Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.4604

Eksplorasi Peran Manajemen Risiko Dalam Meningkatkan Efektivitas Keamanan Siber Pada Badan Siber Dan Sandi Negara

Chairul Akbar Hutasuhut
Fakultas Ekonomi dan Bisnis, Universitas Trisakti, Jakarta, Indoneisa
Email Korespondensi: akbar1994@yahoo.com

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Februari 2026, Article published: 01 Maret 2026

ABSTRACT
This study explores the role of risk management as a strategic instrument in enhancing the effectiveness of cybersecurity within the National Cyber and Crypto Agency of Indonesia (Badan Siber dan Sandi Negara – BSSN). The research adopts an exploratory qualitative approach, with data collected through policy document analysis, semi structured interviews with key informants within BSSN, and limited observations of operational activities related to risk management practices. Data were analyzed using thematic analysis to identify patterns, relationships, and mechanisms through which risk management contributes to cybersecurity effectiveness. The findings indicate that risk management functions not only as a technical mechanism for threat mitigation but also as a governance instrument that strengthens strategic decision making, operational effectiveness in incident response, and the development of a risk aware organizational culture. At the strategic level, organizational risk management supports the prioritization of capacity building initiatives and the formulation of national cybersecurity threat mitigation policies. At the operational and institutional levels, a risk based approach improves the efficiency of resource allocation, enhances incident response preparedness, and fosters a risk aware culture that reinforces decision making accountability. Nevertheless, the study also identifies key challenges, including limited human resource capacity in risk analysis and the rapidly evolving nature of cyber threats. This study recommends strengthening human resource capacities in cybersecurity risk analysis, implementing adaptive and continuous risk reassessment mechanisms, developing a cybersecurity risk metrics framework, and enhancing inter agency coordination. The findings are expected to contribute to the academic discourse on public sector cybersecurity risk management and to serve as a policy reference for strengthening Indonesia's national cyber resilience.
Keywords: *Risk Management, Cybersecurity, Cyber Governance, Organizational Effectiveness, BSSN*

ABSTRAK
Penelitian ini mengeksplorasi peran manajemen risiko sebagai instrumen strategis dalam meningkatkan efektivitas keamanan siber pada Badan Siber dan Sandi Negara (BSSN). Penelitian menggunakan pendekatan kualitatif eksploratif dengan teknik pengumpulan data melalui analisis dokumen kebijakan, wawancara semi terstruktur dengan informan kunci di lingkungan BSSN, serta observasi terbatas terhadap aktivitas operasional terkait pengelolaan risiko. Analisis data dilakukan menggunakan pendekatan analisis tematik untuk mengidentifikasi pola, hubungan, dan mekanisme kontribusi manajemen risiko terhadap efektivitas keamanan siber. Hasil penelitian menunjukkan bahwa manajemen risiko

berfungsi tidak hanya sebagai mekanisme teknis mitigasi ancaman, tetapi juga sebagai instrumen tata kelola (governance) yang memperkuat pengambilan keputusan strategis, efektivitas operasional respons insiden, serta pembentukan budaya organisasi yang sadar risiko. Secara strategis, pendekatan manajemen risiko organisasi turut mendukung penetapan prioritas pembinaan dan kebijakan mitigasi ancaman siber nasional. Pada tingkat operasional dan kelembagaan, pendekatan berbasis risiko meningkatkan efisiensi alokasi sumber daya, memperkuat kesiapan respons insiden, serta mendorong terbentuknya budaya organisasi yang sadar risiko dan meningkatkan akuntabilitas pengambilan keputusan. Namun demikian, penelitian ini juga mengidentifikasi sejumlah tantangan utama, yaitu keterbatasan kapasitas sumber daya manusia dalam analisis risiko serta dinamika ancaman siber yang berkembang sangat cepat. Penelitian ini merekomendasikan penguatan kapasitas SDM analisis risiko, penerapan mekanisme evaluasi ulang risiko yang adaptif dan berkelanjutan, pengembangan kerangka metrik risiko siber, serta penguatan koordinasi lintas instansi. Temuan penelitian ini diharapkan dapat memberikan kontribusi akademik dalam pengembangan kajian manajemen risiko siber sektor publik serta menjadi rujukan kebijakan bagi penguatan ketahanan siber nasional Indonesia.
Kata Kunci: *Manajemen Risiko, Keamanan Siber, Tata Kelola Siber, Efektivitas Organisasi, BSSN*

PENDAHULUAN

Transformasi digital dalam penyelenggaraan pemerintahan yang ditetapkan dalam konsep Sistem Pemerintahan Berbasis Elektronik (SPBE) telah meningkatkan ketergantungan negara terhadap sistem elektronik untuk mendukung layanan publik, pengelolaan data strategis, serta operasional infrastruktur kritis nasional. Di sisi lain, ketergantungan ini secara simultan meningkatkan eksposur pemerintah terhadap ancaman siber yang semakin kompleks, masif, dan bersifat lintas batas negara. Ancaman siber tidak lagi terbatas pada gangguan teknis, tetapi berpotensi menimbulkan dampak strategis terhadap keberlangsungan layanan publik, kepercayaan masyarakat, stabilitas ekonomi, dan bahkan keamanan nasional.

Dalam konteks Indonesia, Badan Siber dan Sandi Negara (BSSN) memegang peran sentral sebagai otoritas nasional dalam bidang keamanan siber dan sandi. BSSN tidak hanya bertanggung jawab terhadap aspek operasional teknis pengamanan sistem elektronik, tetapi juga berperan dalam perumusan kebijakan, penetapan standar nasional, serta pembinaan kapasitas keamanan siber di seluruh kementerian, lembaga, dan pemerintah daerah. Kompleksitas peran tersebut menempatkan BSSN pada posisi strategis yang menuntut pendekatan pengelolaan keamanan siber yang sistematis, terukur, dan berbasis risiko.

Berbagai laporan resmi menunjukkan bahwa ancaman siber terhadap sektor pemerintahan di Indonesia berada pada tingkat yang mengkhawatirkan. Dalam Dokumen Lanskap Keamanan Siber Indonesia 2024 yang dikeluarkan oleh Direktorat Operasi Keamanan Siber tercatat bahwa total trafik anomali di Indonesia selama tahun 2024 adalah 330.527.636 anomali, 241 dugaan insiden kebocoran data, hingga temuan *data exposure* sejumlah 56.128.160. Kondisi ini menegaskan bahwa pendekatan keamanan siber yang reaktif dan berfokus semata pada solusi teknis tidak lagi memadai. Diperlukan pendekatan manajemen risiko yang mampu

mengintegrasikan dimensi strategis, operasional, kelembagaan, dan kebijakan dalam satu kerangka pengelolaan yang komprehensif.

Literatur internasional dan nasional menegaskan bahwa manajemen risiko merupakan fondasi utama dalam membangun ketahanan siber organisasi, khususnya di sektor publik. Penelitian oleh Syarifa Tommy dan Muhammad Irwan Padli Nasution (2025) mengevaluasi manajemen risiko keamanan siber pada Pusat Data Nasional (PDN) sebagai sebuah infrastruktur kritis milik pemerintah. Mereka menemukan bahwa kelemahan dalam manajemen keamanan, pencadangan data, dan tata kelola sistem berkontribusi pada kerentanan pemerintah terhadap insiden siber besar. Kasus tersebut menyoroti betapa pentingnya integrasi manajemen risiko dalam sistem publik karena kegagalan mengelola risiko dapat mengganggu operasional nasional secara luas. Dalam lingkungan BSSN sendiri, penelitian kebijakan dan operasional mengenai manajemen risiko juga mulai muncul. Sebagai contoh, penelitian oleh Jefferson Benyamin, Much Mualim, dan Editha Praditya Duarte (2023) mengkaji manajemen risiko keamanan informasi di Pusat Data dan Teknologi Informasi Komunikasi BSSN. Mereka mengidentifikasi bahwa penerapan manajemen risiko di pusat data BSSN sangat penting untuk meningkatkan pertahanan siber nasional dan mengurangi potensi ancaman. Penelitian semacam ini secara langsung relevan karena menggambarkan bagaimana manajemen risiko berjalan di dalam lembaga BSSN dan bagaimana hal tersebut dapat memengaruhi efektivitas pertahanan siber nasional.

Penerapan manajemen risiko di pemerintahan juga menghadapi tantangan khas sektor publik, seperti kebutuhan koordinasi antar lembaga, keterbatasan sumber daya manusia, dan tata kelola anggaran. Dalam diskusi kebijakan nasional, misalnya dalam Focus Group Discussion (FGD) yang diselenggarakan oleh Fakultas Hukum Universitas Indonesia bersama BSSN dan Microsoft Indonesia, para pemangku kepentingan menyoroti bahwa risiko siber di sektor industri dan pemerintahan tidak bisa diatasi hanya dengan teknologi sehingga diperlukan pendekatan manajerial dan regulatif. Diskusi ini juga menunjukkan bahwa pemangku kebijakan harus menciptakan mekanisme manajemen risiko yang mempertimbangkan kerentanan struktural dan kebijakan publik agar sistem keamanan siber nasional dapat dikelola secara holistik.

Selain tantangan tersebut, kajian empiris yang secara khusus mengeksplorasi bagaimana manajemen risiko diterapkan dan dioperasionalkan pada lembaga keamanan siber nasional di Indonesia masih sangat terbatas. Sebagian besar penelitian cenderung berfokus pada aspek teknis keamanan atau evaluasi kebijakan secara normatif. Berdasarkan kesenjangan tersebut, penelitian ini bertujuan untuk mengeksplorasi secara mendalam peran manajemen risiko dalam meningkatkan efektivitas keamanan siber di BSSN. Secara khusus, penelitian ini berupaya menjawab pertanyaan penelitian sebagai berikut: (1) bagaimana mekanisme manajemen risiko diterapkan dalam konteks strategis dan operasional di BSSN; (2) bagaimana kontribusi manajemen risiko terhadap efektivitas keamanan siber; dan (3) apa saja tantangan utama yang dihadapi dalam implementasi manajemen risiko di BSSN. Temuan penelitian ini diharapkan dapat memberikan kontribusi teoritis dan praktis bagi pengembangan tata kelola keamanan siber nasional.

Dalam mengkaji peran manajemen risiko terhadap efektivitas keamanan siber di BSSN, diperlukan pemahaman mendalam mengenai beberapa konsep inti, yaitu manajemen risiko, tata kelola keamanan, manajemen risiko SPBE, serta integrasi manajemen risiko dan efektivitas keamanan. Teori-teori ini menjadi landasan konseptual untuk menjelaskan bagaimana manajemen risiko secara sistematis dapat memperkuat ketahanan siber dan meningkatkan efektivitas keamanan di instansi pemerintah seperti BSSN.

Manajemen risiko merupakan proses sistematis yang mencakup identifikasi, analisis, evaluasi, dan penanganan risiko guna meminimalkan dampak negatif dan mendukung pencapaian tujuan organisasi. Dalam konteks sektor publik, manajemen risiko memiliki dimensi tambahan berupa tuntutan akuntabilitas, kepatuhan regulasi, serta perlindungan kepentingan publik. Dalam studi tentang faktor keberhasilan implementasi manajemen risiko di instansi pemerintah, Jauhari, Sukmadilaga, dan Mulyani (2021) menemukan bahwa *Critical Success Factor* (CSF) untuk manajemen risiko mencakup komitmen pimpinan, kultur organisasi, kompetensi SDM, serta proses formal manajemen risiko. CSF ini sangat relevan bagi BSSN, karena leadership dan kultur organisasi yang mendukung risiko adalah fondasi agar manajemen risiko dapat berjalan efektif (Jauhari et al., 2021).

Dalam konteks kebijakan keamanan siber nasional, studi oleh Sutomo, Thamrin, Widodo, dan Reksoprodjo (2025) mengembangkan model strategi pertahanan siber berbasis manajemen risiko. Penelitian tersebut menekankan pentingnya kerja sama lintas sektor, perencanaan strategis, dan evaluasi berkelanjutan untuk mencapai ketahanan digital nasional. Model ini dapat diterapkan sebagai kerangka teoretis dalam penelitian pada BSSN karena BSSN memiliki peran koordinatif dan strategis dalam menerapkan pembinaan dan penyusunan kebijakan siber nasional (Sutomo et al., 2025).

Tata kelola keamanan siber mengacu pada struktur, proses, dan mekanisme yang memastikan bahwa risiko siber dikelola secara selaras dengan tujuan strategis organisasi. Pendekatan tata kelola menekankan keterlibatan pimpinan, penggunaan metrik risiko, serta integrasi keamanan siber dalam kebijakan dan perencanaan organisasi. Dalam organisasi publik strategis seperti BSSN, tata kelola siber berperan sebagai jembatan antara kebijakan nasional dan implementasi teknis.

Literatur kontemporer menekankan bahwa tata kelola keamanan siber harus berbasis data dan metrik yang memungkinkan pengambilan keputusan strategis oleh manajemen puncak. Dalam tinjauan sistematis oleh Modi, Kuzminykh, dan Ghita (2023), ditemukan bahwa pimpinan eksekutif, seperti dewan atau eksekutif lembaga sering kekurangan instrumen metrik yang dapat mereka gunakan untuk mengelola risiko siber dalam bahasa yang mereka pahami. Mereka menyimpulkan bahwa pendekatan berbasis data *(data driven*) dalam tata kelola siber sangat penting agar pengambilan keputusan terinformasi dan akuntabel (Modi, Kuzminykh, & Ghita, 2023).

Tata kelola yang kuat memungkinkan manajemen risiko menjadi bagian integral dari manajemen strategis, bukan sekedar mekanisme teknis. Dalam konteks pemerintahan, hal ini berarti bahwa BSSN tidak hanya bertindak sebagai operator teknis, tetapi juga sebagai koordinator kebijakan, pembuat pedoman, dan

pemangku kepentingan utama dalam menetapkan standar nasional terkait mitigasi risiko siber.

Manajemen risiko, dalam konteks organisasi modern, merupakan proses sistematis yang mencakup identifikasi risiko, analisis, evaluasi, dan penanganan (treatment) risiko untuk meminimalkan dampak negatif dan memaksimalkan peluang (Asiyanti & Agussalim, 2024). Dalam sektor publik, manajemen risiko juga berfungsi sebagai alat pengendalian tata kelola dan akuntabilitas karena organisasi publik harus mempertimbangkan risiko tidak hanya dari sisi teknis, tetapi juga reputasi, kepatuhan, dan kontinuitas layanan.

Berdasarkan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (SPBE), manajemen risiko SPBE adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur dan budaya untuk menentukan tindakan terbaik terkait risiko SPBE. Tujuan dari impelementasi pedoman tersebut bagi organisasi publik adalah untuk meningkatkan kemungkinan pencapaian tujuan penerapan SPBE, memberikan dasar yang kuat untuk perencanaan dan pengambilan keputusan, meningkatkan optimalisasi pemanfaatan sumber daya, serta menciptakan budaya sadar risiko bagai pegawai di lingkungan organisasi.

Dalam manajemen risiko SPBE, yang digunakan sebagai proses yang dapat mengurangi munculnya dampak yang merugikan atau risiko yang dapat memberikan akibat bagi organisasi pemerintah, terdapat risiko negatif sekaligus risiko positif yang akan mempengaruhi keberhasilan terhadap pencapaian tujuan penerapan SPBE (Kurniati, Nugroho, & Rizal, 2020). Di lingkungan organisasi sebagaimana dicontohkan dalam studi literatur di Dinas Komunikasi dan Informatika Pemerintah Kota Balikpapan, manajemen risiko SPBE juga dapat menjadikan pegawai patuh dan menciptakan budaya sadar risiko dalam penerapan SPBE (Rahadian Bisma, 2022).

Secara kerangka kerja, pedoman manajemen risiko tersebut mengadopsi standar internasional yaitu ISO 31000:2018. Standar ini memberikan panduan lintas sektor untuk membangun sistem manajemen risiko yang *robust* dan berkelanjutan. Dalam studi kasus instansi pemerintah, penerapan ISO 31000 telah terbukti efektif dalam meningkatkan tata kelola dan kinerja organisasi. Sebagai contoh, pada tingkat unit teknis pemerintahan, Febriyanti, Febrinazahra, dan Masdiyasa (2024) mengeksplorasi manajemen risiko sistem informasi di unit BPIW Kementerian PUPR menggunakan ISO 31000:2018. Hasil penelitian menunjukkan bahwa kerangka tersebut dapat membantu unit organisasi dalam menetapkan konteks risiko (*risk context*), menilai profil risiko, dan merancang strategi mitigasi yang sesuai dengan kapasitas organisasi. Temuan ini memperkuat relevansi ISO 31000 dalam konteks pemerintahan, termasuk di sektor keamanan siber, di mana konteks risiko sangat dinamis dan menyentuh berbagai lapisan operasional dan strategis (Febriyanti et al., 2024).

Dengan demikian, Pedoman Manajemen Risiko SPBE adalah landasan teoretis penting dalam penelitian ini. Dalam konteks BSSN, manajemen risiko SPBE memungkinkan organisasi tidak hanya merespons ancaman siber secara reaktif,

tetapi juga merencanakan mitigasi dan pemulihan secara strategis melalui pemahaman risiko yang menyeluruh dan terstruktur. Kerangka ini memberikan pijakan konseptual untuk menggambarkan bagaimana risiko dapat dikelola secara proaktif sebagai bagian dari strategi keamanan siber organisasi yang mendukung penguatan pembinaan keamanan siber sektoral.

Efektivitas keamanan siber dapat dilihat dari kemampuan organisasi dalam mendeteksi, merespons, dan memulihkan diri dari insiden siber, serta menjaga keberlangsungan layanan. Manajemen risiko berperan sebagai mekanisme pengarah yang memastikan bahwa upaya keamanan siber difokuskan pada ancaman dengan tingkat risiko tertinggi dan selaras dengan kapasitas organisasi.

Lebih jauh, literatur menyebutkan bahwa manajemen risiko bukan sekadar respons teknis, tetapi juga budaya organisasi. Asiyanti dan Agussalim (2024) dalam kajian mereka menjelaskan bahwa risiko dalam ekonomi digital mencakup risiko teknologi dan non teknologi, dan bahwa strategi manajemen risiko harus mencakup pelatihan, kesadaran, dan penyesuaian kebijakan agar risiko terkelola. Dalam organisasi publik seperti BSSN, budaya risiko yang matang (*risk aware culture*) penting agar semua lapisan pegawai, dari teknis hingga kebijakan, memahami peran mereka dalam mitigasi risiko dan pemulihan.

Selain itu, kemampuan penilaian risiko yang lebih matang, seperti melalui kerangka manajemen risiko SPBE, memberikan dasar kuantitatif yang lebih baik bagi manajemen dan pengambil kebijakan. Hal ini memungkinkan BSSN untuk melakukan alokasi anggaran mitigasi berdasarkan analisis risiko nyata dan proyeksi biaya kerugian, bukan hanya berdasarkan intuisi atau kepanikan reaktif. Selain itu, tata kelola berbasis metrik (*data driven governance*) memungkinkan laporan risiko siber yang akuntabel dan transparan di level manajemen puncak, memperkuat legitimasi kebijakan dan memfasilitasi dukungan lintas lembaga (Modi et al., 2023).

Penelitian ini menggunakan kerangka konseptual yang menempatkan manajemen risiko sebagai mekanisme penghubung antara tata kelola keamanan siber dan efektivitas operasional organisasi. Kerangka ini disusun untuk menjelaskan bagaimana proses manajemen risiko memengaruhi kinerja keamanan siber secara sistematis dalam konteks organisasi publik strategis seperti BSSN. Secara konseptual, kerangka penelitian ini terdiri atas tiga komponen utama yang saling berhubungan sebagaimana tercantum dalam Gambar 1.

Gambar 1. Kerangka Konseptual Peran Manajemen Risiko terhadap Efektivitas Keamanan Siber

Pertama, *input* manajemen risiko, yang mencakup proses identifikasi risiko siber, analisis dan evaluasi risiko, penetapan prioritas mitigasi, serta pemantauan dan evaluasi berkelanjutan. Input ini merepresentasikan kapasitas awal organisasi dalam mengenali ancaman dan kerentanan yang relevan dengan mandat strategis dan operasionalnya.

Kedua, proses keamanan siber, yang mencerminkan bagaimana *input* manajemen risiko diinternalisasikan ke dalam aktivitas operasional keamanan siber. Proses ini meliputi kemampuan identifikasi dan deteksi insiden, mekanisme respons insiden, serta proses pemulihan dan keberlangsungan layanan. Pada tahap ini, manajemen risiko berfungsi sebagai pengarah alokasi sumber daya, penyusunan prosedur operasional standar, dan jalur eskalasi pengambilan keputusan.

Ketiga, *outcome* efektivitas keamanan siber, yang ditunjukkan melalui tingkat kesiapan organisasi menghadapi ancaman siber, kecepatan dan ketepatan respons insiden, kemampuan pemulihan sistem dan layanan publik, serta terbentuknya budaya organisasi yang sadar risiko. *Outcome* ini menjadi indikator keberhasilan implementasi manajemen risiko dalam mendukung ketahanan siber organisasi.

Hubungan antar ketiga komponen tersebut bersifat dinamis dan iteratif. Hasil dari outcome efektivitas keamanan siber memberikan umpan balik (*feedback loop*) terhadap proses manajemen risiko melalui pembaruan penilaian risiko, penyesuaian kebijakan, dan peningkatan kapasitas organisasi. Dengan demikian, manajemen risiko dipahami sebagai proses berkelanjutan yang terus beradaptasi terhadap dinamika ancaman siber dan perubahan lingkungan strategis.

Kerangka konseptual ini digunakan sebagai lensa analitis dalam penelitian untuk menafsirkan temuan empiris dan menjelaskan mekanisme kontribusi manajemen risiko terhadap efektivitas keamanan siber di BSSN.

METODE

Penelitian ini menggunakan pendekatan kualitatif eksploratif untuk memperoleh pemahaman mendalam mengenai penerapan manajemen risiko keamanan siber di BSSN. Data dikumpulkan melalui analisis dokumen kebijakan dan laporan resmi, wawancara semi terstruktur dengan informan kunci yang dipilih secara purposif, serta observasi terbatas terhadap aktivitas operasional terkait manajemen risiko. Pilihan pendekatan kualitatif eksploratif didasarkan pada kenyataan bahwa fenomena manajemen risiko siber di instansi pemerintah seperti BSSN sangat kompleks, melibatkan banyak aktor, kebijakan, budaya organisasi, dan variabel kontekstual yang sulit diukur secara kuantitatif dengan cepat. Dengan metode ini, penelitian dapat menangkap nuansa dan dinamika implementasi manajemen risiko yang mungkin tersembunyi dalam kebijakan formal maupun praktik sehari-hari. Pengumpulan data dilakukan melalui beberapa teknik. Pertama, studi dokumenter merupakan sumber utama data primer. Dokumen yang dianalisis mencakup kebijakan BSSN terkait manajemen risiko, pedoman keamanan informasi, rencana strategi keamanan siber nasional, laporan tahunan BSSN, serta materi internal seperti panduan respons insiden dan struktur organisasi risiko. Dokumen-dokumen ini memberikan landasan untuk memahami kerangka formal manajemen risiko BSSN, termasuk bagaimana risiko diidentifikasi, dinilai, dan dimitigasi dalam konteks operasional dan strategis. Kedua, penelitian menggunakan wawancara semi terstruktur dengan informan kunci di BSSN sesuai dengan struktur manajemen risiko organisasi serta pimpinan dan satuan kerja yang melaksanakan pembinaan keamanan siber sektoral. Informan dipilih secara purposif, berdasarkan posisi institusional dan pengetahuan mereka tentang manajemen risiko dan operasi keamanan siber, sehingga wawancara dapat menggali persepsi, praktik, hambatan, dan masukan strategis dari dalam. Ketiga, penelitian juga melakukan observasi partisipatif konseptual, di mana peneliti meninjau kegiatan BSSN yang terkait manajemen risiko, seperti simulasi insiden siber, workshop pelatihan, dan rapat koordinasi antar unit untuk memperoleh gambaran nyata bagaimana manajemen risiko diimplementasikan dalam aktivitas sehari-hari.

Analisis data dilakukan menggunakan analisis tematik melalui tahapan pengodean terbuka, pengelompokan tema, dan penafsiran hubungan antar tema. Untuk menjaga keabsahan data, penelitian menerapkan triangulasi sumber (antara dokumen kebijakan, wawancara, dan observasi), *member checking* (ringkasan hasil disampaikan kembali kepada beberapa informan kunci untuk meminta konfirmasi apakah interpretasi benar mencerminkan pengalaman dan pandangan mereka), serta pencatatan audit selama proses analisis untuk memungkinkan keterlacakan cara analisis tema terbentuk dan bagaimana kesimpulan ditarik. Pertimbangan etika penelitian dijaga melalui pemberian informed consent dan perlindungan kerahasiaan informan. Adapun batasan penelitian diakui sebagai bagian penting dari metodologi. Karena sifat kualitatif dan eksploratif, hasil penelitian tidak dapat digeneralisasikan secara kuantitatif ke semua instansi pemerintah atau ke skala nasional. Temuan bersifat kontekstual dan sangat tergantung pada struktur organisasi, kebijakan, dan kultur di BSSN; instansi lain mungkin memiliki dinamika berbeda. Selain itu, akses ke dokumen internal BSSN mungkin terbatas, terutama

dokumen yang sangat sensitif, sehingga data bisa jadi tidak komprehensif. Dalam wawancara, informan mungkin bersikap *politically correct* atau membatasi ungkapan kritik terhadap kebijakan organisasi, yang dapat menimbulkan bias. Peneliti harus menyadari kemungkinan bias sosial desirabilitas dan berupaya memitigasinya melalui pertanyaan wawancara yang netral dan reflektif. Dengan metodologi dan kerangka konseptual seperti ini, penelitian diharapkan dapat menghasilkan pemahaman komprehensif tentang praktik manajemen risiko di BSSN dan bagaimana praktik tersebut berkontribusi pada efektivitas keamanan siber. Penelitian tidak hanya menjadi deskriptif, tetapi juga analitis, memberikan insight bagi pembuat kebijakan, pemimpin organisasi BSSN, dan pemangku kepentingan terkait untuk meningkatkan tata kelola risiko siber nasional.

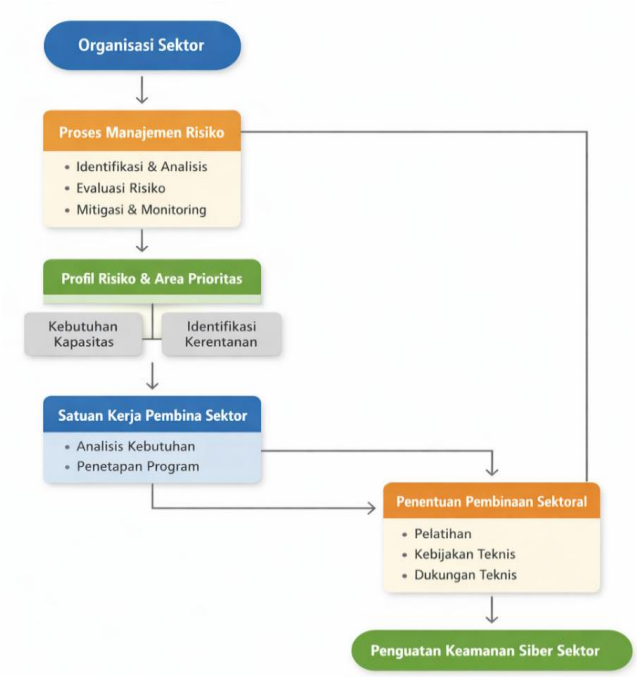
HASIL DAN PEMBAHASAN

Hasil analisis menunjukkan bahwa manajemen risiko di BSSN berkontribusi signifikan terhadap efektivitas keamanan siber pada tiga dimensi utama, yaitu strategis, operasional, dan kelembagaan. Pada dimensi strategis, pendekatan manajemen risiko organisasi turut mendukung penetapan prioritas pembinaan dan kebijakan mitigasi ancaman siber nasional. Pada dimensi operasional, pendekatan berbasis risiko meningkatkan efisiensi alokasi sumber daya dan memperkuat kesiapan respons insiden. Pada dimensi kelembagaan, manajemen risiko mendorong terbentuknya budaya organisasi yang sadar risiko dan meningkatkan akuntabilitas pengambilan keputusan.

Dimensi Strategis

Dari perspektif strategis, proses identifikasi dan evaluasi risiko yang diterapkan oleh BSSN mencerminkan pemahaman bahwa ancaman siber adalah elemen sistemik dan tidak dapat diselesaikan hanya dengan solusi teknis. Dalam wawancara dengan para informan kunci BSSN, terlihat bahwa manajemen risiko bukan hanya digunakan untuk menyusun kebijakan internal, tetapi juga sebagai dasar pembinaan keamanan siber nasional dan sebagai instrumen koordinasi lintas instansi. Dengan demikian, BSSN menggunakan pendekatan manajemen risiko organisasi pada proses pembinaan sektoral sebagai landasan tata kelola (*governance*) keamanan siber nasional, sehingga keputusan strategis terkait prioritas mitigasi ancaman dilakukan berdasarkan analisis risiko yang sistematis dan berbasis data.

Implementasi manajemen risiko yang diterapkan dalam organisasi mendukung identifikasi risiko oleh unit kerja pembina sektor terhadap layanan dan profil keamanan siber sektoral sehingga turut mendukung penentuan rencana perbaikan berkelanjutan dalam proses pembinaan keamanan siber sektoral. Secara sederhana, proses tersebut ditunjukkan dalam Gambar 2 di bawah ini.



Gambar 2. Proses Implementasi Manajemen Risiko dalam Penentuan Pembinaan Keamanan Siber Sektoral

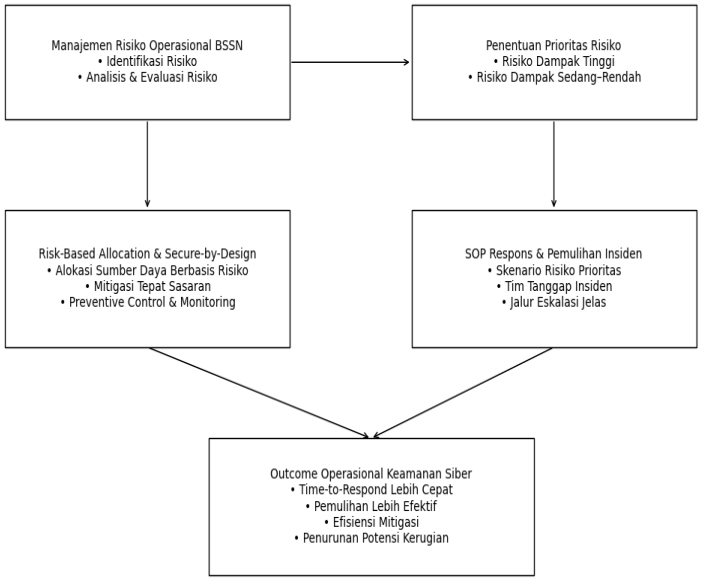
Temuan ini sejalan dengan literatur kontemporer yang menekankan pentingnya tata kelola siber berbasis metrik (*data driven governance*). Studi sistematis oleh Modi, Kuzminykh, dan Ghita (2023) misalnya menyoroti bahwa dewan pengambil keputusan di banyak organisasi (termasuk publik) sering kekurangan metrik yang relevan dalam bahasa yang dapat mereka pahami, sehingga pendekatan berbasis data sangat diperlukan agar keputusan strategis dapat mencerminkan risiko siber secara nyata. Dengan demikian, BSSN yang telah mengintegrasikan analisis risiko ke dalam pengambilan keputusan strategis menunjukkan kematangan tata kelola siber yang tidak hanya responsif tetapi proaktif.

Dimensi Operasional

Pada aspek operasional, manajemen risiko di BSSN memperkuat efektivitas keamanan siber melalui implementasi konsep *secure by design* untuk mekanisme mitigasi yang lebih tepat sasaran dan efisien sebagaimana ditampilkan dalam Gambar 3. Dari analisis dokumen dan observasi kegiatan operasional, terlihat bahwa BSSN mengalokasikan sumber daya mitigasi berdasarkan hasil penilaian risiko, contohnya adalah skenario ancaman dengan dampak tinggi mendapatkan prioritas tindakan mitigasi, sedangkan ancaman dengan efek lebih rendah ditangani melalui kebijakan preventif dan pemantauan. Hal ini mendukung hasil studi kasus di publik sektor Indonesia, seperti penelitian oleh Syarifa Tommy dan Nasution (2025) yang mengevaluasi manajemen risiko di Pusat Data Nasional (PDN). Mereka menemukan bahwa kegagalan pengelolaan risiko *(risk governance*) terkait cadangan data, backup, dan kebijakan respons insiden menjadi penyebab utama kebocoran

data dan serangan ransomware. Dengan mengadopsi pendekatan *risk based allocation*, BSSN dapat meningkatkan efisiensi mitigasi sekaligus mengurangi potensi kerugian besar bila insiden terjadi.

Lebih lanjut, manajemen risiko juga memperkuat proses respons dan pemulihan. Dalam wawancara dengan pimpinan di unit kerja yang membidangi *security operation center* di BSSN, peneliti menemukan bahwa Standar Operasional Prosedur (SOP) respons insiden disusun berdasarkan hasil analisis risiko. Impelementasi yang diterapkan berupa skenario yang telah diidentifikasi sebagai prioritas risiko tinggi memiliki prosedur respons insiden yang jelas, tim tanggap insiden yang siap siaga, dan jalur eskalasi yang telah ditetapkan. Pendekatan ini memperpendek waktu tanggap (*time to respond*) dan memperlancar proses pemulihan. Analisis ini konsisten dengan prinsip manajemen risiko yang dikemukakan dalam literatur manajemen siber modern, di mana penilaian risiko menjadi dasar untuk merancang rencana respons dan pemulihan yang efektif.

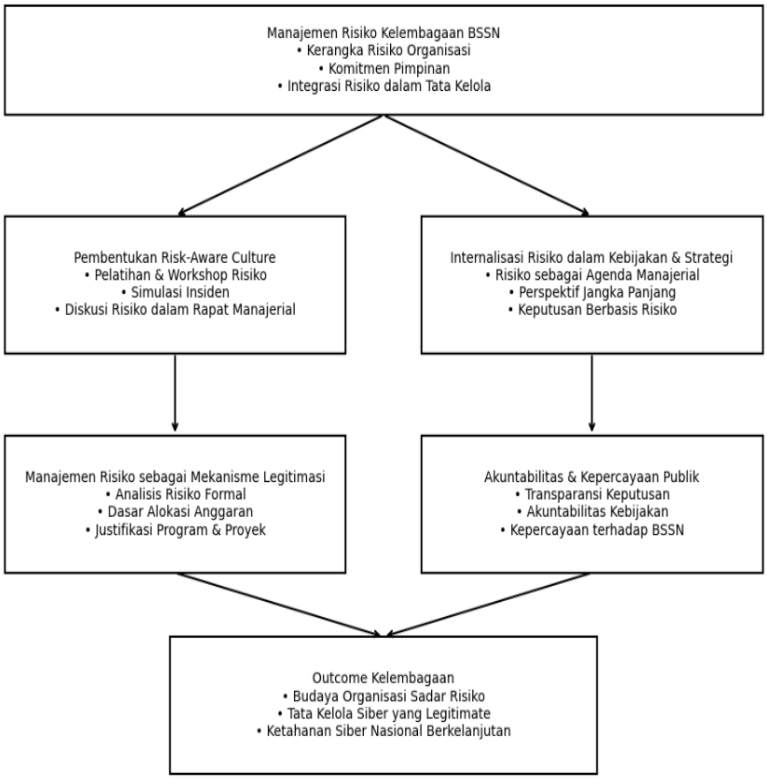


Gambar 3. Alur Manajemen Risiko dalam Dimensi Operasional di BSSN

Dimensi Kelembagaan

Dari sisi kelembagaan dan budaya organisasi, manajemen risiko berhasil mendorong terbentuknya budaya risiko (*risk aware culture*) di BSSN. Budaya ini tercermin dalam pelatihan rutin, workshop evaluasi risiko, dan simulasi insiden yang melibatkan banyak unit. Staf BSSN yang diwawancara menyebut bahwa diskusi risiko menjadi bagian dari rapat manajerial rutin sehingga proses identifikasi risiko tidak lagi hanya di tingkat teknis, tetapi juga dibahas dalam konteks kebijakan dan strategi jangka panjang. Budaya semacam ini sangat penting agar manajemen risiko tidak menjadi dokumen formal semata, melainkan bagian hidup dari tata kelola organisasi. Literatur mendukung pentingnya kultur risiko, menunjukkan bahwa dalam ekosistem digital, proses manajemen risiko harus meliputi komitmen organisasi dan budaya kesadaran risiko agar mitigasi dapat berjalan efektif dan adaptif (Asiyanti dan Agussalim, 2024).

Analisis lebih lanjut menyoroti bahwa manajemen risiko di BSSN juga berfungsi sebagai mekanisme legitimasi kebijakan. Karena BSSN beroperasi dalam ranah publik dan tanggung jawab nasional, keputusan alokasi anggaran untuk mitigasi risiko siber atau investasi peningkatan kapabilitas SDM siber harus dapat dipertanggungjawabkan. Dokumentasi internal menunjukkan bahwa setiap kebijakan besar maupun proyek mitigasi risiko disertai dengan analisis risiko formal yang dipresentasikan kepada pimpinan dan pemangku kebijakan. Hal ini memperkuat akuntabilitas lembaga dan menumbuhkan kepercayaan publik terhadap komitmen BSSN untuk menjaga keamanan ruang siber nasional. Model ini selaras dengan gagasan governance cyber yang berbasis metrik dan akuntabilitas, sebagaimana dijelaskan oleh studi sistematis dari Modi et al. (2023). Proses manajemen risiko dari sudut pandang kelembagaan ditunjukkan dalam Gambar 4 di bawah ini.



Gambar 4. Alur Manajemen Risiko dalam Dimensi Kelembagaan di BSSN

Tantangan Implementasi

Dalam proses analisis data penelitian, teridentifikasi sejumlah tantangan yang secara signifikat membatasi efektivitas manajemen risiko di BSSN. Salah satu isu utama adalah keterbatasan kapasitas SDM. Meskipun ada pelatihan dan workshop, beberapa informan menyatakan bahwa belum semua staf memiliki kompetensi analisis risiko yang mendalam. Dalam wawancara, unit kepatuhan risiko menyebut bahwa evaluasi risiko strategis seringkali melibatkan tim kecil, sementara unit operasional lebih banyak terfokus pada tugas teknis sehari-hari. Kondisi ini berpotensi menciptakan kesenjangan antara analisis risiko strategis dan implementasi operasional mitigasi. Tantangan kapasitas ini konsisten dengan kajian

di sektor publik lain, di mana regulasi dan kebijakan mungkin sudah matang, tetapi eksekusi teknis dan sumber daya manusia menjadi *bottleneck* signifikan.

Tantangan kedua yang muncul adalah dinamika ancaman yang cepat. Sebagian informan mencatat bahwa skenario risiko yang dinilai dalam penilaian risiko strategis menjadi kurang relevan setelah beberapa waktu karena munculnya faktor ancaman baru, seperti eksploit IoT, serangan ransomware mutakhir, dan gangguan *supply chain* pada pengelolaan keamanan siber. Karena itu, analisis risiko harus bersifat adaptif dan terus diperbarui agar mitigasi yang dirancang tetap efektif. Namun, proses pembaruan analisis risiko menghadapi kendala birokrasi dan keterbatasan sumber daya, terutama dalam mengorganisir workshop evaluasi ulang, simulasi skenario baru, dan uji pemulihan insiden. Situasi ini menegaskan bahwa manajemen risiko di BSSN harus bersifat dinamis dan iteratif, bukan statis.

Secara konseptual, analisis tematik dari data penelitian menggambarkan sebuah model kontribusi manajemen risiko terhadap efektivitas keamanan siber di BSSN yang terdiri dari tiga dimensi utama yaitu peningkatan kesiapan dan mitigasi melalui risiko strategis, peningkatan respons dan pemulihan insiden, dan pembentukan budaya risiko serta legitimasi kebijakan. Namun, di bawah permukaan kontribusi positif ini, tantangan kapasitas sumber daya manusia, koordinasi antar unit kerja, dan ketidakpastian ancaman menuntut agar manajemen risiko diperlakukan sebagai proses berkelanjutan dan adaptif.

Terakhir, analisis memperlihatkan potensi sinergi antara manajemen risiko BSSN dengan inisiatif nasional lainnya, seperti regulasi SPBE), strategi pertahanan siber nasional, dan pengembangan SDM siber. Peneliti menyimpulkan bahwa manajemen risiko yang efektif di BSSN bisa berfungsi sebagai katalisator untuk integrasi kebijakan keamanan siber organisasi yang berdampak pada penguatan kebijakan siber nasional, memperkuat kolaborasi antar unit kerja dengan beragam tugas dan fungsi, serta membangun ketahanan ekosistem siber.

Dengan demikian, pembahasan ini menggarisbawahi bahwa manajemen risiko tidak hanya merupakan alat teknis mitigasi, tetapi juga instrumen strategis dan kelembagaan yang mampu meningkatkan efektivitas keamanan siber BSSN dalam jangka panjang asalkan tantangan kapasitas, koordinasi, dan adaptasi ancaman ditangani secara sistematis dan berkelanjutan.

Kontribusi Dan Kebaruan Penelitian

Penelitian ini menawarkan sejumlah kebaruan dan kontribusi ilmiah yang membedakannya dari studi-studi sebelumnya mengenai manajemen risiko dan keamanan siber, khususnya dalam konteks sektor publik. Pertama, dari sisi **kontribusi teoretis**, penelitian ini memposisikan manajemen risiko tidak semata sebagai instrumen teknis pengendalian ancaman siber, melainkan sebagai instrumen tata kelola strategis (*governance instrument*) dalam organisasi publik. Berbeda dengan sebagian besar literatur yang membahas manajemen risiko siber secara terpisah dari kerangka tata kelola, studi ini menunjukkan bagaimana manajemen risiko di BSSN berfungsi sebagai penghubung antara kebijakan nasional, pengambilan keputusan strategis pimpinan, dan implementasi operasional keamanan siber. Dengan demikian, penelitian ini memperkaya literatur

tata kelola keamanan siber dengan perspektif institusional dan kebijakan pada level otoritas nasional.

Kedua, dari sisi **kontribusi empiris**, penelitian ini merupakan salah satu kajian kualitatif eksploratif yang secara spesifik mengkaji praktik manajemen risiko di lembaga keamanan siber nasional Indonesia. Literatur yang ada cenderung berfokus pada sektor swasta, studi teknis sistem informasi, atau analisis normatif kebijakan. Dengan menggali data dari dokumen internal, wawancara informan kunci, dan observasi terbatas, penelitian ini memberikan gambaran empiris yang kontekstual mengenai bagaimana manajemen risiko dioperasionalkan dalam lingkungan organisasi publik strategis yang memiliki mandat nasional dan lintas sektor.

Ketiga, dari sisi **kontribusi konseptual**, penelitian ini mengusulkan pemahaman integratif mengenai hubungan antara input manajemen risiko (identifikasi, evaluasi, mitigasi, dan pemantauan risiko), proses keamanan siber (identifikasi, deteksi, respons, serta penanggulangan dan pemulihan), serta *outcome* efektivitas keamanan siber (kesiapan organisasi, kecepatan respons, kontinuitas layanan, dan budaya sadar risiko). Kerangka konseptual ini dapat digunakan sebagai lensa analitis bagi penelitian selanjutnya maupun sebagai alat bantu refleksi kebijakan bagi pembuat keputusan di sektor publik.

Keempat, dari sisi **kontribusi kebijakan dan praktis**, temuan penelitian ini memberikan dasar argumentatif bagi penguatan kebijakan keamanan siber nasional berbasis risiko. Rekomendasi yang dihasilkan seperti pengembangan metrik risiko siber, peningkatan kapasitas SDM analisis risiko, serta penguatan koordinasi lintas unit kerja yang bersifat aplikatif dan relevan bagi BSSN maupun kementerian/lembaga lain yang berada dalam ekosistem keamanan siber nasional. Dengan demikian, penelitian ini tidak hanya berkontribusi pada diskursus akademik, tetapi juga pada perbaikan praktik tata kelola keamanan siber di Indonesia.

SIMPULAN

Penelitian ini menyimpulkan bahwa manajemen risiko merupakan instrumen strategis yang berperan penting dalam meningkatkan efektivitas keamanan siber di BSSN. Manajemen risiko tidak hanya berfungsi sebagai alat mitigasi teknis, tetapi juga sebagai mekanisme tata kelola yang memperkuat pengambilan keputusan, akuntabilitas, dan ketahanan siber nasional. Dalam dimensi strategis, manajemen risiko organisasi turut diinternalisasi sebagai landasan tata kelola siber nasional. Hal ini mendukung BSSN dalam menetapkan prioritas pembinaan dan kebijakan berdasarkan profil ancaman dan dampak risiko yang sistematis terkait sektor yang dibina. Penelitian ini menujukkan bahwa manajemen risiko di BSSN bukan sekadar kebijakan formal, tetapi menjadi bagian integral dari pengambilan keputusan strategis di level pimpinan.

Pada dimensi operasional dan kelembagaan, pendekatan berbasis risiko memperkuat alokasi sumber daya mitigasi secara lebih efisien dan tepat sasaran, dengan memperlakukan skenario ancaman berdampak tinggi sebagai prioritas mitigasi utama. Prosedur respons insiden yang disusun berdasarkan penilaian

risiko juga menghasilkan peningkatan kecepatan tanggapan insiden (*time to respond*) dan pemulihan yang lebih sistematis, karena SOP dan jalur eskalasi telah dipetakan melalui analisis risiko yang matang. Lebih jauh, manajemen risiko di BSSN berkontribusi menciptakan budaya organisasi yang sadar risiko (*risk aware culture*), melalui pelatihan rutin, simulasi insiden, dan diskusi risiko di berbagai jenjang. Budaya ini memastikan bahwa risiko siber tidak hanya dipahami pada level teknis, tetapi juga diintegrasikan dalam pemikiran strategis dan manajerial. Pada penelitian ini juga diidentifikasi tantangan signifikan yaitu keterbatasan kapasitas sumber daya manusia dalam analisis risiko dan dinamika ancaman yang cepat berubah. Proses evaluasi skenario risiko juga masih terkendala birokrasi dan keterbatasan sumber daya, mengingat ancaman siber berkembang sangat cepat.

DAFTAR RUJUKAN

Asiyanti, A. P. D., & Agussalim, A. (2024). Strategi manajemen risiko dan keamanan siber dalam ekonomi digital: Tinjauan literatur. Jurnal Penelitian Sistem Informasi (JPSI), 2(4).

Badan Siber dan Sandi Negara. (2024). Lanskap Keamanan Siber Indonesia Tahun 2024. Badan Siber dan Sandi Negara.

Bisma, R. (2022). Manajemen Risiko Aset Teknologi Informasi: Studi kasus Implementasi Manajemen Risiko SPBE Dinas Komunikasi dan Informatika Pemerintah Kota Balikpapan. JIEET (Journal Information Engineering and Educational Technology), 06, 73 - 78.doi:https://doi.org/10.26740/jieet.v6n2.p73-7

Fakultas Hukum Universitas Indonesia, & BSSN. (2022). FGD: Manajemen keamanan siber industri dalam menyikapi risiko siber bersama BSSN dan Microsoft. Portal UI.

Febriyanti, L., Febrinazahra, M., & Masdiyasa, I. G. S. (2024). Manajemen risiko sistem informasi unit organisasi BPIW Kementerian PUPR menggunakan framework ISO 31000:2018. Jurnal Sistem Informasi dan Aplikasi.

ISO. (2018). ISO 31000: Risk management — Guidelines. International Organization for Standardization.

Jauhari, R., Sukmadilaga, C., & Mulyani, S. (2021). Implementasi dan critical success factor manajemen risiko di instansi pemerintah. Jurnal Paradigma Ekonomika, 16(2), 285–298.

Jefferson Benyamin, Mualim, M., & Duarte, E. P. (2023). Manajemen risiko keamanan informasi dalam meminimalisasi ancaman siber pada pusat data dan teknologi informasi komunikasi Badan Siber dan Sandi Negara. Universitas Pertahanan Republik Indonesia.

Kurniati, A., Nugroho, L. E., & Rizal, M. N. (2020). Manajemen Risiko Teknologi Informasi pada e-Government: Ulasan Literatur Sistematis. Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi), 22, 219. doi:https://doi.org/10.33164 /iptekkom.22.2.2020.207-222

Modi, A., Kuzminykh, I., & Ghita, B. (2023). Data-driven approaches to cybersecurity governance for board decision-making: A systematic review. arXiv.

Kementerian Pendayagunaan Aparatur Negara dan Reformasi (2020). Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (SPBE). Kementerian Pendayagunaan Aparatur Negara dan Reformasi

Sutomo, A., Thamrin, S., Widodo, P., & Reksoprodjo, Y. (2025). Membangun ketahanan digital: Pengembangan model strategi pertahanan siber berbasis manajemen risiko. TEMALI: Jurnal Pembangunan Sosial, 8(1), 29–40.

Tommy, S., & Nasution, M. I. P. (2025). Evaluasi manajemen risiko keamanan siber pada infrastruktur digital pemerintah: Studi kasus Pusat Data Nasional (PDN). Jurnal Ilmiah Ekonomi dan Manajemen, 3(6), 330–346.

