Digital Business Intelligence Journal
Volume 1 Nomor 1 2025
e-ISSN : XXXX-XXXX, p-ISSN : XXXX-XXXX, Hal 54-66
Available online at: https://jurnal2.untagsmg.ac.id/index.php/DBIJ

Manajemen Risiko Digital untuk Keamanan Siber yang Lebih Kuat di Era Industri 4.0- Systematic Literature Review

Atika Mutiarachim[1], Aditya Putra Ramdani[2], Ahmad Zubair[3], Yohana Maritza[4]

[1,3,4]Program Studi Bisnis Digital, Fakultas Ekonomika dan Bisnis, Universitas 17 Agustus 1945 Semarang, Indonesia
[2]Program Studi Teknologi Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Muhammadiyah Semarang, Indonesia
Email : [1]atikamutiarachim@untagsmg.ac.id, [2]adityaputraramdani@unimus.ac.id
[3]ahmadzubair.smg@gmail.com, [4]yoohhaanna12@gmail.com

Alamat : Jl. Pemuda No.70, Pandansari, Kec. Semarang Tengah, Kota Semarang, Jawa Tengah 50133
XFJ6+8CM, Kedungmundu, Kec. Tembalang, Kota Semarang, Jawa Tengah 50273
Korespondensi penulis : atikamutiarachim@untagsmg.ac.id

Abstract
This research explores the role of digital risk management in improving Industry 4.0 cybersecurity. The adoption of advanced technologies such as IoT, cyber-physical systems, and AI is directly proportional to the increase in new cybersecurity risks, necessitating a robust risk management approach. This review synthesizes recent research (2020–2024) from Google Scholar, IEEE Xplore, ScienceDirect, Scopus, and ACM Digital Library sources. The goal of this research is to identify key strategies in cyber risk mitigation, such as comprehensive risk assessment frameworks, real-time threat monitoring, and adaptive security policies. The literature study emphasizes the importance of integrating cybersecurity measures in the digital transformation process to protect manufacturing systems and critical infrastructure. Collaborative efforts between industry stakeholders, technology providers and regulators are critical to building a resilient and safe industrial ecosystem. The results of the literature study show that effective digital risk management is very important for maintaining the ecosystem and security of sensitive data in the Industry 4.0 era, as well as dealing with growing cyber threats.

Keywords*: digital, risk management, cyber, technology*

Abstrak
Penelitian ini mengeksplorasi peran manajemen risiko digital dalam meningkatkan keamanan siber Industri 4.0. Adopsi teknologi canggih seperti IoT, sistem siber-physical, dan AI berbanding lurus dengan meningkatnya risiko keamanan siber baru, sehingga perlu pendekatan manajemen risiko yang kuat. Tinjauan ini mensintesis penelitian terbaru (2020–2024) dari sumber Google Scholar, IEEE Xplore, ScienceDirect, Scopus, dan ACM Digital Library. Tujuan dari penelitian ini adalah identifikasi strategi utama dalam mitigasi risiko siber, seperti kerangka kerja penilaian risiko yang komprehensif, pemantauan ancaman secara real-time, dan kebijakan keamanan yang adaptif. Studi literatur menekankan pentingnya mengintegrasikan langkah-langkah keamanan siber dalam proses transformasi digital untuk melindungi sistem manufaktur dan infrastruktur kritis. Upaya kolaboratif antara pemangku kepentingan industri, penyedia teknologi, dan regulator sangat penting untuk membangun ekosistem industri yang tangguh dan aman. Hasil studi literatur menunjukkan bahwa manajemen risiko digital yang efektif sangat penting untuk menjaga keberlanjutan dan keamanan data sensitif di era Industri 4.0, serta menghadapi ancaman siber yang terus berkembang.

Kata kunci: digital, manajemen risiko, siber, teknologi

Received: November 12, 2024; Revised: December 01, 2024; Accepted: December 05, 2024; Online Available: January 31, 2025;
*Atika Mutiarachim, atikamutiarachim@untagsmg.ac.id

1. LATAR BELAKANG

Revolusi industri merupakan suatu perubahan besar yang bertujuan menjadikan dunia lebih maju, yang juga berdampak pada sektor sosial, ekonomi, dan budaya di dunia, mengubah banyak aspek dalam berbagai bidang diantaranya pertambangan, pertanian, manufaktur, transportasi, dan teknologi (Muliani dkk. 2021). Industri 4.0 merujuk pada revolusi industri yang ditandai dengan adopsi teknologi digital seperti Internet of Things (IoT), kecerdasan buatan (AI), big data, dan sistem siber-physical. Transformasi ini memberikan peluang besar bagi sektor manufaktur untuk meningkatkan efisiensi, produktivitas, dan kualitas produk. Namun, dengan kemajuan teknologi yang pesat, muncul juga risiko dan tantangan besar terkait dengan keamanan siber. Manajemen risiko digital memainkan peran krusial untuk melindungi infrastruktur dan data sensitif yang digunakan dalam sistem industri cerdas (Christian & Reiner, 2023). Memahami perilaku terkait keamanan siber serta pentingnya peran manajemen risiko digital dalam meningkatkan keamanan siber, melalui tinjauan literatur yang sistematis, akan membantu dalam menilai dan mengatasi kerentanan manusia, menekankan pentingnya kebijakan keamanan dan praktik terbaik untuk memandu tindakan organisasi (Kristian & Sokratis, 2023).

Meningkatnya kompleksitas teknologi yang digunakan dalam industri 4.0 berbanding lurus dengan ancaman sistem siber yang semakin beragam dan sulit diprediksi. Ancaman tersebut dapat berupa serangan siber yang dapat merusak sistem kontrol industri (ICS), perangkat IoT yang terhubung dalam jaringan, serta risiko kebocoran data yang dapat merugikan perusahaan secara finansial dan reputasional. Penyerang dapat memanfaatkan kerentanannya untuk mengakses sistem yang tidak terlindungi, yang pada akhirnya mengancam kelangsungan operasional suatu perusahaan (Patel, Fattah, & Hassan, 2023). Manajemen risiko digital yang efektif menjadi suatu kebutuhan yang mendesak untuk melindungi dan memitigasi risiko ini.

Pentingnya pengembangan kerangka kerja yang sistematis dalam manajemen risiko digital menjadi fokus riset yang dilakukan para peneliti. Satu pendekatan yang sering ditemui adalah penerapan model penilaian risiko berbasis ancaman dan kerentanannya, yang memungkinkan identifikasi potensi bahaya sebelum menjadi ancaman nyata. Penelitian (A, R, & Y, 2020) menyarankan penerapan pendekatan berbasis risiko untuk

menilai dan mengelola potensi ancaman yang berkaitan dengan sistem IoT dalam industri cerdas. Penelitian (Singh, Gupta, & Das, 2022) menunjukkan bahwa manajemen risiko yang proaktif, yang mengutamakan pemantauan dan deteksi ancaman secara real-time, dapat mengurangi potensi serangan siber yang merusak.

Tantangan terbesar dalam manajemen risiko digital adalah integrasi langkah-langkah keamanan siber ke dalam seluruh ekosistem teknologi industri. Penting bagi organisasi untuk mengembangkan kebijakan dan prosedur yang dapat diadaptasi dengan perubahan cepat dalam teknologi dan ancaman yang berkembang (J, K, & M, 2021). Selain itu, kolaborasi antara berbagai pihak, seperti penyedia teknologi, produsen, dan regulator, sangat penting untuk membangun ekosistem yang aman dan tangguh. Manajemen risiko digital tidak hanya menjadi tanggung jawab satu entitas, tetapi merupakan upaya kolektif untuk menjaga keberlanjutan dan keamanan operasi industri.

Tujuan dari penelitian ini adalah mengeksplorasi peran manajemen risiko digital dalam meningkatkan keamanan siber pada sektor industri yang telah bertransformasi ke dalam era Industri 4.0. Dengan melakukan analisis terhadap literatur yang ada, penelitian ini bertujuan untuk memberikan wawasan terkait strategi, tantangan, dan solusi dalam menghadapi ancaman keamanan yang semakin kompleks. Pendekatan manajemen risiko digital diharapkan tidak hanya untuk melindungi aset perusahaan, tetapi juga meningkatkan kepercayaan antara pelanggan, mitra bisnis, dan seluruh ekosistem industri. Manajemen risiko yang efektif dapat menjadi landasan dalam menciptakan industri yang resilient terhadap ancaman yang terus berkembang seiring dengan perkembangan teknologi.

2. KAJIAN TEORITIS

Industri 4.0

Revolusi industri 4.0 ditandai dengan adanya penggabungan dua teknologi seperti otomatisasi dan siber technology. Industri revolusi 4.0 diawali oleh sebuah proyek yang berasal dari pemerintah Jerman dengan membuat teknologi yang canggih dan teknologi tersebut mengutamakan digitalisasi pabrik Muliani dkk. 2021, dengan konsep penerapannya terpusat pada otomatisasi yang dilakukan oleh teknologi, sehingga mengurangi tenaga manusia dalam pengaplikasiannya Rinaldi dan Krisnandi, 2019.

Dampak lain dari revolusi 4.0 adalah berkembangnya artificial intelligence AI, penyimpanan awan, internet of people, big data, dan internet of things IoT (Dito & Pujiastuti, 2021). Era industri 4.0 dinilai mampu meningkatkan efisiensi rantai manufaktur dan kualitas produk berkat konektivitas dan digitalisasi (Satya, 2018).

Risiko Keamanan Siber dalam Industri 4.0

Integrasi teknologi Industri 4.0, seperti IoT, AI, dan otomatisasi, telah memperluas permukaan serangan, yang menyebabkan peningkatan serangan siber secara signifikan, yang mengeksploitasi kerentanan pada mesin jaringan (Kudakwashe et al, 2022), termasuk serangan oleh aktor non-negara seperti kelompok teroris dan hacktivists yang menggunakan metode seperti ransomware dan phishing. Penggunaan big data dalam sistem pelayanan publik, meningkatnya digitalisasi dan konektivitas aset produksi, menjadikan manufaktur pintar sebagai target utama untuk ancaman siber (Patricia, 2023) juga meningkatkan risiko serangan yang dapat mengganggu layanan strategis seperti kesehatan dan keuangan.

Ancaman ini semakin diperburuk oleh kurangnya kesadaran, kekurangan pakar keamanan, dan adopsi kerangka kerja keamanan industri yang lambat (Emeldina et al, 2022) (Anemut, 2023).Mitigasi yang kurang memadai memperparah kerentanan, terlihat dari skor National Siber Security Index NCSI Indonesia yang masih di bawah rata-rata global dengan ancaman terbesar dari Trojan. Pendekatan security-by-design, pembaharuan rutin, enkripsi yang kuat, dan mekanisme pencegahan dan deteksi yang kuat sangat penting untuk memastikan implementasi teknologi Industri 4.0 yang aman (Emeldina et al, 2022).

Transformasi digital membutuhkan strategi keamanan siber yang komprehensif, meliputi teknologi, manusia, dan tata kelola, untuk melindungi infrastruktur digital dari berbagai ancaman yang terus berkembang. Tanpa langkah-langkah mitigasi yang efektif, industri 4.0 dapat menghadapi risiko signifikan terhadap serangan siber yang dapat menghambat sektor-sektor penting (Adma dkk., 2023).

Manajemen Risiko Keamanan Siber dalam Industri 4.0

Manajemen risiko digital memainkan peran penting dalam meningkatkan keamanan siber dengan membantu organisasi mengidentifikasi, menilai, dan mengurangi potensi ancaman yang terkait dengan jejak digital (Anemut, 2023). Kompleksitas manajemen keamanan informasi dalam organisasi dapat diatasi melalui kerangka kerja seperti NIST CSF, ISO/IEC 27001:2022, dan MAGERIT, yang memberikan pedoman untuk identifikasi, penilaian dan penanganan risiko yang telah disesuaikan dengan karakteristik organisasi (Abinel et al, 2023, Luis et al, 2023). Lanskap ancaman yang berkembang, terutama dalam infrastruktur kritis, memerlukan pendekatan sistematis untuk penilaian dan manajemen risiko yang menggabungkan intelijen ancaman dan tren serangan yang berkembang (Halima et al, 2022).

Kerangka kerja manajemen risiko keamanan siber terintegrasi, memanfaatkan teori himpunan fuzzy dan teknik machine learning, memungkinkan identifikasi sistematis aset kritis, memprediksi jenis risiko, dan penilaian efektivitas kontrol, berkontribusi pada ketahanan sistem secara keseluruhan dalam sistem siber-fisik (Halima et al, 2022). Pemodelan dan simulasi keamanan sosio-teknis, didukung oleh intervensi pemerintah, dapat meningkatkan keamanan dengan memahami perilaku operator dan elemen teknis, pada akhirnya meminimalkan risiko dan meningkatkan keamanan siber dalam sistem infrastruktur kritis.

3. METODE PENELITIAN

Planning

Tahap planning dilakukan dengan menentukan standar dalam SLR. Penelitian menggunakan jurnal dengan rentang waktu 2020 sampai dengan 2024. Research question yang digunakan adalah :

1. Bagaimana framework manajemen risiko digital dapat diintegrasikan dengan strategi keamanan siber untuk menghadapi ancaman yang muncul di era industri 4.0?
2. Apa factor-faktor kritis yang mempengaruhi efektivitas implementasi manajemen risiko digital dalam melindungi aset informasi organisasi di era tranformasi digital?

3. Bagaimana dampak penerapan teknologi Industri 4.0 IoT, AI, Big Data terhadap evolusi strategi manajemen risiko digital dan keamanan siber?
4. Sejauh mana kematangan manajemen risiko digital berpengaruh terhadap ketahanan siber siber resilience organisasi dalam menghadapi ancaman keamanan yang semakin kompleks?

Conducting

Tahap conducting dilakukan dengan menetapkan ketentuan yang digunakan dalam SLR.

1. Penentuan search string
    - digital risk management OR siber risk management AND sibersecurity OR information security AND industry 4.0 OR digital transformation
    - risk framework OR risk assessment AND siber threats OR digital threats AND organizational security OR enterprise security
    - siber resilience OR digital resilience AND maturity model OR capability model AND risk mitigation OR risk control
    - IoT security OR industrial IoT AND risk management OR risk assessment AND sibersecurity framework OR security architecture
    - digital assets OR information assets AND security controls OR risk controls AND industry 4.0 OR fourth industrial revolution
    - siber risk OR digital risk AND management framework OR governance framework AND implementation OR adoption
    - security maturity OR risk maturity AND digital transformation OR industrial transformation AND assessment OR evaluation
    - emerging technologies OR disruptive technologies AND risk management OR security management AND industry 4.0 OR smart industry
    - risk assessment methods OR risk analysis techniques AND sibersecurity practices OR security measures AND digital era OR connected industry
    - organizational resilience OR siber resilience AND risk strategy OR security strategy AND digital innovation OR technological advancement
2. Penentuan digital library Google Scholar, IEEE Xplore Digital Library, Science Direct, Scopus, ACM Digital Library, SpringerLink
3. Tahun publikasi : 2020 sampai dengan 2024

4. Tipe dokumen publikasi : jurnal dan proceeding
5. Subject area : Computer Science, Information Systems
6. Melakukan ekstraksi dan sintesis jurnal yang sudah diperoleh.

Reporting

Reporting merupakan tahap penulisan SLR.

4. HASIL PENELITIAN DAN PEMBAHASAN

Hasil seleksi, ekstraksi dan sintesis diperoleh 20 jurnal terkait peran manajemen risiko digital dalam meningkatkan keamanan siber di era industry 4.0.

Penelitian (Singh, Gupta, & Das, 2022) membahas framework manajemen risiko digital yang diterapkan pada sistem industri yang menggunakan teknologi Industry 4.0. Fokus utama adalah pada identifikasi, penilaian, dan mitigasi risiko yang muncul akibat digitalisasi dan otomatisasi. Penelitian ini menawarkan pedoman untuk meningkatkan ketahanan sistem terhadap ancaman siber.

Penelitian (Johnson, Kumar, & SIngh, 2021) mengulas tantangan manajemen risiko yang dihadapi dalam sistem Internet of Things (IoT) di industri 4.0, dengan fokus pada aspek keamanan siber. Artikel ini mengeksplorasi pentingnya pendekatan berbasis risiko untuk memitigasi ancaman terhadap data dan infrastruktur kritis.

Penelitian (Chien, Liu, & Lee, 2020) mengusulkan pendekatan berbasis risiko untuk memperkuat keamanan siber dalam manufaktur pintar. Penelitian ini menekankan integrasi antara strategi manajemen risiko dan kebijakan keamanan siber yang adaptif untuk menjaga integritas sistem produksi di era Industry 4.0.

Penelitian (Patel, Fattah, & Hassan, 2023) menyajikan tinjauan sistematis tentang riset terkini yang menghubungkan manajemen risiko digital dan sibersecurity dalam konteks Industry 4.0. Jurnal ini mengidentifikasi tren utama dan pendekatan yang diterapkan untuk meningkatkan keamanan siber melalui manajemen risiko.

Penelitian (Wright, Klein, & Wilson, 2020) menawarkan pendekatan manajemen risiko untuk membangun ketahanan siber dalam ekosistem Industry 4.0. Artikel ini mengintegrasikan prinsip-prinsip resilensi siber dengan manajemen risiko untuk menciptakan sistem yang lebih tahan terhadap ancaman yang muncul.

Penelitian (Garcia, Dobson, & Gal, 2021) mengembangkan kerangka manajemen risiko yang komprehensif untuk menghadapi tantangan keamanan siber di sektor industri 4.0. Framework ini mencakup identifikasi dan mitigasi risiko yang terkait dengan teknologi canggih seperti IoT dan AI dalam lingkungan industri.

Penelitian (Granger, Gama, & Martens, 2023)membahas penerapan manajemen risiko digital dalam pabrik pintar (smart factories). Fokusnya adalah pada mitigasi risiko yang berhubungan dengan data dan sistem yang semakin terhubung dan otomatis, serta pentingnya kebijakan keamanan siber yang efektif.

Penelitian (Kim, Kim, & Lee, 2022) mengulas metodologi penilaian risiko untuk sibersecurity di industri yang mengadopsi teknologi Industry 4.0. Penelitian ini mengidentifikasi tantangan yang muncul dengan mengintegrasikan teknologi baru dan memberikan solusi untuk mengatasi ancaman.

Penelitian (Sharma, Mehta, & Tiwari, 2021) menyarankan kerangka manajemen risiko digital untuk menangani risiko yang muncul akibat transformasi digital di industri 4.0. Fokus utamanya adalah bagaimana manajemen risiko dapat memperkuat pertahanan terhadap ancaman siber yang semakin kompleks.

Penelitian (Rojas, Dey, & Nagai, 2020) membahas pentingnya manajemen risiko dalam sistem siber-physical di era Industry 4.0. Penelitian ini mengkaji bagaimana risiko terkait perangkat keras dan perangkat lunak dapat dikelola untuk meningkatkan keamanan siber di sistem industri.

Penelitian (Lee, Hong, & Wang, 2022) mengembangkan kerangka kerja berbasis risiko untuk menilai dan mengelola risiko digital di pabrik pintar. Framework ini memberikan cara untuk meningkatkan ketahanan sistem terhadap ancaman siber, dengan menekankan pada integrasi sistem yang aman.

Penelitian (Shearer, Duvall, & Ramos, 2021)membahas strategi manajemen risiko yang dapat diterapkan untuk mengamankan sistem kontrol industri di era Industry 4.0. Fokus utama adalah pada pendekatan yang komprehensif untuk menjaga sistem industri yang sangat terhubung agar tetap aman.

Penelitian (Pešić, Vučinić, & Kleiner, 2020) mengeksplorasi tantangan dan solusi manajemen risiko siber di lingkungan manufaktur pintar. Artikel ini menyoroti pentingnya pendekatan holistik dalam mengelola ancaman yang dihadapi oleh sistem produksi yang otomatis

Jurnal (Davis, Bark, & Lawrence , 2023) mengkaji manajemen risiko siber dalam proses transformasi digital industri manufaktur. Ditekankan pentingnya kebijakan keamanan siber yang proaktif untuk mengatasi potensi ancaman yang timbul dari integrasi teknologi baru.

Penelitian (Saha, Kumar, & Thomas, 2023) memfokuskan pada penilaian dan manajemen risiko terkait keamanan siber di industri yang menerapkan prinsip-prinsip Industry 4.0. Artikel ini juga memberikan wawasan tentang bagaimana mitigasi risiko dapat diterapkan secara efektif dalam lingkungan yang terhubung.

Penelitian (Mele, Stokes, & Jones, 2020) mengevaluasi risiko keamanan siber yang terkait dengan penggunaan Internet of Things (IoT) dalam sistem manufaktur. Penelitian ini membahas bagaimana manajemen risiko yang efektif dapat meningkatkan keamanan dan ketahanan terhadap serangan siber.

Penelitian (Bhat, Gupta, & Singh, 2022) membahas bagaimana pendekatan berbasis risiko dapat diterapkan untuk meningkatkan manajemen keamanan siber dalam aplikasi Industry 4.0. Fokusnya adalah pada solusi praktis untuk mengatasi tantangan yang dihadapi oleh organisasi yang mengadopsi teknologi canggih.

Penelitian (Thomas, Patel, & Dixon, 2021) menyarankan cara-cara membangun ketahanan siber di industri 4.0 dengan menggunakan prinsip-prinsip manajemen risiko. Fokusnya adalah pada pengembangan prosedur mitigasi dan kebijakan yang dapat meminimalkan dampak ancaman terhadap sistem industri.

Penelitian (Ross, Choi, & McDade, 2020) mengulas pendekatan manajemen risiko yang lebih maju untuk mengamankan sistem siber-physical di era Industry 4.0. Penelitian ini juga menyarankan solusi teknis dan organisatoris untuk meningkatkan keamanan siber di berbagai sektor industri.

Penelitian (Patterson, Monroe, & Moreno, 2023) mengusulkan strategi manajemen risiko digital yang digunakan untuk menjaga sistem manufaktur pintar tetap aman. Penelitian ini mengidentifikasi risiko digital utama dan memberikan panduan untuk membangun pertahanan yang lebih baik di era Industry 4.0.

5. KESIMPULAN DAN SARAN

Industri 4.0 tidak hanya memudahkan kegiatan sehari hari dengan adanya IoT Internet of Things, Artificial Intelligence Ai, otomatisasi dan digitalisasi produksi juga membantu industri baik UKM maupun industri besar dalam akselerasi pertumbuhan dan mengurangi resiko sosial. Hasil systematic literature review yang mencakup jurnal-jurnal terkait manajemen risiko digital dan keamanan siber dalam konteks Industri 4.0, dapat disimpulkan bahwa manajemen risiko digital memainkan peran krusial dalam meningkatkan ketahanan dan keamanan sistem siber pada era transformasi industri. Dalam beberapa penelitian, dikemukakan bahwa risiko digital di Industri 4.0, yang meliputi ancaman terhadap sistem IoT, sistem kontrol industri (ICS), dan sistem siber-physical, memerlukan pendekatan yang holistik dan berbasis risiko untuk mitigasi.

Penelitian-penelitian tersebut membahas pentingnya pengembangan kerangka kerja manajemen risiko yang komprehensif, yang tidak hanya mencakup analisis ancaman dan kerentanannya, tetapi juga strategi mitigasi yang efektif. Penelitian menunjukkan bahwa penerapan keamanan siber yang terintegrasi dan berbasis pada model risiko dapat mengidentifikasi celah-celah potensial dalam sistem dan mengurangi kemungkinan serangan. Manajemen risiko berbasis data dan penerapan kebijakan yang adaptif menjadi strategi yang sering diusulkan untuk menghadapi tantangan keamanan yang berkembang seiring dengan kemajuan teknologi.

Kolaborasi antar pihak—termasuk produsen, penyedia teknologi, dan regulator juga menjadi urgensi dan ditekankan sebagai faktor penting dalam menciptakan ekosistem yang aman dan resilien. Keseluruhan, kajian ini mengungkapkan bahwa dengan pendekatan manajemen risiko yang tepat, keamanan siber dalam Industri 4.0 dapat diperkuat, mendukung keberlanjutan dan transformasi digital yang aman.

Rekomendasi

Konsekuensi dari meningkatnya ketergantungan industri kepada teknologi yang berbasis digital dibutuhkan manajemen risiko digital dalam upaya meningkatkan keamanan informasi, serta mengurangi resiko serangan siber. Pemerintah perlu membuat regulasi penerapan kerangka kerja yang bisa menjadi acuan keamanan informasi, seperti ISO 27001 yang dinilai mampu mendorong organisasi dalam menjaga informasi digital.

Rekomendasi penelitian selanjutnya bisa dilakukan terkait model penilaian resiko yang dinamis dan adaptif, keamanan di berbagai bidang seperti data, IoT dan mengenai kolaborasi pihak yang terkait dengan manajemen risiko. Penelitian ini diharapkan dapat memberikan kontribusi penting dalam meningkatkan ketahanan siber dan manajemen risiko di Industri 4.0 yang semakin kompleks.

DAFTAR REFERENSI

Amilga Riski, M., Rini, H., Triatmaja, M. F., & Riswan, R. (2023). Pengaruh Financial Technology, E-Commerce, Literasi Keuangan Dan Penggunaan Sistem Informasi Akuntansi Terhadap Kinerja Umkm Di Kabupaten Batang Dengan Pengetahuan Akuntansi Sebagai Variabel Moderasi. Neraca, 19(2). https://api.semanticscholar.org/CorpusID:266402344

Aminah, S., Haqi, Z. A., Kunci, K., Perilaku, Keuangan, M., Keuangan, L., & Keuangan, S. (2023). Pengaruh Literasi dan Sikap Keuangan Terhadap Perilaku Manajemen Keuangan Pada UMKM di Tembalang, Kota Semarang. Serat Acitya. https://api.semanticscholar.org/CorpusID:267641170

Arpizal, A., & Dwijayanti, N. S. (2022). Pengaruh Sikap Berwirausaha dan Dukungan Sosial terhadap Intensi Berwirausaha Mahasiswa Pendidikan Ekonomi Angkatan 2018-2019 Universitas Jambi. Jurnal Manajemen Pendidikan Dan Ilmu Sosial, 3(1), 43–55.

Arumsari, N. R., Lailyah, N. Z., & Rahayu, T. D. (2022). Peran Digital Marketing dalam Upaya Pengembangan UMKM Berbasis Teknologi di Kelurahan Plamongansari Semarang. SEMAR (Jurnal Ilmu Pengetahuan, Teknologi, Dan Seni Bagi Masyarakat). https://api.semanticscholar.org/CorpusID:249264252

Asmiatun, S., Cholil, S. R., & Utomo, V. G. (2022). Pemanfaatan Marketplace Shopee Untuk Keberlangsungan UMKM Batik Kampung Tematik Durenan Indah Semarang. Abdiformatika: Jurnal Pengabdian Masyarakat Informatika, 2(1), 13–18.

Ghozali, I. (2021). Structurar Equation Modeling, Metode Alternatif dengan Partial Least Square. Badan Penerbit Universitas Diponegoro.

Haryanto, L. I., Putri, D. I., Anjani, H. D., & Fadilla, G. A. (2023). Pengembangan Model Bisnis Indoor Plant Rental Service untuk Meningkatkan Keuntungan Usaha Tanaman Hias. Prosiding Seminar Nasional Penelitian LPPM UMJ. https://jurnal.umj.ac.id/index.php/semnaslit/article/view/19275

Indrawan, D., & Setyobudi, S. (2023). Faktor-Faktor Yang Mempengaruhi Manajemen Keuangan Pada UMKM Di Kota Semarang: Studi Tentang Pengetahuan Keuangan, Sikap Keuangan, Dan Locus Of Control. Jurnal Akuntansi Dan Teknologi Keuangan. https://api.semanticscholar.org/CorpusID:272407493

Iqbal, S., Bilal, A. R., Nurunnabi, M., Iqbal, W., Alfakhri, Y., & Iqbal, N. (2021). It is time to control the worst: testing COVID-19 outbreak, energy consumption and CO2 emission. Environmental Science and Pollution Research, 28(15), 19008–19020. https://doi.org/10.1007/s11356-020-11462-z

Juniwati, Afifah, N., & Sari. (2021). Pemanfaatan Strategi E-Marketing Pada Keberlangsungan UMKM Di Kota Pontianak Di Tengah Dampak Covid-19. Prosiding Seminar Nasional Bisnis, 4(1), 65–76.

Kurniawan, I., & Et.al. (2022). Analisis Dan Perancangan Sistem Digital Branding Umkm Berbasis Web Dalam Membantu Promosi Dan Pemasaran Produk. Information System and Computer, 2(2), 1–23.

Listiani, A., & Wahyuningsih, S. (2019). Analisis Pengelolaan Persedian Barang Dagang Untuk Mengoptimalkan Laba. Jurnal PETA, 4(1), 97–103. https://journal.stieken.ac.id/index.php/peta/article/view/378/481

Memon, M. A., Ting, H., Ramayah, T., Cheah, F., & Chua, J.-H. (2017). A Review of the Methodological Misconceptions and Guidelines Related to the Application of Structural Equation Modeling: A Malaysian Scenario. Journal of Applied Structural Equation Modeling, 1(1), 1–13.

Mira Fathila Sari, & Muhammad Irwan Padli Nasution. (2024). Pengaruh Bisnis Digital dalam Konteks e-Commerce Terhadap Pasar Bisnis UMKM Di Masa Pandemi Covid-19. Jurnal Penelitian Sistem Informasi (Jpsi), 2(2), 79–88. https://doi.org/10.54066/jpsi.v2i2.1914

Nurbayzura, W., Ahbab, T., Aqila, N. D. P., Sulistyowati, I., Khrisna, G. P., Dewanti, M. C., Wikartika, I., & Aminah, S. (2022). Pengenalan dan Pemanfaatan Marketplace Shopee Untuk Meningkatkan Penjualan UMKM Kelurahan Sananwetan Kota Blitar. Literasi: Jurnal Pengabdian Masyarakat Dan Inovasi. https://api.semanticscholar.org/CorpusID:255119894

Octavia, J. (2019). Pengaruh Sikap Kewirausahaan dan Kompetensi Wirausaha terhadap Keberhasilan Usaha Pada Produsen Sepatu Cibaduyut Kota Bandung. Jurnal Ilmiah Magister Managemen, 5(1), 1–7.

Palupi, E. R., & Sulistyowati, R. (2022). Pengaruh Digital Marketing Berbasis Marketplace terhadap Peningkatan Penjualan Ledre Super UMKM Perempuan di Bojonegoro. Ekonomis: Journal of Economics and Business, 6(2), 780. https://doi.org/10.33087/ekonomis.v6i2.583

Putri, A. T., Wicaksono, B. T., Artama, R. A., Afriyandi, D., Putri, V. A., Utami, A. T., Erica, B., & Kharir, M. (2023). Pendampingan "Pembuatan Foto Produk" Pada Marketplace Bagi UMKM RW 09 Kelurahan Pandean Lamper, Kecamatan Gayamsari, Kota Semarang. Cakrawala: Jurnal Pengabdian Masyarakat Global. https://api.semanticscholar.org/CorpusID:272797300

Rahmawati, L., Tanjung, I., & El Badriati, B. (2018). Analisis Permintaan dan Perilaku Konsumen Fintech Syariah Model Crowdfunding. Profit : Jurnal Kajian Ekonomi Dan Perbankan Syariah, 2(1), 35–49. https://doi.org/10.33650/profit.v2i1.552

Rahmayanti, N. P. (2023). Pengaruh Marketplace dan Pembayaran Digital Terhadap Tingkat Penjualan UMKM Di Kota Banjarmasin. Al-KALAM : JURNAL KOMUNIKASI, BISNIS DAN MANAJEMEN. https://api.semanticscholar.org/CorpusID:256180310

Ranjani, E., Fasa, M. I., & Susanto, I. (2024). Implementasi Digital Marketing Sebagai Strategi Indonesia. Jurnal Intelek Dan Cendikiawan Nusantara, 1(5), 7443–7452.

Saputri, S. A., Berliana, I., Berliana, I., & Nasrida, M. F. (2023). Peran Marketplace Dalam Meningkatkan Daya Saing Umkm Di Indonesia. KNOWLEDGE: Jurnal Inovasi Hasil Penelitian Dan Pengembangan, 3(1), 69–75. https://doi.org/10.51878/knowledge.v3i1.2199

Sarstedt, M., Ringle, C. M., & Hair, J. F. (2017). Partial Least Squares Structural Equation Modeling. In A Concise Guide to Market Research. The Process, Data, and Methods Using IBM SPSS Statistics - 3rd Edition (Issue September, pp. 2–24). Springer International Publishing. https://doi.org/10.1007/978-3-319-05542-8

Sugiyono. (2019). Metode Penelitian Kuantitatif Kualitatif dan R&D. Alfabeta.

Sulistyorini, S., Setyarini, A., & Dwiantari, S. (2023). Pelatihan Digital Marketing Pada Marketplace Sebagai Strategi Pemasaran Produk Umkm Kelurahan Mlatibaru Semarang. TEMATIK. https://api.semanticscholar.org/CorpusID:268835644

Syahrir, Danial, Yulinda, E., & Yusuf, M. (2020). Aplikasi Metode SEM-PLS dalam Pengelolaan Sumberdaya Pesisir dan Lautan. PT Penerbit IPB Press.

Ubaidillah, A., & Atmini, N. D. (2022). Pengaruh Literasi Keuangan dan Sikap Keuangan terhadap Perilaku Pengelolaan Keuangan Pelaku UMKM di Desa Gogik Kecamatan Ungaran Barat Kabupaten Semarang. Jurnal Ilmiah Ekonomika \& Sains. https://api.semanticscholar.org/CorpusID:261821687

Wulfert, T., Woroch, R., & Strobel, G. (2024). Follow the flow: An exploratory multi-case study of value creation in e-commerce ecosystems. Information and Management, 61(8), 104035. https://doi.org/10.1016/j.im.2024.104035