Tata Kelola Keamanan Siber sebagai Kapabilitas Strategis dalam Pertumbuhan Bisnis Digital UMKM

Aliy Hafiz
Program Studi Bisnis Digital, ITBA DCC, Lampung, Indonesia
hafiz@dcc.ac.id

Abstract

Purpose: This study investigates how cybersecurity governance can be conceptualized as a strategic capability that supports operational continuity and business value creation in digital micro, small, and medium-sized enterprises (MSMEs).

Methodology/approach: A PRISMA 2020-guided systematic evidence-mapping process examined scholarly records indexed by Google Scholar between 2020 and October 2026. Of 271 identified records, 45 duplicates were removed; 226 records underwent preliminary screening and 52 were retained for subsequent full-text assessment. An interpretive synthesis of separately verified empirical studies explored governance decisions, cyber resilience, and business outcomes.

Results/findings: The emerging evidence positions cybersecurity governance as a managerial capability involving risk prioritization, accountability, resource allocation, and coordination with technology providers. Empirical studies associate cybersecurity management with organizational performance, although findings do not consistently support cyber resilience as a mediating mechanism. Business continuity and readiness must therefore be distinguished from directly measured revenue growth.

Limitations: Full-text eligibility assessment and methodological appraisal of the candidate corpus are ongoing; the interpretive findings are preliminary rather than definitive estimates of effect.

Contribution: The study develops an evidence-oriented governance–resilience–business-value framework that distinguishes tested relationships from conceptual propositions and identifies priorities for future MSME research.

Keywords: *cybersecurity governance; cyber resilience; digital MSMEs; business performance; systematic literature review*

1. Pendahuluan

Transformasi digital memperluas peluang usaha mikro, kecil, dan menengah (UMKM) untuk mengakses pelanggan, mempercepat transaksi, mengelola inventori, menghubungkan pemasok, dan mengembangkan model bisnis baru. Aktivitas tersebut sekaligus menciptakan ketergantungan terhadap akun digital, layanan komputasi awan, aplikasi pembayaran, basis data konsumen, perangkat bergerak, serta hubungan dengan penyedia platform. Keamanan siber karenanya bukan persoalan perangkat lunak semata, melainkan salah satu prasyarat untuk memastikan manfaat digitalisasi dapat dipertahankan ketika usaha menghadapi penipuan, kebocoran informasi, penghentian layanan, atau penyalahgunaan kredensial. Kajian transformasi digital dalam bisnis menekankan perlunya menghubungkan perubahan teknologi dengan organisasi dan strategi, bukan mengukur digitalisasi hanya dari banyaknya aplikasi yang diadopsi (Kraus et al., 2022).

Bagi UMKM, kebutuhan keamanan siber mempunyai konsekuensi ekonomi yang spesifik. Di satu sisi, sumber daya untuk pembelian perangkat keamanan, pelatihan, konsultasi, dan pemulihan gangguan terbatas. Di sisi lain, insiden keamanan dapat menghambat transaksi, menimbulkan biaya operasional, melemahkan kepercayaan pelanggan, dan mengganggu keberlangsungan proses bisnis. Penelitian terhadap 240 UKM di Inggris oleh Arroyabe et al. (2024) membahas kegagalan pasar, kekurangan informasi, serta kecenderungan kurangnya investasi keamanan. Studi itu menunjukkan bahwa persoalan ekonomi dan pengambilan keputusan relevan untuk dipertimbangkan dalam analisis keamanan UKM, bukan disederhanakan menjadi kepatuhan teknis.

Konsep tata kelola keamanan siber menempatkan pemilik atau pimpinan usaha sebagai aktor penentu toleransi risiko, keputusan investasi, pembagian tanggung jawab, prioritas perlindungan aset, dan kesiapan menghadapi gangguan. OECD (2022) menegaskan bahwa pengelolaan risiko keamanan digital berkaitan dengan kemakmuran dan tujuan ekonomi, sedangkan NIST CSF 2.0 memperkenalkan fungsi Govern sebagai elemen tata kelola yang melengkapi Identify, Protect, Detect, Respond, dan Recover (Pascoe et al., 2024). Bagi UMKM yang beroperasi secara informal, prinsip tersebut perlu diterjemahkan menjadi keputusan sederhana dan proporsional terhadap nilai transaksi, ketergantungan layanan, serta kemampuan organisasi.

Akan tetapi, menganggap semua UMKM belum mengintegrasikan keamanan siber ke strategi bisnis merupakan generalisasi yang tidak dapat diterima tanpa bukti. Studi kasus di Kanada menemukan adanya pergeseran logika manajemen dari keamanan sebagai beban menuju integrasi dalam model bisnis, disertai ketegangan tanggung jawab antara pengelola UMKM dan penyedia keamanan (Hoong et al., 2024). Studi empiris lain mengenai keamanan organisasi dan kinerja berkelanjutan pada UMKM di Arab Saudi juga telah menguji peran ketahanan siber dan budaya organisasi (Al-Somali et al., 2024). Temuan ini berarti tema integrasi keamanan dengan tujuan usaha memang telah diteliti; persoalan ilmiah berikutnya adalah bagaimana merangkum tingkat kepastian, ragam jalur pengaruh, dan konteks berlakunya bukti secara sistematis.

Literatur terbaru semakin menuntut kehati-hatian dalam menilai novelty. Ye (2026), melalui survei 847 UMKM dan wawancara 32 ahli, telah menguji efektivitas manajemen keamanan serta hubungannya dengan kinerja organisasi menggunakan pendekatan TOE, RBV, SEM, dan fsQCA. Artinya, usulan artikel ini tidak dapat mengklaim sebagai kajian pertama yang menyatukan keamanan dan kinerja bisnis. Kontribusi SLR harus menguraikan keseragaman atau perbedaan definisi governance, menguji bagaimana peneliti mengukur outcome pertumbuhan, serta membedakan pola hubungan yang telah divalidasi dari jalur yang baru bersifat normatif.

Penelitian terdahulu sudah menyediakan beberapa sintesis besar. Chaudhary et al. (2023) memetakan kesenjangan literatur kesadaran keamanan UMKM. Brezavšček dan Baggia (2025) menelaah penelitian model kematangan keamanan. Awan dan Alam (2025) memetakan ancaman serta strategi pertahanan pada perusahaan kecil dan menengah. Rombaldo Junior et al. (2026), dalam tinjauan 132 artikel terpilih, mengidentifikasi pola kekurangan literasi, awareness, dan sumber daya. Bahmanova dan Lace (2026) mengembangkan konsep ketahanan siber kolaboratif dengan menggabungkan kajian literatur serta wawancara UMKM. Dengan cakupan yang semakin padat ini, SLR umum mengenai "ancaman keamanan siber UMKM" akan berisiko mengulang pemetaan yang sudah tersedia.

Kesenjangan yang layak diuji adalah belum jelasnya konsistensi bukti tentang bagaimana keputusan tata kelola keamanan berkaitan dengan indikator ketahanan dan hasil bisnis UMKM yang terukur. Meskipun ada studi yang menggunakan kinerja berkelanjutan, biaya, kesiapan, atau kepuasan pelanggan, konstruk dan metode yang berbeda dapat menghasilkan klaim yang tidak langsung dapat dibandingkan. Dalam literatur strategi TI, tinjauan Molete et al. (2025) menilai hubungan perencanaan TI dan kinerja UKM, sedangkan Pelletier dan Raymond (2024) memperlihatkan peran kapabilitas dinamis dalam penyelarasan TI–bisnis melalui studi kasus. Relevansinya terhadap keamanan siber perlu dipilah dengan jelas: tidak semua studi strategi TI menghasilkan temuan tentang keputusan keamanan.

Penelitian ini merumuskan masalah utama: sejauh mana dan melalui mekanisme apa tata kelola keamanan siber dapat dipahami sebagai kapabilitas strategis yang menunjang pertumbuhan bisnis digital UMKM? Pertanyaan tersebut dijabarkan menjadi lima research questions: (RQ1) bagaimana tren dan karakteristik studi; (RQ2) praktik dan peran tata kelola apa yang dilaporkan; (RQ3) bagaimana keterkaitan praktik tersebut dengan ketahanan siber; (RQ4) indikator pertumbuhan dan kinerja bisnis apa yang benar-benar diukur; dan (RQ5) di mana kesenjangan bukti, konteks, teori, dan metode berada. Istilah pertumbuhan tidak otomatis disamakan dengan ketahanan: studi dapat menunjukkan manfaat kontinuitas usaha tanpa membuktikan peningkatan pendapatan atau pangsa pasar.

Penelitian ini bertujuan menjelaskan bagaimana keputusan tata kelola keamanan siber dapat membentuk kapabilitas strategis UMKM digital melalui pengelolaan risiko, pengaturan sumber daya, koordinasi pihak ketiga, dan kesiapan operasional. Dengan pendekatan pemetaan bukti sistematis berpanduan PRISMA 2020, artikel mengintegrasikan hasil identifikasi literatur terstruktur dan pembacaan kritis sejumlah studi empiris yang telah dapat diverifikasi. Keluaran analitis yang dibangun berupa klasifikasi mekanisme tata kelola, pembedaan indikator ketahanan dan pertumbuhan bisnis, serta kerangka hubungan yang siap dievaluasi melalui telaah teks penuh terhadap korpus kandidat. Dalam konteks STABEK IX, kontribusi yang diupayakan adalah pemahaman konseptual tentang bagaimana digitalisasi UMKM dapat berlangsung secara aman, berkelanjutan, dan sesuai dengan kapasitas pengelolaan usaha.

2. Tinjauan Pustaka dan Pengembangan Kerangka Konseptual

2.1. Tata kelola keamanan siber sebagai keputusan bisnis

Tata kelola keamanan siber dapat dimaknai sebagai mekanisme pengarahan dan pengawasan atas risiko keamanan digital agar tetap sejalan dengan tujuan usaha. Praktiknya mencakup penentuan penanggung jawab, penerimaan risiko, kebijakan dasar perlindungan informasi, seleksi vendor, keputusan anggaran, pemantauan insiden, dan evaluasi pemulihan. Penting membedakan tata kelola dari manajemen teknis: konfigurasi keamanan, antivirus, pencadangan, dan autentikasi adalah kontrol atau aktivitas operasional, sedangkan keputusan siapa yang menetapkan kebutuhan, membiayai, memonitor, dan mengevaluasi kontrol merupakan persoalan tata kelola. Pascoe et al. (2024) menempatkan Govern dalam CSF 2.0 sebagai fungsi yang menghubungkan ekspektasi organisasi, strategi, kebijakan, dan pengawasan risiko.

Dalam UMKM, aktor yang memiliki otoritas bisnis biasanya sekaligus mengendalikan keputusan teknologi. Struktur sederhana ini dapat mempercepat penetapan keputusan, tetapi juga menciptakan ketergantungan pada pengetahuan pemilik dan penyedia jasa. Hoong et al. (2024) mengamati bahwa keselarasan persepsi antara manajer UMKM dan penyedia keamanan tidak selalu tercapai. Neri et al. (2022) melalui survei dan wawancara pada UKM Italia memeriksa kesiapan keamanan organisasi dan menunjukkan pentingnya perpaduan antara elemen teknologi, kebijakan, keterampilan, dan budaya. Dengan demikian, review tidak cukup menginventarisasi kontrol yang telah diadopsi; review harus menelusuri proses penetapan keputusan, konteks organisasional, serta bukti bahwa kontrol tersebut diarahkan pada aset bisnis yang kritis. Bukti survei UMKM di Australia Barat menunjukkan keterbatasan anggaran, pengetahuan memulai praktik keamanan, dan pemahaman kerangka keamanan sebagai hambatan kesiapan (Chidukwani et al., 2024). Wawancara pakar UMKM di Jerman mengidentifikasi kesadaran dan pengetahuan, sumber daya, dukungan pimpinan, serta pengembangan berkelanjutan sebagai faktor pembentuk budaya keamanan siber (Gerst et al., 2024).

2.2. Ketahanan siber dan keberlangsungan operasi

Ketahanan siber dalam artikel ini didefinisikan secara operasional sebagai kemampuan UMKM untuk mengantisipasi, menahan, merespons, memulihkan, serta belajar dari gangguan siber sehingga aktivitas usaha dapat dilanjutkan. Definisi operasional ini bukan sekadar jumlah teknologi pelindung. Ketahanan mempunyai dimensi waktu, koordinasi manusia, rencana pemulihan, diversifikasi ketergantungan layanan, dan kemampuan beradaptasi. Tinjauan praktik business continuity management pada UKM menghubungkan dukungan manajemen, kesiapan organisasi, serta keberlangsungan usaha dengan resiliensi dan kinerja organisasi (Awang Ali et al., 2023). Namun, review tersebut melibatkan gangguan usaha yang lebih luas daripada serangan siber; karena itu penerapannya terhadap gangguan siber harus diuji secara eksplisit.

Studi Bahmanova dan Lace (2026) menyimpulkan bahwa kolaborasi lintas organisasi ikut membentuk ketahanan siber UMKM bersama dimensi teknologi, manusia, organisasi, keuangan, dan regulasi. Temuan ini membuka kemungkinan bahwa kapabilitas keamanan yang relevan justru tersebar pada mitra pembayaran, penyedia cloud, komunitas usaha, konsultan, dan regulator. Rombaldo Junior et al. (2026) mengingatkan bahwa banyak temuan pada penelitian UMKM berulang tanpa selalu memiliki bukti baru yang kuat. Oleh karena itu, kajian final perlu memisahkan bukti hasil pengukuran ketahanan, penilaian persepsi, dan rekomendasi konseptual yang belum diuji.

2.3. Pertumbuhan dan kinerja bisnis digital UMKM

Istilah pertumbuhan bisnis digital mencakup peningkatan kapasitas transaksi, perluasan pasar, pertumbuhan pendapatan, pengembangan pelanggan, dan skalabilitas proses berbasis teknologi. Kinerja dapat pula mencakup hasil non-keuangan seperti kontinuitas layanan, keandalan transaksi, reputasi, kepuasan pelanggan, dan efisiensi biaya. Dalam penelitian SLR, masing-masing indikator harus dikodekan terpisah untuk menghindari kesalahan menyamakan outcome antara sumber yang berbeda. Penelitian Al-Somali et al. (2024) menyediakan contoh relasi sistem keamanan dan kinerja bisnis berkelanjutan yang diuji secara empiris. Sebaliknya, Molete et al. (2025) meninjau perencanaan TI dan performance UKM secara lebih umum, sehingga tidak seluruh bukti mereka dapat secara otomatis ditafsirkan sebagai pengaruh keamanan siber.

Arroyabe et al. (2024) menghubungkan keamanan UKM dengan logika ekonomi dan investasi yang tidak optimal akibat masalah informasi. Penelitian Rattanapong et al. (2025) pada organisasi ASEAN menyoroti bahwa pertimbangan risiko, finansial, tata kelola, dan strategi memengaruhi keputusan investasi keamanan. Namun penelitian yang subjeknya organisasi lintas ukuran tidak boleh dikategorikan sebagai studi UMKM tanpa verifikasi karakteristik sampelnya. SLR juga perlu memeriksa apakah ukuran kinerja menggunakan laporan objektif, data sebelum-sesudah insiden, penilaian pengelola, atau hanya ekspektasi manfaat; perbedaan ini sangat menentukan interpretasi hubungan dengan pertumbuhan.

2.4. Perspektif teori dan posisi kebaruan

Tiga lensa teoritis dapat membantu penafsiran, tanpa harus semuanya menjadi model final. Resource-Based View menjelaskan keamanan siber sebagai kombinasi sumber daya organisasi yang potensial menghasilkan nilai jika langka, terorganisasi, dan sulit ditiru. Dynamic Capabilities menyoroti sensing risiko, seizing pilihan investasi, serta transforming rutinitas organisasi agar mampu berubah. Strategic Alignment memusatkan perhatian pada kesesuaian tujuan keamanan, tujuan bisnis, dan mekanisme implementasi. Penelitian Pelletier dan Raymond (2024), yang mempelajari penyelarasan strategis TI pada empat UKM, memperlihatkan pentingnya kapabilitas dinamis dalam menyokong tujuan bisnis, tetapi tidak menjadi bukti langsung bagi semua praktik keamanan siber.

Dengan memanfaatkan ketiga perspektif sebagai kerangka sensitivitas, kajian final menghindari klaim "gap" yang terlalu luas. Kebaruannya tidak berbunyi bahwa belum ada studi keamanan siber dan kinerja UMKM. Sebaliknya, kebaruannya ditargetkan pada penjelasan kondisi ketika praktik tata kelola dikaitkan dengan ketahanan serta tipe outcome bisnis yang berbeda, serta identifikasi hubungan yang hanya disarankan versus hubungan yang diuji. Jika sintesis menunjukkan sudah tersedia model yang identik, kontribusi dapat dialihkan menuju penilaian kualitas dan konsistensi bukti antarkonteks, bukan memaksakan model baru.

Tabel 1. Pemetaan awal penelitian terkait dan batas kontribusinya

Peneliti/tahun	Fokus dan jenis bukti	Relevansi / ruang sintesis
Chaudhary et al. (2023)	SLR awareness UMKM	Tidak secara khusus menilai outcome pertumbuhan
Arroyabe et al. (2024)	Empiris: 240 UKM Inggris, ekonomi keamanan	Pertimbangan investasi dan kegagalan pasar
Hoong et al. (2024)	Empiris: wawancara UKM dan penyedia, Kanada	Tata kelola dan integrasi strategi secara kualitatif
Al-Somali et al. (2024)	Empiris: keamanan, resiliensi, kinerja	Menguji jalur keamanan terhadap business performance
Brezavšček & Baggia (2025)	SLR kematangan keamanan	Fokus model penilaian, bukan seluruh hasil bisnis
Awan & Alam (2025)	Systematic mapping ancaman dan kontrol	Penekanan risiko dan defensive strategy
Rombaldo Junior et al. (2026)	SLR 132 artikel UMKM	Pemetaan hambatan; pembanding penting
Bahmanova & Lace (2026)	SLR + wawancara 14 UMKM Eropa	Dimensi resiliensi kolaboratif

Sumber: Dirancang penulis berdasarkan referensi yang tercantum (2026).

Tabel 1 disusun dari pembacaan awal laman penerbit dan metadata institusional yang dapat diverifikasi; tabel ini bukan daftar studi terpilih hasil penyaringan PRISMA. Status, jumlah, dan klasifikasi artikel yang menjadi korpus review harus ditetapkan setelah ekspor hasil basis data dan penilaian teks penuh. Pembedaan ini penting karena memasukkan artikel hanya berdasarkan kesesuaian judul atau abstrak dapat memperbesar risiko bias seleksi.

2.5. Pendalaman literatur berdasarkan hasil pencarian terbaru

Sebagai penguatan kajian pustaka, hasil pencarian Google Scholar tahun 2026 menampilkan sejumlah karya primer yang belum masuk dalam daftar pustaka draf awal. Verifikasi bibliografis terhadap laman penerbit dan repositori akademik dilakukan untuk memastikan identitas penulis, tahun, judul, serta DOI. Literatur tersebut dikelompokkan menurut relevansinya terhadap tiga konstruk penelitian, yakni mekanisme tata kelola, kemampuan ketahanan siber, dan keluaran bisnis UMKM. Pengelompokan berikut bersifat pemetaan literatur teridentifikasi; bukan keputusan inklusi akhir berdasarkan telaah teks lengkap.

Pada dimensi kapabilitas dan keputusan, Renaud dan Ophoff (2021) membahas kesadaran situasional yang berkaitan dengan keputusan penerapan kontrol keamanan pada UKM; Yigit Ozkan dan Spruit (2023) mengusulkan asesmen kematangan yang dapat disesuaikan dengan kebutuhan UMKM digital; sedangkan Rawindaran et al. (2023) memeriksa persoalan tata kelola dan kebijakan keamanan dalam dua konteks negara. Armenia et al. (2021) memperlihatkan penggunaan simulasi sistem untuk mendukung penilaian risiko dan keputusan investasi keamanan UKM. Keempat sumber memperluas landasan analitis mengenai bagaimana keputusan keamanan dibentuk, tanpa dengan sendirinya membuktikan pertumbuhan penjualan.

Pada dimensi ketahanan dan risiko, Fernandez de Arroyabe et al. (2024) menguji resiliensi siber pada UKM Inggris dengan pendekatan pembelajaran mesin; Neri dan Niccolini (2025) meneliti praktik ketahanan organisasi siber melalui wawancara di Italia; sementara Moneva dan Leukfeldt (2023) memeriksa insiden ancaman orang dalam dan tindakan keamanan pada UKM Belanda. Rawindaran et al. (2025) juga mengembangkan kerangka ketahanan dan kesiapan digital UKM, sedangkan Taskin et al. (2025) memfokuskan perhatian pada keputusan transfer risiko melalui asuransi siber. Studi-studi tersebut mengingatkan bahwa kapasitas pencegahan, respons, pemulihan, dan mekanisme transfer risiko adalah dimensi berbeda yang perlu diekstraksi secara terpisah.

Pada dimensi nilai bisnis, Stentoft et al. (2025) melaporkan adanya pengaruh tidak langsung kesadaran keamanan terhadap kinerja finansial melalui manajemen risiko rantai pasok siber pada UKM manufaktur Denmark; pengaruh totalnya tidak signifikan dan hasil untuk kinerja komersial juga tidak signifikan. Basri (2023) membahas keamanan siber dalam kaitannya dengan efisiensi operasional digital UMKM. Temuan tersebut penting sebagai pembanding bagi argumen bahwa keamanan siber bernilai strategis, sekaligus menuntut pemisahan yang tegas antara kinerja finansial, kinerja komersial, efisiensi digital, dan ketahanan operasional. Penjelasan ini bersandar pada informasi artikel yang dapat diverifikasi; appraisal menyeluruh tetap menjadi bagian tahap kelayakan akhir.

Tabel 2. Studi tambahan yang ditemukan melalui pencarian terbaru dan relevansi analitisnya

Studi hasil PoP	Topik yang dapat diverifikasi	Posisi pada kajian
Renaud & Ophoff (2021)	Kesadaran situasional dan keputusan kontrol	Governance capability
Armenia et al. (2021)	Risiko dinamis dan investasi keamanan	Keputusan investasi
Moneva & Leukfeldt (2023)	Ancaman orang dalam dan tindakan keamanan	Manajemen risiko
Yigit Ozkan & Spruit (2023)	Asesmen kematangan UKM digital	Kematangan kontrol
Rawindaran et al. (2023)	Governance dan kebijakan lintas negara	Tata kelola dan konteks
Basri (2023)	Keamanan dan efisiensi e-operasional	Nilai bisnis nonkeuangan
Fernandez de Arroyabe et al. (2024)	Ketahanan siber UKM Inggris	Kapabilitas resiliensi
Neri & Niccolini (2025)	Resiliensi organisasi siber UKM	Pemulihan dan adaptasi

Studi hasil PoP	Topik yang dapat diverifikasi	Posisi pada kajian
Stentoft et al. (2025)	Risiko siber rantai pasok dan kinerja	Kinerja keuangan/komersial
Rawindaran et al. (2025)	Kerangka ketahanan dan transformasi digital	Kemampuan organisasi
Taskin et al. (2025)	Asuransi siber dan digitalisasi UKM	Transfer risiko

Sumber: Identifikasi enam file pencarian 21 Oktober 2026; identitas publikasi dicocokkan dengan laman penerbit atau repositori akademik. Semua entri pada tabel merupakan kandidat penelitian, bukan studi yang telah diputuskan masuk sintesis final.

3. Metodologi Penelitian

3.1. Desain SLR dan status pelaksanaan

Penelitian menggunakan kerangka Systematic Literature Review (SLR) dengan panduan pelaporan PRISMA 2020 dan PRISMA-S (Page et al., 2021; Rethlefsen et al., 2021). Penelusuran bibliografi dilakukan melalui Google Scholar menggunakan enam strategi pencarian yang dihimpun pada 21 Oktober 2026. Rekaman hasil penelusuran dinormalisasi dan diperiksa duplikasinya berdasarkan judul, DOI, serta tautan sumber, kemudian dilakukan penapisan awal berdasarkan populasi UMKM, konsep tata kelola keamanan siber, dan kaitannya dengan resiliensi maupun nilai bisnis. Tahap yang telah terdokumentasi mencakup identifikasi, deduplikasi, serta seleksi metadata; penilaian kelayakan teks penuh dan appraisal metodologis dilakukan pada tahap lanjutan. Oleh sebab itu, angka alur yang disajikan merepresentasikan tahapan yang telah terlaksana, tanpa mengubah kandidat menjadi studi terinklusi.

Enam set data pencarian memuat 271 rekaman (masing-masing 40, 30, 50, 51, 50, dan 50). Setelah 45 rekaman duplikat diidentifikasi—44 berdasarkan kesamaan judul dan satu berdasarkan URL artikel—diperoleh 226 rekaman unik. Penapisan awal menandai 174 rekaman sebagai tidak memenuhi fokus sementara, sedangkan 52 dipertahankan untuk evaluasi naskah lengkap. Keputusan awal tercatat pada log per artikel dan perlu ditinjau kembali terhadap abstrak penerbit, terutama untuk rekaman yang konteks UMKM atau konstruk kinerjanya belum dapat ditentukan hanya dari metadata.

3.2. Perumusan research questions

Tabel 3. Research questions dan informasi yang diekstraksi

Kode	Pertanyaan penelitian	Informasi yang dibutuhkan
RQ1	Bagaimana perkembangan dan karakteristik studi 2020–2026?	Tahun, negara, sektor, metode, sumber
RQ2	Praktik tata kelola keamanan apa yang ditemukan?	Kepemimpinan, strategi, kebijakan, anggaran, vendor
RQ3	Bagaimana tata kelola dikaitkan dengan cyber resilience?	Mekanisme kesiapan, respons, pemulihan, adaptasi
RQ4	Hasil bisnis apa yang diukur atau dilaporkan?	Pendapatan, efisiensi, pelanggan, kontinuitas, kepercayaan
RQ5	Di mana kesenjangan teori, konteks, dan bukti?	Kualitas studi, arah hubungan, proksi, bias, konteks

Sumber: Dirancang penulis berdasarkan referensi yang tercantum (2026).

Kerangka pemilihan studi menggunakan Population–Concept–Context (PCC). Population ialah usaha mikro, kecil, dan menengah atau pelaku bisnis dengan karakteristik UMKM yang dijelaskan eksplisit oleh studi. Concept adalah tata kelola keamanan siber, keputusan strategis risiko keamanan digital, dan kaitannya dengan kapabilitas ketahanan serta outcome usaha. Context mencakup aktivitas digital, perusahaan yang bertransformasi secara digital, dan ekosistem usaha berbasis platform. Artikel yang hanya membahas serangan secara teknis tanpa proses tata kelola atau dimensi bisnis akan dikeluarkan dari sintesis utama, namun dapat dipakai sebagai konteks teoretis dalam pendahuluan.

3.3. Basis data, rentang waktu, dan strategi pencarian

Pencarian yang telah dilaksanakan bersumber dari Google Scholar melalui Publish or Perish. Enam ekspor CSV mencatat tanggal pengambilan data, judul, sumber, tautan, dan sebagian metadata DOI atau cuplikan abstrak. File ekspor tidak memuat string pencarian serta pengaturan kueri yang digunakan; karena itu informasi tersebut harus dicatat dari riwayat atau tangkapan layar PoP sebelum review dapat

dinyatakan sepenuhnya dapat direplikasi. Tidak ada klaim bahwa Scopus, Web of Science, IEEE Xplore, atau ACM Digital Library telah digunakan. Pemakaian Google Scholar sebagai sumber tunggal harus dinyatakan sebagai batasan cakupan dan keterulangan pencarian. Audit kelengkapan metadata menunjukkan bahwa 270 dari 271 entri memuat tanda elipsis (…), dengan 267 cuplikan dimulai oleh tanda tersebut. Semua 52 kandidat telaah teks penuh hanya memiliki cuplikan pendek; tidak satu pun abstrak lengkap disediakan pada ekspor CSV. Oleh karena itu, kolom Abstract dari PoP tidak diperlakukan sebagai ringkasan penelitian yang memadai untuk mengekstraksi temuan studi.

Rentang waktu pencarian ditetapkan 1 Januari 2020–21 Oktober 2026. Enam berkas hasil penelusuran bertanggal 21 Oktober 2026. Pembatasan tahun 2026 berdasarkan metadata PoP belum membuktikan semua artikel telah benar-benar terbit sebelum tanggal pencarian; tanggal publikasi kandidat harus dikonfirmasi saat telaah teks penuh. Satu rekaman tanpa tahun publikasi sementara dikeluarkan. Bahasa, jenis publikasi, serta kriteria peer review harus diperiksa pada tahap penilaian kelayakan penuh karena metadata Google Scholar dapat menyertakan buku, preprint, skripsi/tesis, dan publikasi nonjurnal.

Strategi konseptual pencarian mencakup istilah UMKM/SME/MSME, cybersecurity atau information security, serta governance, resilience, risk management, investment, strategic alignment, atau business performance. Sebagai contoh yang dapat direplikasi untuk pencarian berikutnya: "cybersecurity governance" "SMEs"; "cyber resilience" "business performance" SMEs; dan "cybersecurity investment" "SMEs". Ini merupakan contoh desain kueri, bukan pernyataan bahwa string tersebut persis digunakan menghasilkan enam CSV yang terlampir. Kueri aktual, parameter tahun, jumlah hasil maksimum, dan tanggal pengambilan harus ditambahkan peneliti dari pengaturan PoP asli.

Berkas sumber disimpan tanpa perubahan, kemudian setiap rekaman diberi identitas unik serta dicatat berkas asal, nomor baris, tahun, DOI, URL, status seleksi, dan alasan pengecualian. Duplikasi diperiksa menggunakan normalisasi judul (penghapusan karakter nonalfanumerik) dan pencocokan URL artikel; pencocokan DOI dilakukan bila tersedia. Penyaringan pertama menggunakan informasi judul dan cuplikan abstrak yang tersedia di PoP. Tahap berikutnya adalah mengambil abstrak asli dan naskah lengkap 52 kandidat, mengecek jenis publikasi dan relevansi kinerja UMKM, mendokumentasikan alasan setiap keputusan full-text, dan menggunakan appraisal menurut desain studi.

3.4. Kriteria inklusi dan eksklusi

Tabel 4. Kriteria kelayakan artikel

Aspek	Inklusi	Eksklusi
Tahun	2020 hingga 21 Oktober 2026	Di luar rentang utama
Jenis dokumen	Artikel jurnal dan prosiding peer-reviewed	Blog, iklan, materi tanpa review
Konteks usaha	UMKM/SME atau subsampel UMKM yang jelas	Hanya perusahaan besar tanpa analisis SME
Substansi	Tata kelola keamanan, strategi risiko, resiliensi, outcome bisnis	Murni algoritma/teknik tanpa konteks governance-bisnis
Bukti	Metode dan temuan dapat diperiksa; review dipisah dari primer	Opini tanpa prosedur atau temuan ilmiah
Akses	Teks penuh tersedia untuk penilaian	Tidak dapat diakses setelah upaya penelusuran

Sumber: Dirancang penulis berdasarkan referensi yang tercantum (2026).

Satu kekhususan protokol adalah pemisahan artikel penelitian primer dan sekunder. Studi empiris primer digunakan untuk membuat klaim keterkaitan konstruk dan hasil bisnis. SLR yang telah terbit digunakan untuk cross-check tema dan konteks, tetapi tidak dihitung sebagai pengganti studi primer dalam agregasi temuan untuk mencegah penghitungan ganda. Publikasi kebijakan dan pedoman resmi NIST/OECD dibahas sebagai kerangka normatif, bukan dikodekan sebagai bukti empiris tentang kinerja UMKM. Jika ada artikel yang mencampur usaha besar dan kecil, hanya temuan spesifik pada kategori usaha kecil/menengah yang diekstraksi bila dapat dipisahkan.

3.5. Tahapan screening dan diagram PRISMA

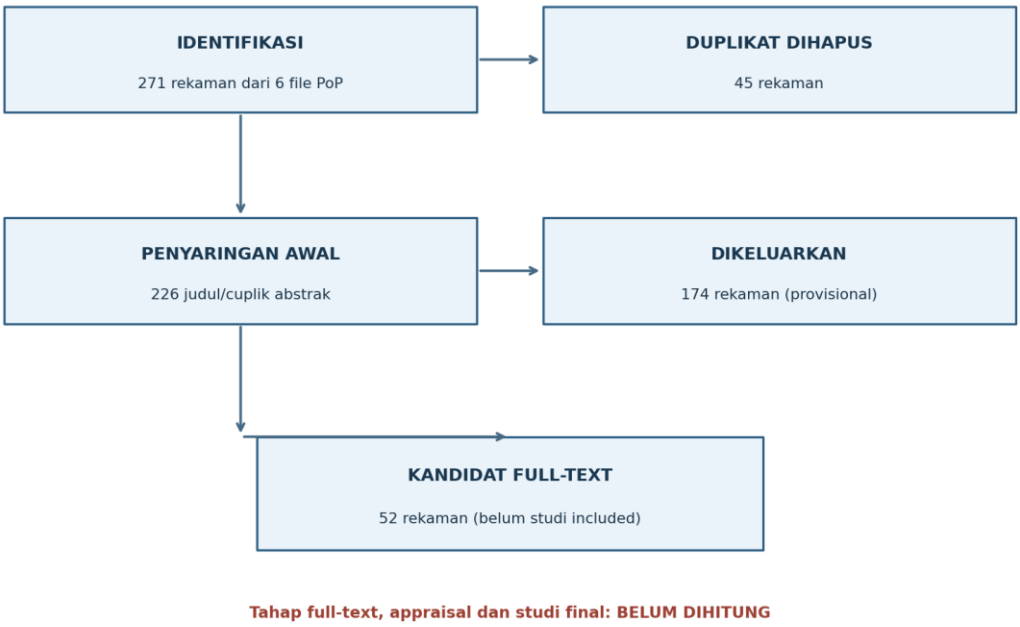
Tahapan dilakukan secara berurutan: identifikasi 271 rekaman dari enam file PoP; deduplikasi 45 rekaman; penyaringan awal 226 judul/cuplikan abstrak; pengecualian sementara 174 rekaman; serta penetapan 52 kandidat untuk tahap pencarian dan pemeriksaan teks lengkap. Status kandidat tidak sama dengan laporan teks lengkap yang sudah diperoleh ataupun studi terinklusi. Karena cuplikan abstrak sering terpotong dan pemilihan dilakukan melalui satu siklus penilaian berbantuan asisten, alasan eksklusi awal harus diperiksa kembali oleh penulis dan, bila memungkinkan, penilai independen sebelum diagram final disahkan. Karena 270/271 entri berisi cuplikan terpotong, pengecualian berbasis metadata berisiko menghilangkan studi relevan; tahap verifikasi perlu mencakup abstrak lengkap artikel yang dikeluarkan karena informasi tidak mencukupi.

Penghitungan dalam Tabel 4 didasarkan pada berkas ekspor pencarian aktual dan log seleksi per rekaman. Jumlah rekaman yang ditemukan, duplikasi, dan kandidat merupakan hasil proses yang sudah terdokumentasi. Adapun jumlah laporan yang berhasil diperoleh, dinilai kelayakannya, dan akhirnya diikutsertakan dalam sintesis akan dilaporkan setelah penilaian teks lengkap; sel yang belum memiliki data tidak diartikan sebagai nilai nol. Pemisahan ini menjaga konsistensi pelaporan PRISMA 2020 dan keterlacakan keputusan seleksi.

Tabel 5. Alur seleksi PRISMA 2020 yang dapat diaudit (tahap awal, 21 Oktober 2026)

Tahap audit awal	Jumlah aktual	Sumber/perhitungan
Records identified from Google Scholar via PoP	271	40 + 30 + 50 + 51 + 50 + 50
Duplicate records removed	45	44 kesamaan judul; 1 kesamaan URL artikel
Records screened (title/snippet)	226	271 − 45
Records excluded at initial screening	174	Keputusan awal sesuai log 226 rekaman; perlu validasi penulis
Candidate records for full-text retrieval	52	226 − 174; belum sama dengan reports sought aktual
Reports sought for retrieval	Belum dihitung	Proses permintaan/pengambilan teks lengkap belum dimulai secara sistematis
Reports not retrieved	Belum dihitung	Tidak dapat diisi angka 0 tanpa log penelusuran full-text
Reports assessed for eligibility	Belum dihitung	Tunggu telaah teks penuh 52 kandidat
Reports excluded after full text	Belum dihitung	Alasan tiap artikel perlu dicatat
Studies included in final synthesis	Belum dihitung	Belum tersedia angka inklusi yang sah

Gambar 1. Alur identifikasi dan screening awal berbasis 6 ekspor Google Scholar (belum tahap inklusi).



Sumber: Audit terstruktur enam ekspor Publish or Perish dari Google Scholar, 21 Oktober 2026. Gambar ini merupakan alur sementara, bukan diagram PRISMA 2020 final yang telah menyelesaikan seleksi teks penuh.

3.6. Penilaian kualitas dan ekstraksi data

Kualitas metodologis akan dievaluasi dengan matriks appraisal yang dibedakan menurut desain artikel. Untuk survei diperiksa desain sampling, validitas konstruk, kesesuaian metode statistik, missing data, dan keterbatasan inferensi kausal. Untuk studi kualitatif diperiksa strategi pemilihan partisipan, kecukupan penjelasan analisis, triangulasi, refleksivitas, dan keterlacakan kutipan. Untuk studi campuran diperiksa integrasi dua jenis bukti. Hasil appraisal dinyatakan sebagai kekuatan dan keterbatasan bukti, bukan sekadar skor tunggal yang menyamarkan perbedaan desain. Apabila dua evaluator tersedia, ketidaksepakatan kriteria appraisal diselesaikan melalui diskusi dan didokumentasikan.

Formulir ekstraksi pada setiap artikel minimal berisi identitas DOI, negara, sektor, ukuran usaha, jenis aktivitas digital, karakteristik responden, kerangka teori, desain penelitian, ukuran sampel, definisi governance, dimensi cyber resilience, indikator business performance, arah serta signifikansi hasil bila tersedia, faktor kontekstual, kelemahan metodologi, dan kutipan halaman sumber. Setiap penilaian tentang hubungan variabel juga diberi label: (a) diuji secara empiris; (b) didukung bukti kualitatif; (c) ditawarkan sebagai model konseptual; atau (d) disimpulkan oleh penulis review sekunder. Label ini penting supaya peneliti tidak mengubah pernyataan normatif menjadi kesimpulan berbasis data.

Tabel 6. Matriks ekstraksi dan pengodean sintesis

Kode kategori	Contoh indikator	Sumber data saat review
GOV – governance	Pemilik bertanggung jawab, policy, risk appetite, anggaran	Bagian metode/hasil studi primer
RES – resilience	Recovery time, incident response, backup dan pembelajaran	Hasil yang benar-benar dilaporkan
BUS – business outcome	Pendapatan, biaya, trust, continuity, efisiensi	Indikator/ukuran empiris spesifik
CTX – context	Skala usaha, digital maturity, negara, sektor	Profil sampel dan konteks penelitian
EVD – evidence strength	Desain, sampel, validitas, keterbatasan	Metode dan appraisal full text

Sumber: Dirancang penulis berdasarkan referensi yang tercantum (2026).

3.7. Strategi sintesis dan kontrol bias

Sintesis direncanakan dalam tiga tahap. Pertama, analisis deskriptif memetakan periode terbit, lokasi, sektor, metode, dan kerangka teori. Kedua, thematic synthesis mengelompokkan praktik tata kelola ke dalam pengarah strategis, pengorganisasian, investasi dan alokasi sumber daya, manajemen pihak ketiga, respons-pemulihan, serta evaluasi dan pembelajaran. Ketiga, evidence mapping menghubungkan tiap kelompok praktik ke indikator cyber resilience dan business performance disertai informasi mengenai desain studi, mutu metodologi, dan konsistensi arah temuan. Metode ini dipilih karena indikator dan pendekatan studi kemungkinan heterogen sehingga meta-analisis kuantitatif belum dapat dijanjikan sebelum korpus final diketahui.

Risiko bias publikasi dan bahasa akan dibahas melalui pencarian tambahan ke rujukan mundur dan sitasi maju dari artikel kunci, dengan tetap mengikuti kriteria awal. Risiko overlap sumber sekunder ditangani dengan membatasi agregasi bukti ke studi primer. Untuk membatasi confirmatory bias, setiap artikel yang melaporkan tidak adanya pengaruh atau hubungan negatif tetap harus ditampilkan dalam matriks. Sensitivity analysis dapat dilakukan dengan membandingkan simpulan pada studi yang mempunyai ukuran kinerja objektif dengan studi yang hanya memakai persepsi. Jika tersedia cukup data, hasil dipisah menurut negara berpendapatan tinggi/berkembang dan jenis UMKM, tanpa menyimpulkan bahwa satu konteks mewakili seluruh UMKM.

4. Hasil dan Pembahasan: Pemetaan Bukti dan Kapabilitas Strategis UMKM

4.1. Hasil identifikasi dan penyaringan literatur

Identifikasi dari enam penelusuran Google Scholar menghasilkan 271 rekaman. Sebanyak 45 duplikasi dihapus sehingga 226 rekaman unik menjalani penyaringan awal; 174 rekaman dikelompokkan sebagai pengecualian sementara dan 52 artikel masuk daftar kandidat telaah teks penuh. Alasan pengecualian awal terdiri atas literatur sekunder atau sumber konteks (70), fokus artikel di luar keamanan siber (67), relevansi tata kelola maupun luaran bisnis belum cukup jelas (24), konteks UMKM belum teridentifikasi (12), dan tahun publikasi tidak tersedia (1). Kategori ini mencerminkan klasifikasi awal atas metadata ringkas; keputusan yang belum tegas akan diverifikasi melalui abstrak asli sebelum seleksi final. Dengan demikian, alur PRISMA sudah memberikan jejak penelusuran yang dapat diaudit, tetapi jumlah studi yang benar-benar memenuhi syarat untuk sintesis akhir belum ditetapkan.

4.2. Temuan empiris yang relevan dengan nilai strategis keamanan siber

Pembacaan kritis beberapa publikasi primer yang telah terverifikasi dipergunakan untuk menilai potensi mekanisme teoritis dan mengembangkan kerangka sintesis. Bukti ilustratif ini dikaji terpisah dari penghitungan studi terinklusi dalam alur PRISMA, sehingga tidak digunakan untuk menghitung prevalensi temuan pada 52 kandidat. Studi yang dipertimbangkan mewakili perspektif pengambilan keputusan dan investasi keamanan (Arroyabe et al., 2024), tata kelola lintas aktor (Hoong et al., 2024), kesiapan organisasi (Neri et al., 2022), serta keterkaitan dengan kinerja organisasi (Al-Somali et al., 2024; Ye, 2026).

Dalam studi terhadap 240 UKM Inggris, Arroyabe et al. (2024) menemukan bahwa asimetri informasi dan keterbatasan persepsi atas risiko berkaitan dengan investasi keamanan yang kurang optimal; implementasi juga lebih banyak menitikberatkan kontrol teknis daripada sistem manajemen. Hoong et al. (2024), melalui wawancara dengan 35 wakil UKM dan 11 penyedia keamanan di Kanada, menunjukkan bahwa tanggung jawab keamanan dipengaruhi negosiasi antara kebutuhan bisnis dan model layanan penyedia. Neri et al. (2022) menilai kesiapan keamanan organisasi UKM Italia dan menunjukkan pentingnya kebijakan, keterampilan, serta pelatihan yang melengkapi solusi teknologi. Ketiga studi ini mendukung interpretasi keamanan siber sebagai persoalan tata kelola, bukan semata adopsi perangkat proteksi.

Bukti tentang kinerja bisnis memperlihatkan jalur hubungan yang lebih bernuansa. Al-Somali et al. (2024) mengolah survei terhadap 394 responden UMKM Arab Saudi dan melaporkan hubungan positif sistem keamanan siber organisasi dengan sustainable business performance ($\beta = 0{,}784$; $p < 0{,}001$).

Namun hubungan cyber resilience dengan kinerja tidak signifikan (β = 0,023; p = 0,531), demikian pula efek mediasi yang diuji. Ye (2026), menggunakan survei terhadap 847 UMKM dan wawancara 32 ahli, melaporkan hubungan positif efektivitas manajemen keamanan dengan kinerja organisasi. Karena indikator kinerja dalam penelitian tersebut bersumber dari instrumen penelitian dan konteksnya berbeda, pola tersebut tidak dapat ditafsirkan sebagai bukti kausal peningkatan omzet. Secara bersama-sama, temuan ini menegaskan perlunya memisahkan asosiasi langsung tata kelola–kinerja dari jalur tidak langsung melalui ketahanan siber.

Daftar 52 kandidat memuat penelitian mengenai investasi keamanan, kepemimpinan, tata kelola layanan, budaya keamanan, resiliensi, serta luaran organisasi. Sebelum kelayakan teks penuh dinilai, daftar tersebut berfungsi sebagai ruang penelusuran, bukan denominator bagi generalisasi atau frekuensi tema. Tabel 7 menyajikan bukti primer terverifikasi sebagai landasan kerangka interpretatif; Tabel 8 memuat sejumlah kandidat yang akan diperiksa lebih lanjut. Kedua kelompok sumber dipisahkan secara eksplisit agar simpulan substansial tidak disamakan dengan hasil seleksi PRISMA yang masih berjalan.

Tabel 7. Matriks bukti empiris pembentuk kerangka sintesis awal (di luar hitungan inklusi PRISMA)

Studi	Desain / konteks	Temuan bukti yang diperiksa	Batas interpretasi
Neri et al. (2022)	Italia; survei dan wawancara	Kesiapan keamanan relatif terbatas; kebijakan, pelatihan, dan budaya organisasi saling melengkapi	Tidak mengukur pertumbuhan pendapatan
Arroyabe et al. (2024)	Inggris; studi 240 UKM	Asimetri informasi dan penilaian risiko yang lemah berkaitan dengan keputusan investasi keamanan	Menjelaskan implementasi dan investasi, bukan efek kausal pertumbuhan
Hoong et al. (2024)	Kanada; wawancara 35 wakil UKM dan 11 penyedia	Tata kelola dibentuk oleh hubungan manajer UKM dan penyedia, serta pergeseran logika pengelolaan bisnis	Bukti kualitatif; tidak mengestimasi dampak finansial
Al-Somali et al. (2024)	Arab Saudi; survei n=394; PLS-SEM	Sistem keamanan–kinerja β=0,784 (p<0,001); resiliensi–kinerja p=0,531	Mediasi resiliensi tidak didukung; asosiasi survei bukan kausalitas
Ye (2026)	Survei n=847; wawancara pakar n=32	Efektivitas pengelolaan keamanan berkaitan positif dengan kinerja organisasi	Kinerja diukur melalui konstruk penelitian

Tabel 8. Delapan contoh kandidat hasil pencarian yang memerlukan telaah teks penuh

Studi	Bukti awal dari abstrak/metadata	Status
Renaud & Ophoff (2021)	Model kesadaran situasional untuk keputusan kontrol siber UKM	Kandidat; verifikasi metode dan temuan full text
Yigit Ozkan & Spruit (2023)	Kerangka kematangan keamanan untuk UKM digital	Kandidat; verifikasi hasil evaluasi
Rawindaran et al. (2023)	Kebijakan dan tata kelola keamanan UKM Saudi–Inggris	Kandidat; verifikasi kelayakan
Fernandez de Arroyabe et al. (2024)	Kapasitas penanganan, pemulihan, adaptasi insiden UKM	Kandidat; pemeriksaan hasil dan appraisal
Armenia et al. (2021)	Simulasi risiko dan dukungan keputusan investasi UKM	Kandidat; periksa konteks dan implementasi
Stentoft et al. (2025)	Manajemen risiko siber rantai pasok dan kinerja UKM	Kandidat; pemeriksaan efek dan indikator
Neri & Niccolini (2025)	Praktik cyber-organizational resilience UKM Italia	Kandidat; telaah full text
Taskin et al. (2025)	Asuransi siber dan transformasi digital UKM	Kandidat; konfirmasi relevansi

Sumber Tabel 7: telaah awal terhadap laporan empiris yang dapat diverifikasi; Tabel 8: metadata pencarian tanggal 21 Oktober 2026. Penyebutan suatu studi pada kedua tabel tidak berarti status inklusinya pada SLR final telah ditetapkan.

4.3. Taksonomi mekanisme tata kelola dan keluaran bisnis

Tabel 9. Kerangka pengodean mekanisme governance, resiliensi, dan nilai bisnis

Dimensi tata kelola	Jalur ketahanan yang ditelaah	Outcome bisnis yang diuji
Kepemimpinan pemilik dan prioritas risiko	Kesiapan dan respons insiden	Minim gangguan layanan
Kebijakan, peran, dan akuntabilitas	Konsistensi kontrol dan perilaku	Kepercayaan dan keandalan transaksi
Investasi dan penilaian biaya-risiko	Kemampuan mitigasi dan pemulihan	Biaya kerugian/efisiensi
Tata kelola vendor dan platform	Pengelolaan ketergantungan	Kelangsungan kanal penjualan
Pembelajaran pascainsiden	Adaptasi dan perbaikan berkelanjutan	Ketahanan relasi pelanggan
Keselarasan strategi keamanan-bisnis	Prioritas perlindungan aset kritis	Indikator pertumbuhan bila tersedia

Sumber: Dirancang penulis berdasarkan referensi yang tercantum (2026).

Tabel 9 merumuskan jalur analitis yang akan dikodekan pada setiap studi terpilih. Kategori kesiapan, kemampuan pulih, dan kesinambungan operasi merupakan indikator ketahanan yang berbeda dari ukuran pertumbuhan seperti pendapatan atau perluasan pasar. Pemisahan luaran diperlukan karena manfaat keamanan siber dapat muncul sebagai pencegahan kerugian atau stabilitas transaksi tanpa diikuti pengukuran pertumbuhan usaha. Setiap jalur pada tabel diperlakukan sebagai proposisi interpretatif sampai dapat dibandingkan terhadap hasil, desain, dan mutu studi primer.

Pembandingan literatur baru menegaskan perlunya memisahkan jenis bukti. Kajian tentang kematangan kontrol, kesiapan insiden, keputusan investasi, dan transfer risiko menyajikan mekanisme kebijakan atau kapabilitas yang berbeda (Armenia et al., 2021; Yigit Ozkan & Spruit, 2023; Taskin et al., 2025). Di sisi hasil bisnis, Stentoft et al. (2025) menunjukkan bahwa kesadaran keamanan dan kinerja perusahaan tidak selalu terhubung secara langsung; manajemen risiko siber rantai pasok dapat menjadi salah satu mekanisme tidak langsung untuk dimensi finansial. Karena temuan ini ditelaah dari publikasi individual dan belum seluruh kandidat melewati appraisal seragam, maknanya adalah pengayaan landasan sintesis, bukan prevalensi temuan seluruh korpus 52 artikel.

4.4. Sintesis interpretatif: keamanan siber sebagai kapabilitas strategis

Temuan awal memungkinkan pembedaan tiga komponen konseptual. Pertama, governance capability merujuk pada kemampuan pimpinan menetapkan prioritas risiko, membagi akuntabilitas, mengalokasikan anggaran, dan mengawasi penyedia layanan. Kedua, cyber resilience capability merepresentasikan kesiapan operasional untuk mempertahankan dan memulihkan proses bisnis saat terjadi gangguan. Ketiga, business value berkaitan dengan kontinuitas transaksi, efisiensi pengeluaran, kepercayaan pelanggan, serta—apabila diukur secara eksplisit—pertumbuhan pendapatan atau pasar. Ketiga komponen mempunyai relasi potensial, tetapi bukan konstruk yang dapat dipertukarkan. Perbedaan hasil Al-Somali et al. (2024) dan Ye (2026) memperlihatkan bahwa asosiasi keamanan dengan kinerja dapat muncul tanpa bukti konsisten bahwa ketahanan siber bertindak sebagai mediator.

Dari sudut pandang Resource-Based View dan Dynamic Capabilities, pengetahuan yang dapat ditarik pada tahap ini ialah perlunya memandang keamanan sebagai rangkaian keputusan yang mempertahankan kemampuan UMKM menangkap nilai dari digitalisasi. UMKM tidak hanya membutuhkan kontrol autentikasi atau pencadangan, tetapi juga pilihan yang terukur mengenai aset bisnis kritis, batas toleransi gangguan, pembagian tanggung jawab transaksi, pemulihan data, dan pengelolaan ketergantungan platform. Namun, konfigurasi kapabilitas tersebut dapat berbeda antara usaha mikro yang bergantung pada marketplace dan usaha menengah yang memiliki personel TI internal. Karena itu, ukuran usaha, intensitas digitalisasi, dan struktur layanan pihak ketiga perlu diperlakukan sebagai konteks pembatas dalam sintesis dan penelitian berikutnya.

Secara lebih operasional, kapabilitas strategis yang relevan dapat diuraikan menjadi empat mekanisme: (1) pengarahan, yaitu penetapan tujuan perlindungan yang mengikuti prioritas usaha; (2) orkestrasi, yaitu integrasi kebijakan, pekerja, teknologi, dan vendor; (3) adaptasi, yaitu kemampuan mengubah prosedur ketika risiko dan model bisnis berubah; serta (4) akuntabilitas nilai, yaitu pengukuran biaya gangguan, pemulihan layanan, dan konsekuensi bagi pelanggan. Keempat mekanisme adalah kategori sintesis interpretatif yang diajukan untuk pengujian, bukan frekuensi temuan dari keseluruhan korpus pencarian.

Perbedaan antara manfaat langsung dan tidak langsung juga penting. Tata kelola dapat menciptakan nilai bisnis melalui pengurangan keputusan keamanan yang tidak efisien, kejelasan pembagian peran, dan pengelolaan risiko platform, sementara kemampuan pulih dapat menjaga transaksi ketika insiden terjadi. Meski demikian, pertumbuhan bisnis merupakan outcome yang lebih jauh dan dipengaruhi pasar, modal, produk, serta kondisi eksternal. Oleh karena itu, review berikutnya perlu menilai apakah studi mengukur omzet, retensi pelanggan, atau efisiensi secara nyata, bukan hanya persepsi bahwa organisasi sudah lebih aman.

4.5. Implikasi teoretis, manajerial, dan kebijakan

Kontribusi teoretis dari pemetaan awal terletak pada taksonomi berjenjang antara keputusan tata kelola, kapabilitas ketahanan siber, dan luaran nilai bisnis, sehingga literatur tidak menyamakan keamanan teknis, kesiapan organisasi, dan pertumbuhan. Kerangka tersebut juga menawarkan dua jalur yang dapat diuji pada studi empiris berikutnya: hubungan langsung tata kelola keamanan dengan nilai bisnis serta hubungan tidak langsung melalui ketahanan operasional. Bukti yang ada belum cukup untuk menetapkan besar atau kausalitas kedua jalur, tetapi sudah memberikan dasar untuk merumuskan definisi konstruk dan ukuran yang lebih presisi.

Bagi manajemen UMKM, implikasi awalnya ialah menempatkan keamanan siber dalam keputusan operasional dan investasi yang relevan dengan aktivitas penghasil pendapatan. Prioritas proporsional dapat meliputi inventarisasi akun transaksi dan aset data kritis, tanggung jawab pengelolaan kredensial, penggunaan autentikasi berlapis, prosedur pencadangan, kontak darurat penyedia platform, dan latihan pemulihan sederhana. Praktik ini konsisten dengan prinsip pengelolaan risiko dalam NIST CSF 2.0 untuk usaha kecil (Eliot, 2024); efektivitas ekonominya pada berbagai kategori UMKM masih memerlukan pengujian empiris.

Bagi pembina UMKM dan perumus kebijakan, keamanan siber dapat ditempatkan sebagai prasyarat keberlanjutan manfaat ekonomi digitalisasi. Asimetri informasi dan insentif investasi yang ditemukan Arroyabe et al. (2024) memberikan alasan untuk mempertimbangkan intervensi yang menggabungkan literasi, pendampingan keputusan risiko, dan kejelasan tanggung jawab penyedia layanan. Namun, rekomendasi tersebut bersifat implikasi kebijakan dari penelitian terdahulu dan belum merupakan evaluasi dampak program pada UMKM Indonesia.

4.6. Agenda riset untuk menguji kerangka kapabilitas strategis

Agenda riset berikutnya diarahkan pada pengujian empiris atas dua jalur tata kelola–kinerja, identifikasi mediator atau moderator yang sesuai, dan pemilahan indikator kinerja objektif dari persepsi pemilik usaha. Secara metodologis, tahap lanjutan review akan menyelesaikan pemeriksaan abstrak asli, telaah teks lengkap terhadap kandidat, pencatatan alasan pengecualian, appraisal yang sesuai dengan desain, serta sintesis berdasarkan mutu dan arah hasil. Tahap itu juga perlu mengevaluasi keterulangan pencarian dan ketahanan simpulan ketika studi berbasis persepsi dibandingkan dengan studi berindikator keuangan atau operasional. Dengan demikian, kerangka konseptual yang ditawarkan dapat berkembang menjadi model yang lebih teruji, tanpa mengasumsikan bahwa setiap bentuk resiliensi otomatis meningkatkan penjualan.

5. Kesimpulan

Pemetaan bukti menunjukkan bahwa tata kelola keamanan siber memiliki relevansi strategis bagi bisnis digital UMKM melalui penetapan prioritas risiko, pembagian tanggung jawab, keputusan investasi, serta koordinasi dengan penyedia layanan. Hasil penelitian terdahulu yang diperiksa mengindikasikan hubungan antara pengelolaan keamanan dan luaran organisasi, tetapi mekanisme yang melibatkan ketahanan siber belum menunjukkan bukti yang seragam. Karena itu, ketahanan operasional, perlindungan nilai usaha, dan pertumbuhan pendapatan perlu dibedakan secara konseptual maupun dalam pengukurannya. Kerangka governance–resilience–business value yang diajukan merupakan hasil interpretasi awal untuk mengarahkan evaluasi bukti dan pengujian lanjut.

Secara metodologis, pencarian terstruktur telah mengidentifikasi 271 rekaman, menyisihkan 45 duplikasi, serta mempertahankan 52 kandidat setelah penapisan awal dari 226 rekaman unik. Temuan tematik pada naskah ini berasal dari studi jangkar empiris yang ditinjau secara terpisah, bukan dari korpus terinklusi yang telah final. Kontribusi tahap penelitian saat ini ialah tersedianya jejak seleksi yang dapat ditelusuri dan formulasi mekanisme kapabilitas strategis yang dapat diperiksa kembali. Penguatan kesimpulan lintas studi menunggu selesainya penilaian kelayakan, appraisal metodologis, dan sintesis atas studi yang benar-benar memenuhi kriteria.

Limitasi Penelitian dan Agenda Pengembangan

Penafsiran hasil perlu mempertimbangkan tiga batasan utama. Pertama, cakupan penelusuran berasal dari satu indeks ilmiah sehingga sensitivitas pencarian dan representasi lintas bidang belum dapat diasumsikan setara dengan penelusuran multibasis data. Kedua, penapisan awal menggunakan metadata bibliografi ringkas; penilaian naskah lengkap, konfirmasi kriteria inklusi, dan appraisal kualitas terhadap korpus kandidat belum diselesaikan. Oleh karena itu, sintesis substantif pada tahap ini bersifat indikatif dan tidak dimaksudkan sebagai estimasi efek keseluruhan literatur. Ketiga, heterogenitas ukuran UMKM, sektor, tingkat digitalisasi, serta indikator kinerja organisasi membatasi transferabilitas hasil antar konteks. Studi lanjutan perlu menuntaskan dokumentasi kueri dan keputusan seleksi, melibatkan verifikasi independen apabila memungkinkan, serta menilai konsistensi temuan melalui pemisahan studi dengan ukuran kinerja objektif dan perseptual.

Referensi

Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs) in Saudi Arabia: The mediating and moderating role of cybersecurity resilience and organizational culture. Sustainability, 16(5), 1880. https://doi.org/10.3390/su16051880

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, 113580. https://doi.org/10.1016/j.dss.2021.113580

Arroyabe, M. F., Arranz, C. F. A., Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. Technology in Society, 78, 102670. https://doi.org/10.1016/j.techsoc.2024.102670

Awan, M., & Alam, A. (2025). Cybersecurity threats and defensive strategies for small and medium firms: A systematic mapping study. Administrative Sciences, 15(12), 481. https://doi.org/10.3390/admsci15120481

Awang Ali, Q. S., Hanafiah, M. H., & Mogindol, S. H. (2023). Systematic literature review of business continuity management (BCM) practices: Integrating organisational resilience and performance in small and medium enterprises (SMEs) BCM framework. International Journal of Disaster Risk Reduction, 99, 104135. https://doi.org/10.1016/j.ijdrr.2023.104135

Bahmanova, A., & Lace, N. (2026). Key factors shaping collaborative cyber resilience in SMEs through open innovation. Journal of Open Innovation: Technology, Market, and Complexity, 12(1), 100715. https://doi.org/10.1016/j.joitmc.2026.100715

Basri, W. S. (2023). Artificial intelligence, cyber security measures and SME's e-operational efficiency: Moderating role of employees perception of AI usefulness. Operational Research in Engineering Sciences: Theory and Applications, 6(4), 169–194. https://doi.org/10.31181/oresta/060409

Brezavšček, A., & Baggia, A. (2025). Recent trends in information and cyber security maturity assessment: A systematic literature review. Systems, 13(1), 52. https://doi.org/10.3390/systems13010052

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review, 50, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. Computers & Security, 145, 104026. https://doi.org/10.1016/j.cose.2024.104026

Eliot, D. (2024). NIST cybersecurity framework 2.0: Small business quick-start guide (NIST SP 1300). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1300

Fernandez de Arroyabe, J. C., Arroyabe, M. F., Fernandez, I., & Arranz, C. F. A. (2024). Cybersecurity resilience in SMEs: A machine learning approach. Journal of Computer Information Systems, 64(6), 711–727. https://doi.org/10.1080/08874417.2023.2248925

Gerst, M., Kappe, M., Härting, R.-C., & Karg, C. (2024). Determinants of the successful establishment of a cyber security culture in SMEs. Procedia Computer Science, 246, 510–518. https://doi.org/10.1016/j.procs.2024.09.431

Hoong, Y., Rezania, D., & Baker, R. (2024). When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands. Technology in Society, 78, 102650. https://doi.org/10.1016/j.techsoc.2024.102650

Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. International Journal of Information Management, 63, 102466. https://doi.org/10.1016/j.ijinfomgt.2021.102466

Molete, O. B., Mokhele, S. E., Ntombela, S. D., & Thango, B. A. (2025). The impact of IT strategic planning process on SME performance: A systematic review. Businesses, 5(1), 2. https://doi.org/10.3390/businesses5010002

Moneva, A., & Leukfeldt, R. (2023). Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. Journal of Criminology, 56(4), 416–440. https://doi.org/10.1177/26338076231161842

Neri, M., & Niccolini, F. (2025). On the path to cyber organizational resilience: Shedding light on the context of SMEs. International Journal of Organizational Analysis, 33(12), 105–131. https://doi.org/10.1108/IJOA-06-2024-4572

Neri, M., Niccolini, F., & Pugliese, R. (2022). Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey. Online Journal of Applied Knowledge Management, 10(2), 1–22. https://doi.org/10.36965/OJAKM.2022.10(2)1-22

OECD. (2022). OECD policy framework on digital security: Cybersecurity for prosperity. OECD Publishing. https://doi.org/10.1787/a69df866-en

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Pelletier, C., & Raymond, L. (2024). Investigating the strategic IT alignment process with a dynamic capabilities view: A multiple case study. Information & Management, 61(4), 103819. https://doi.org/10.1016/j.im.2023.103819

Rattanapong, P., Sukma, N., & Darakorn Na Ayuthaya, S. (2025). Determinants of cybersecurity investment in ASEAN organizations: An integrated structural equation modeling approach. Frontiers in Communications and Networks, 6, 1594554. https://doi.org/10.3389/frcmn.2025.1594554

Rawindaran, N., Jayal, A., & Prakash, E. (2025). Cybersecurity framework: Addressing resiliency in Welsh SMEs for digital transformation and Industry 5.0. Journal of Cybersecurity and Privacy, 5(2), 17. https://doi.org/10.3390/jcp5020017

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in Industry 5.0: A comparative study between Saudi Arabia and the United Kingdom. Digital, 3(3), 200–231. https://doi.org/10.3390/digital3030014

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Organizational Cyber Security, 1(1), 24–46. https://doi.org/10.1108/OCJ-03-2021-0004

Rethlefsen, M. L., Kirtley, S., Waffenschmidt, S., Ayala, A. P., Moher, D., Page, M. J., & Koffel, J. B. (2021). PRISMA-S: An extension to the PRISMA statement for reporting literature searches in systematic reviews. Systematic Reviews, 10, 39. https://doi.org/10.1186/s13643-020-01542-z

Rombaldo Junior, C., Becker, I., & Johnson, S. D. (2026). Unaware, unfunded, untrained, and unsupported: A systematic review of cybersecurity in small and medium enterprises. Journal of Cybersecurity, 12(1), tyag030. https://doi.org/10.1093/cybsec/tyag030

Stentoft, J., Peressotti, M., Mayer, P., Wickstrøm, K. A., Schmitt, O., Keating, V. C., Theussen, A., Tumchewics, L. A., & Kankam-Boateng, J. (2025). The relationship between cybersecurity awareness, cybersecurity supply chain risk management and firm performance. Supply Chain Management, 30(5), 497–517. https://doi.org/10.1108/SCM-11-2024-0765

Taskin, N., Özkeleş Yıldırım, A., Ercan, H. D., Wynn, M., & Metin, B. (2025). Cyber insurance adoption and digitalisation in small and medium-sized enterprises. Information, 16(1), 66. https://doi.org/10.3390/info16010066

Ye, W. (2026). Strengthening cybersecurity in small and medium-sized enterprises: Balancing technology, costs, compliance, and employee awareness. SAGE Open, 16(1). https://doi.org/10.1177/21582440251414951

Yigit Ozkan, B., & Spruit, M. (2023). Adaptable security maturity assessment and standardization for digital SMEs. Journal of Computer Information Systems, 63(4), 965–987. https://doi.org/10.1080/08874417.2022.2119442