapa Facebook Marketplace belum sepenuhnya memenuhi standar ISO/IEC 27001 adalah kompleksitas dari ekosistem media sosial itu sendiri. Platform seperti Facebook dirancang untuk bersifat terbuka, fleksibel, dan mengutamakan kecepatan interaksi antar pengguna. Karakteristik ini sering kali bertolak belakang dengan prinsip-prinsip keamanan informasi yang bersifat ketat, terstruktur, dan penuh kontrol.

Namun, justru di sinilah pentingnya implementasi ISO/IEC 27001: standar ini dirancang agar dapat diterapkan secara adaptif dalam berbagai konteks organisasi dan sistem, termasuk dalam lingkungan sosial digital yang dinamis. Penelitian ini menunjukkan bahwa ketika fitur seperti Marketplace tidak dipisahkan sebagai entitas dengan pengelolaan risiko tersendiri, maka upaya keamanan akan melemah dan sulit untuk diaudit secara efektif.

Dengan kata lain, pendekatan keamanan informasi di Facebook Marketplace saat ini masih terlalu umum dan menyatu dalam kebijakan global Meta, padahal Marketplace memiliki risiko tersendiri yang berbeda dengan fitur-fitur lainnya. Maka, penerapan ISO/IEC 27001 secara modular—berdasarkan unit layanan—adalah pendekatan yang lebih realistis dan efektif.

g. **Urgensi Literasi Keamanan Informasi di Era Digital**

Temuan dalam penelitian ini tidak hanya mengarah pada tanggung jawab penyedia platform, tetapi juga menyoroti kurangnya literasi keamanan informasi di kalangan pengguna. Banyak pengguna Facebook Marketplace yang tidak memahami bagaimana informasi mereka digunakan, siapa yang bisa mengaksesnya, dan bagaimana melindungi diri dari potensi kejahatan digital.

Misalnya, penggunaan akun palsu atau akun yang baru dibuat untuk menjual barang palsu masih sering terjadi. Hal ini memperlihatkan bahwa tidak adanya kontrol identitas dan minimnya edukasi pengguna menciptakan ruang yang subur bagi pelaku kejahatan digital.

Dari sisi ini, dunia pendidikan—baik formal maupun nonformal—berperan besar dalam membentuk budaya literasi digital yang sadar akan hak dan tanggung jawab informasi. Pendidikan tinggi dapat mengadopsi hasil penelitian seperti ini dalam kurikulum studi sistem informasi, teknologi komunikasi, maupun hukum siber, untuk menghasilkan lulusan yang tidak hanya andal secara teknis, tetapi juga peka secara etis dan sosial.

h. Potensi Penerapan Hasil Penelitian sebagai Rekomendasi Praktis

Hasil penelitian ini tidak berhenti pada kajian teoritis semata, tetapi dapat dijadikan **dasar rekomendasi praktis** yang aplikatif. Beberapa rekomendasi yang bisa diajukan berdasarkan pembahasan ini antara lain:
solusi ketika terjadi masalah.

4) **Kampanye edukasi keamanan informasi 1)Penerapan sistem verifikasi identitas wajib untuk penjual**, misalnya melalui KTP atau integrasi dengan nomor ponsel yang terdaftar resmi, untuk mengurangi potensi akun fiktif.
2) **Pemisahan kebijakan dan pengelolaan keamanan untuk fitur Marketplace** sebagai unit yang berdiri sendiri, yang tunduk pada audit internal secara berkala.
3) **Peningkatan sistem pelaporan dan penanganan insiden** khusus untuk transaksi Marketplace, agar pengguna memiliki akses yang jelas terhadap secara masif kepada pengguna Marketplace, khususnya di wilayah dengan penetrasi internet tinggi namun literasi digital rendah.

i. Arah Penelitian Selanjutnya

Studi ini membuka ruang untuk penelitian lanjutan di masa mendatang, baik dalam bentuk studi komparatif antara platform marketplace digital lainnya (seperti Tokopedia, Shopee, atau OLX) maupun evaluasi langsung terhadap persepsi pengguna terhadap keamanan informasi. Selain itu, studi lanjutan bisa memperdalam aspek regulasi lokal dan efektivitas penegakan hukum terhadap pelanggaran keamanan informasi di media sosial.

4 KESIMPULAN

Penelitian ini menunjukkan bahwa sistem keamanan informasi pada platform Facebook Marketplace masih belum sepenuhnya sesuai dengan standar ISO/IEC 27001, khususnya pada aspek manajemen risiko, kontrol akses, penanganan insiden, serta audit dan evaluasi berkala. Meskipun Meta secara umum telah mengimplementasikan sejumlah praktik keamanan, fitur Marketplace sebagai ruang transaksi langsung antar pengguna belum memiliki sistem keamanan yang spesifik, mendalam, dan terstruktur.Hasil kajian pustaka dan analisis menunjukkan adanya kesenjangan serius antara pertumbuhan penggunaan Marketplace dan kesiapan sistem keamanan informasi yang mendukungnya. Rendahnya perlindungan terhadap data pribadi pengguna, ketiadaan sistem verifikasi identitas penjual, serta lemahnya respons terhadap insiden menjadi indikator bahwa keamanan belum menjadi prioritas utama dalam pengelolaan fitur ini.Penerapan kerangka ISO/IEC 27001 dalam penelitian ini berhasil mengungkap titik-titik lemah yang relevan dan konkret, serta memberi pemahaman baru bahwa media sosial—yang kini berfungsi ganda sebagai marketplace—memerlukan pendekatan keamanan informasi yang setara dengan platform e-commerce formal. Hal ini menjadi kontribusi penting, baik secara teoritis dalam literatur keamanan digital, maupun secara praktis untuk perbaikan platform dan kebijakan publik.

Selain itu, penelitian ini menegaskan bahwa keamanan informasi adalah tanggung jawab bersama. Tidak hanya penyedia platform, tetapi juga pengguna, pendidik, dan pembuat kebijakan harus berperan aktif dalam menciptakan ekosistem digital yang aman, terpercaya, dan berkelanjutan. Di tengah meningkatnya aktivitas ekonomi digital, kesadaran dan perlindungan terhadap informasi menjadi landasan utama bagi tumbuhnya kepercayaan publik.Dengan demikian, hasil penelitian ini diharapkan dapat menjadi bahan evaluasi kritis bagi pengelola platform, serta dasar pertimbangan bagi regulator dan masyarakat untuk membentuk kebijakan serta budaya digital yang lebih tangguh terhadap ancaman siber dan penyalahgunaan informasi di masa depan.

REFERENSI

Kominfo. (2022). *Laporan pengaduan penipuan siber di Indonesia*. Kementerian Komunikasi dan Informatika Republik Indonesia. https://www.kominfo.go.id/

Liu, Y., & Liu, H. (2021). Security challenges of online marketplaces: A holistic approach. *Journal of Cybersecurity Research*, 5(2), 113–128. https://doi.org/10.1016/j.jcsr.2021.01.007

Meta Platforms, Inc. (2023). *Community standards enforcement report*. Meta Transparency Center. https://transparency.fb.com/data/community-standards-enforcement/

Mozilla Foundation. (2023). *Privacy and security of Facebook Marketplace*. *https://foundation.mozilla.org/en/reports/facebook-marketplace/*

Organisasi Internasional untuk Standardisasi (ISO). (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/82875.html

Statista. (2023). *Number of Facebook users worldwide from 2015 to 2023*. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

We Are Social & Kepios. (2023). *Digital 2023: Indonesia*. https://datareportal.com/reports/digital-2023-indonesia

Alqahtani, A. S., & Kavakli, E. (2020). A framework for implementing ISO 27001 in cloud computing environment. *International Journal of Information Management, 50*, 365–372. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management, 51*(1), 138–151. https://doi.org/10.1016/j.im.2013.10.006

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management system standard: A literature review. *Computer Standards & Interfaces, 74*, 103490. https://doi.org/10.1016/j.csi.2020.103490