VISI SAKTI: Jurnal Industri Kreatif dan Inovatif
Desain Komunikasi Visual ITBK Bukit Pengharapan
ISSN: 3026-149X

Vol. 3, No. 2 (2025): Oktober

KERANGKA TATA KELOLA RISIKO SIBER UNTUK PERUSAHAAN NON-TEKNIS

Yohan Purnawan[1], Hendri Mayanta[2], Benny Sofian Pandinata Purba[3]
Universitas Efarina, Indonesia[1,2,3]
Email: yohanpurnawan@gmail.com tariganhendri606@gmail.com

Abstrak
Seiring meningkatnya digitalisasi dan ketergantungan pada sistem informasi, ancaman siber berkembang menjadi risiko strategis yang signifikan, terutama bagi perusahaan non-teknis yang sering tidak memiliki sumber daya atau keahlian TI yang memadai. Penelitian ini bertujuan menyusun kerangka tata kelola risiko siber yang relevan untuk perusahaan non-teknis dengan mengacu pada prinsip-prinsip dari AICD & CSCRC serta pendekatan defensive social engineering dari MIT Sloan. Kerangka ini mencakup identifikasi pemangku kepentingan, prosedur manajemen risiko, serta mekanisme pelaporan dan evaluasi yang terintegrasi. Landasan teori menegaskan pentingnya memandang risiko siber sebagai risiko strategis, sehingga penguatan budaya keamanan melalui edukasi dan pelatihan karyawan menjadi pendekatan utama non-teknis. Penunjukan Chief Information Security Officer (CISO) juga disorot sebagai jembatan untuk mengurangi kesenjangan antara kebutuhan teknis dan konteks manajerial. Metodologi penelitian menggunakan pendekatan kualitatif melalui studi literatur, dengan analisis yang memetakan temuan pada lima komponen utama: kepemimpinan dan akuntabilitas, edukasi dan pelatihan, manajemen risiko, kebijakan dan prosedur, serta kolaborasi dan pelaporan. Hasil analisis menunjukkan bahwa diperlukan pendekatan sistematis untuk menginternalisasi budaya keamanan di seluruh organisasi. Kesimpulannya, perusahaan non-teknis perlu mengadopsi langkah strategis dalam tata kelola risiko siber untuk meminimalkan potensi kerugian finansial dan reputasi.
Kata kunci: Tata Kelola Risiko Siber, Perusahaan Non-Teknis, Manajemen Risiko, Edukasi, Pelatihan Keamanan Siber

Abstract
As digitalization increases and reliance on information systems grows, cyber threats have evolved into significant strategic risks—especially for non-technical organizations that often lack adequate IT resources or in-depth expertise. This study aims to develop a cyber risk governance framework relevant to non-technical companies by drawing on principles from AICD & CSCRC and the defensive social engineering approach proposed by MIT Sloan. The proposed framework includes stakeholder identification, risk management procedures, and integrated reporting and evaluation mechanisms. The theoretical foundation highlights the importance of treating cyber risk as a strategic risk. Therefore, strengthening a security culture through employee education and training is emphasized as a vital non-technical approach. Appointing a Chief Information Security Officer (CISO) is also discussed as a way to bridge the gap between technical needs and managerial governance, covering policy, training, and readiness evaluation. The research employs a qualitative methodology using literature study, with qualitative analysis mapped to five main components: leadership and accountability, education and training, risk management, policies and procedures, and collaboration and reporting. The findings indicate that a systematic approach is necessary to internalize a security culture across the organization. In conclusion, non-technical organizations should adopt strategic steps in cyber risk governance to minimize potential financial and reputational losses.
Keywords: Cyber Risk Governance, Non-Technical Companies, Risk Management, Education, Cybersecurity Training

PENDAHULUAN

Seiring meningkatnya digitalisasi dan semakin besarnya ketergantungan perusahaan terhadap sistem informasi, ancaman siber kini tidak lagi dipandang sebagai persoalan teknis semata. Dalam banyak organisasi, aktivitas bisnis yang sebelumnya bersifat manual mulai berpindah ke platform digital, sehingga permukaan serangan (attack surface) ikut meluas. Kondisi ini membuat risiko siber berkembang

menjadi salah satu risiko strategis yang dapat memengaruhi kelangsungan operasional perusahaan, termasuk dari sisi keamanan data, layanan, hingga kepercayaan pihak terkait.

Bagi perusahaan non-teknis, tantangan mengelola risiko siber cenderung lebih kompleks dibanding perusahaan yang memiliki kapabilitas teknologi internal yang kuat. Umumnya perusahaan jenis ini tidak memiliki sumber daya, kompetensi, maupun keahlian teknis yang mendalam di bidang siber, sehingga pengendalian keamanan sering tidak berjalan secara sistematis. Akibatnya, keputusan terkait keamanan informasi sering terlambat, bersifat reaktif, atau hanya menekankan aspek teknologi tertentu tanpa menata faktor tata kelola, proses, dan tanggung jawab di tingkat organisasi.

Selain keterbatasan sumber daya, masalah lain yang sering muncul adalah belum terintegrasinya tata kelola risiko siber ke dalam strategi bisnis perusahaan. Ketika risiko siber diperlakukan sebagai urusan semata-mata "bagian IT", maka dewan direksi dan manajemen puncak tidak memiliki kerangka yang jelas untuk mengawasi, mengevaluasi, serta memastikan akuntabilitas pengelolaan risiko. Padahal, literatur terkait pengawasan dewan menegaskan bahwa risiko siber harus dipandang sebagai risiko strategis yang memerlukan keterlibatan pengambil keputusan tingkat atas agar perusahaan mampu meminimalkan dampak insiden, baik dari segi finansial maupun reputasi.

Pentingnya tata kelola juga terkait dengan kenyataan bahwa insiden siber tidak hanya dipicu oleh kelemahan teknis, melainkan juga oleh faktor manusia dan proses organisasi. Dalam konteks ini, pendekatan non-teknis seperti defensive social engineering menekankan bahwa perusahaan dapat menurunkan risiko melalui edukasi dan peningkatan kesadaran karyawan, misalnya melalui pelatihan mengenali phishing, pengendalian kata sandi, dan penguatan perilaku aman dalam aktivitas sehari-hari. Dengan demikian, budaya keamanan menjadi elemen kunci yang menentukan seberapa siap organisasi mencegah sekaligus merespons insiden.

Permasalahan selanjutnya adalah lemahnya dokumentasi kebijakan dan prosedur keamanan siber yang mudah dipahami serta dapat dijalankan oleh seluruh lini organisasi. Pada banyak perusahaan non-teknis, ketiadaan pedoman yang jelas menyebabkan kontrol keamanan tidak konsisten, mekanisme pelaporan insiden tidak berjalan efektif, dan proses evaluasi berkala tidak dilakukan secara disiplin. Kekosongan ini dapat menjadi celah bagi pihak yang tidak bertanggung jawab sekaligus menghambat respons internal ketika insiden terjadi, karena perusahaan kesulitan menentukan langkah apa yang harus diambil dan siapa yang bertanggung jawab.

Kebutuhan akan kerangka tata kelola semakin mendesak karena dinamika ancaman siber terus berubah dan berkembang, sementara kemampuan adaptasi organisasi non-teknis sering kali terbatas. Tanpa pendekatan manajemen risiko yang terstruktur, perusahaan cenderung mengalokasikan sumber daya secara tidak proporsional, sehingga prioritas kontrol keamanan tidak sesuai dengan tingkat ancaman terhadap aset kritis. Oleh sebab itu, diperlukan proses identifikasi aset, penilaian risiko secara kualitatif, hingga pengembangan mitigasi dan rencana kontinjensi yang dapat diterapkan dalam konteks perusahaan non-teknis.

Dari sisi penguatan organisasi, keterlibatan dewan direksi menjadi faktor penentu untuk memastikan program keamanan siber memiliki arah, dukungan, dan akuntabilitas yang jelas. Salah satu upaya yang menonjol adalah penunjukan Chief Information Security Officer (CISO) atau penanggung jawab siber di tingkat yang mampu menjembatani kesenjangan antara aspek teknis dan kebutuhan manajerial. Melalui peran tersebut, pelaksanaan kebijakan keamanan, pelatihan dan evaluasi kesiapan, serta pengawasan berkelanjutan dapat dilakukan secara lebih terkoordinasi, sehingga pengelolaan risiko siber tidak berhenti di level kebijakan formal, tetapi benar-benar menjadi praktik organisasi.

Berdasarkan kebutuhan tersebut, penelitian ini berangkat dari urgensi untuk menyusun kerangka tata kelola risiko siber yang relevan bagi perusahaan non-teknis, dengan menekankan komponen yang dapat dipahami dan diimplementasikan meskipun kapabilitas teknis terbatas. Kerangka tersebut perlu memuat arah strategis berbasis prinsip tata kelola siber (termasuk akuntabilitas dewan), mekanisme manajemen risiko yang sederhana namun terukur, kebijakan dan prosedur yang jelas, serta sistem pelaporan dan kolaborasi internal-eksternal. Dengan adanya kerangka yang komprehensif, perusahaan diharapkan mampu membangun budaya keamanan siber secara menyeluruh, mengurangi potensi kerugian, sekaligus meningkatkan kesiapan menghadapi ancaman yang semakin kompleks.

LANDASAN TEORI

Sejumlah literatur telah menyoroti pentingnya tata kelola siber sebagai bagian dari strategi manajemen risiko. Contohnya, dokumen "Board Oversight of Cyber Risks and Cybersecurity" menekankan bahwa risiko siber harus dipandang sebagai risiko strategis dan tidak hanya masalah operasional IT. Beberapa penelitian menunjukkan bahwa perusahaan yang mengintegrasikan pengelolaan risiko siber ke dalam strategi bisnis utamanya cenderung lebih mampu menghadapi insiden siber dan meminimalisir kerugian – baik secara finansial maupun reputasi.

Lebih lanjut, pendekatan "defensive social engineering" yang ditawarkan oleh MIT Sloan memberikan gambaran tentang bagaimana perusahaan non-teknis dapat meminimalkan risiko siber melalui edukasi dan pelatihan karyawan. Lawrence Susskind menekankan bahwa upaya non-teknis seperti pengendalian kata sandi, pelatihan mengenali email mencurigakan, dan penunjukan seorang Chief Information Security Officer (CISO) merupakan Langkah efektif untuk mencegah terjadinya serangan siber melalui manipulasi sosial.

Selain itu, prinsip-prinsip tata kelola siber yang dikembangkan oleh AICD dan CSCRC memberikan panduan praktis mengenai peran dewan dalam menetapkan kerangka tata kelola yang efektif. Prinsip-prinsip tersebut mencakup penetapan akuntabilitas, penguatan budaya keamanan, dan pemanfaatan alat ukur kinerja untuk menilai efektivitas program pengelolaan risiko siber. Studi-studi lain juga menyatakan bahwa perusahaan non-teknis seringkali kekurangan dokumentasi kebijakan dan prosedur yang jelas terkait dengan pengelolaan risiko siber, sehingga menjadi titik lemah yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Dengan demikian, kerangka tata kelola yang sistematis dan mudah dipahami sangat diperlukan agar seluruh lini organisasi, mulai dari dewan direksi hingga karyawan, memiliki pemahaman yang sama mengenai tanggung jawab dalam rangka mengelola risiko siber.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan studi literatur sebagai metode utama. Data dikumpulkan dari berbagai sumber primer dan sekunder yang relevan, termasuk:

1. Laporan tata kelola siber dewan direksi:

Sumber-sumber seperti dokumen "Board Oversight of Cyber Risks and Cybersecurity" menyajikan data dan analisis mengenai peran dewan dalam pengelolaan risiko siber.

2. Pendekatan non-teknis dalam pengelolaan risiko siber:

Artikel "8 non-technical ways to improve your company's cybersecurity" memberikan gambaran langkah praktis yang dapat diterapkan oleh perusahaan non-teknis untuk meningkatkan keamanan siber tanpa bergantung sepenuhnya pada teknologi canggih.

3. Prinsip tata kelola siber dari AICD dan CSCRC:

Prinsip-prinsip tata kelola siber yang dikeluarkan oleh AICD dan CSCRC menjadi rujukan untuk menyusun elemen-elemen kerangka tata kelola yang komprehensif bagi
perusahaan non-teknis .

4. Format Laporan Penelitian (IMRAD):

Struktur laporan penelitian mengikuti format IMRAD, yang mencakup bagian Abstrak, Pendahuluan, Tinjauan Pustaka, Metodologi, Analisis, dan Kesimpulan. Data yang diperoleh dianalisis secara kualitatif dengan memetakan elemen-elemen penting yang mendasari tata kelola risiko siber. Proses analisis dilakukan melalui pengelompokan temuan-temuan ke dalam lima komponen utama: kepemimpinan dan akuntabilitas, edukasi dan pelatihan, manajemen risiko, kebijakan dan prosedur, serta kolaborasi dan pelaporan. Hasil analisis kemudian disajikan dalam bentuk diagram alur dan tabel ringkasan untuk memudahkan pemahaman dan implementasi kerangka kerja yang disarankan.

HASIL DAN PEMBAHASAN

1. Kepemimpinan dan Akuntabilitas

Dalam kerangka tata kelola risiko siber, kepemimpinan yang kuat dan akuntabilitas yang jelas merupakan fondasi utama. Dewan direksi memiliki tanggung jawab besar untuk memastikan bahwa strategi pengelolaan risiko siber telah terintegrasi ke dalam seluruh lini organisasi.

Penunjukan seorang Chief Information Security Officer (CISO) atau penanggung jawab siber di tingkat dewan adalah langkah esensial. Walaupun perusahaan non-teknis sering menghadapi keterbatasan dalam sumber daya teknis, penunjukan CISO dapat membantu menjembatani kesenjangan antara aspek teknis dan non-teknis. Tugas CISO mencakup:

a. Mengawasi pelaksanaan kebijakan keamanan siber
b. Menjamin pelatihan dan edukasi karyawan terkait risiko siber
c. Melakukan evaluasi rutin atas kesiapan keamanan siber perusahaan

Hal ini mendapat dukungan dari literatur yang menekankan bahwa keterlibatan dewan direksi secara langsung dalam pengawasan risiko siber dapat meningkatkan efektivitas pengelolaan risiko secara keseluruhan.

2. Edukasi dan Pelatihan

Edukasi dan pelatihan merupakan aspek yang tidak kalah penting, terutama bagi perusahaan non-teknis yang kerap mengalami keterbatasan keahlian di bidang siber. Pendekatan "defensive social engineering" menekankan bahwa pendidikannya tidak selalu bergantung pada teknologi canggih, melainkan pada peningkatan kesadaran dan pengetahuan karyawan.

Beberapa langkah strategis yang direkomendasikan meliputi:

a. Pelatihan rutin mengenai cara mengenali email phishing dan serangan siber lainnya: Karyawan perlu dilatih untuk memahami tanda-tanda serangan dan berperilaku waspada terhadap lampiran atau tautan yang mencurigakan.

b. Workshop dan seminar mengenai kebijakan dan prosedur keamanan: Mengadakan workshop secara berkala dapat menanamkan budaya keamanan dalam organisasi.

Simulasi insiden siber:

Melakukan latihan simulasi serangan siber untuk memastikan setiap individu memahami peran dan tanggung jawabnya. Strategi edukasi ini tidak hanya membantu mencegah serangan yang berasal dari kesalahan manusia, tetapi juga meningkatkan respons dan kesiapsiagaan jika terjadi insiden siber.

3. Manajemen Risiko

Manajemen risiko siber merupakan proses identifikasi, penilaian, dan penanggulangan risiko yang dapat menggangu operasional perusahaan. Bagi perusahaan non-teknis, proses ini harus disederhanakan agar mudah dipahami dan diimplementasikan.
Komponen utama manajemen risiko siber meliputi:
a. Identifikasi Aset Kritis:
Perusahaan harus menentukan aset penting yang perlu diidentifikasi dan dilindungi, seperti data pelanggan, informasi keuangan, dan rahasia perusahaan.
b. Penilaian Risiko:
Menggunakan metode kualitatif untuk menilai kemungkinan dan dampak serangan siber terhadap aset kritis.
c. Pengembangan Rencana Mitigasi:
Strategi untuk mengurangi risiko berupa penerapan langkah-langkah preventif serta rencana kontinjensi untuk mengatasi insiden yang terjadi.
Proses manajemen risiko yang terstruktur sangat penting untuk membantu perusahaan non-teknis mengalokasikan sumber daya secara proportional terhadap ancaman yang dihadapi, serta menentukan apakah risiko tersebut harus diterima, dikurangi, atau dialihkan melalui asuransi.

4. Kebijakan dan Prosedur

Kebijakan dan prosedur yang terdokumentasi dengan jelas merupakan tulang punggung dari kerangka tata kelola risiko siber. Untuk perusahaan non-teknis, dokumen-dokumen ini harus disusun dengan menggunakan bahasa yang mudah dipahami dan tidak terlalu teknis.

Unsur-essential dalam penyusunan kebijakan meliputi:

a. Dokumentasi Kebijakan Keamanan Siber:

Panduan tertulis mengenai standar operasional, kontrol akses, serta prosedur tanggap insiden.

b. Prosedur Pelaporan:

Mekanisme pelaporan yang memungkinkan karyawan untuk menginformasikan aktivitas mencurigakan atau celah keamanan secara cepat.

c. Audit Internal dan Evaluasi Berkala:

Rencana untuk melakukan audit internal guna memastikan kebijakan yang telah ditetapkan dijalankan dengan efektif serta melakukan evaluasi berkala untuk menangkap perubahan lingkungan risiko. Kebijakan dan prosedur yang solid dapat meningkatkan transparansi dan memudahkan perusahaan dalam beradaptasi dengan perubahan regulasi serta dinamika ancaman siber yang terus berkembang.

5. Kolaborasi dan Pelaporan

Kolaborasi antara berbagai unit dalam perusahaan, serta dengan pihak eksternal seperti penyedia layanan keamanan dan regulator, sangat penting untuk membangun sistem tata kelola yang komprehensif.

Aspek yang perlu diperhatikan antara lain:

a. Kerjasama Tim Internal:

Mengintegrasikan fungsi keamanan siber ke dalam operasi sehari-hari, di mana setiap bagian organisasi berkontribusi untuk meminimalkan risiko.

b. Pelaporan dan Komunikasi yang Efisien:

Sistem pelaporan yang jelas, transparan, dan terstruktur sangat diperlukan agar informasi seputar risiko dan insiden siber dapat segera direspons oleh dewan direksi.

c. Kemitraan dengan Pihak Eksternal:

Berkolaborasi dengan konsultan keamanan, auditor eksternal, serta otoritas regulasi dapat membantu perusahaan dalam mendapatkan pandangan objektif mengenai efektivitas kebijakan keamanan yang berjalan. Kolaborasi ini tidak hanya memperkuat respons internal, tetapi juga memberikan validitas eksternal terhadap upaya pengelolaan risiko siber perusahaan.

6. Visualisasi Proses Tata Kelola Risiko Siber

Tabel Ringkasan Elemen Utama dalam Kerangka Tata Kelola Risiko Siber

Komponen Utama	Deskripsi	Tindakan Kunci
Kepemimpinan dan Akuntabilitas	Penunjukan CISO dan pelibatan aktif dewan direksi dalam pengawasan risiko siber.	Menetapkan struktur pengambilan keputusan, penunjukan CISO.
Edukasi dan Pelatihan	Pengembangan budaya keamanan melalui pelatihan karyawan dan simulasi insiden siber.	Melaksanakan workshop, simulasi insiden, dan program pelatihan rutin.
Manajemen Risiko	Identifikasi dan penilaian aset kritis serta pengembangan rencana mitigasi.	Inventarisasi aset, evaluasi risiko, dan rencana mitigasi serta kontinjensi.
Kebijakan dan Prosedur	Penyusunan dokumen kebijakan dan prosedur yang mudah dipahami.	Menyusun panduan keamanan, prosedur pelaporan, dan audit berkala.

Kolaborasi dan Pelaporan	Integrasi komunikasi internal dan eksternal untuk pelaporan insiden dan evaluasi kinerja.	Pengembangan sistem pelaporan, kerjasama dengan auditor eksternal dan regulator.

Penjelasan Tabel:

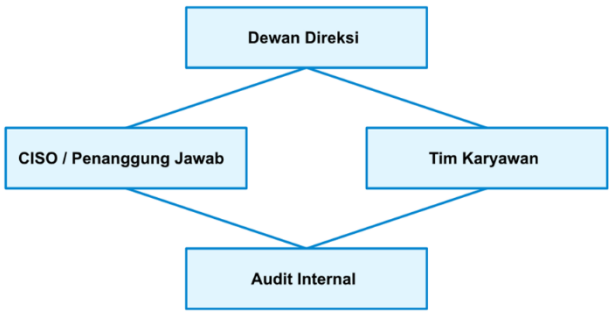
Tabel di atas merangkum komponen utama dalam kerangka tata kelola risiko siber untuk perusahaan non-teknis. Setiap komponen dilengkapi dengan tindakan kunci yang harus diimplementasikan untuk mencapai pengelolaan risiko yang terintegrasi dan efektif.

Diagram Alur Implementasi Tata Kelola Risiko Siber

Deskripsi Diagram:

Diagram alur di atas menggambarkan proses implementasi tata kelola risiko siber secara menyeluruh. Proses dimulai dengan analisis lingkungan siber, diikuti oleh identifikasi aset kritis, penilaian risiko, pengembangan strategi mitigasi, penyusunan kebijakan, pelatihan karyawan, implementasi, serta diakhiri dengan pelaporan dan evaluasi berkala. Diagram ini bertujuan untuk memberikan gambaran visual yang mudah dipahami oleh perusahaan non-teknis.

SVG Diagram: Struktur Organisasi Tata Kelola Risiko Siber



Deskripsi SVG Diagram:

Diagram SVG tersebut mengilustrasikan struktur organisasi tata kelola risiko siber dalam perusahaan non-teknis. Diagram menampilkan dewan direksi di puncak, yang terhubung secara langsung dengan CISO dan tim karyawan di tingkat operasional. Selanjutnya, sistem pengawasan melalui audit internal mendukung proses pengendalian dan evaluasi secara menyeluruh.

KESIMPULAN

Berdasarkan hasil analisis, dapat disimpulkan bahwa perusahaan non-teknis memerlukan kerangka tata kelola risiko siber yang bersifat terstruktur, terintegrasi, dan selaras dengan kebutuhan organisasi yang tidak didukung sumber daya IT secara penuh. Risiko siber harus diposisikan sebagai risiko strategis yang melibatkan kepemimpinan tingkat atas, bukan semata urusan teknis. Oleh karena itu, kerangka yang disusun perlu mencakup aspek kepemimpinan, manajemen risiko, serta mekanisme pelaporan yang jelas agar pengelolaan risiko dapat berjalan konsisten, terukur, dan dapat dipertanggungjawabkan.

Selain itu, internalisasi budaya keamanan menjadi kunci agar pengendalian risiko siber tidak berhenti pada dokumen kebijakan, melainkan benar-benar dipraktikkan dalam aktivitas harian seluruh pemangku kepentingan. Edukasi dan peningkatan kesadaran karyawan melalui pelatihan yang relevan, termasuk pendekatan non-teknis seperti defensive social engineering, perlu dibarengi dengan penataan peran dan tanggung jawab, misalnya melalui pengangkatan CISO untuk menjembatani kesenjangan teknis dan kebutuhan tata kelola. Dengan penerapan langkah strategis tersebut, perusahaan diharapkan mampu menurunkan potensi dampak insiden terhadap kerugian finansial dan reputasi, sekaligus meningkatkan kesiapan menghadapi ancaman siber yang terus berkembang.

REFERENSI

Ahlan, A. R., & Lubis, M. (2022). Information Security Governance in Non-IT Organizations: Challenges and Opportunities. Journal of Information Systems and Technology Management, 7(25), 45-60.

AICD & CSCRC. (2022). Cyber Security Governance Principles. Sydney: Australian Institute of Company Directors & Cyber Security Cooperative Research Centre.

American Institute of Certified Public Accountants (AICPA). (2024). Board Oversight of Cyber Risks and Cybersecurity: A Practical Guide for Directors. New York: AICPA.

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Indianapolis: Wiley.

Brotby, W. (2019). Information Security Governance: A Practical Development and Implementation Approach. Hoboken: John Wiley & Sons.

Chatterjee, S., & Kar, A. K. (2023). Assessing Cyber Risk Readiness in Manufacturing SMEs: A Managerial Perspective. International Journal of Information Management, 68, 102-115.

He, W., Zhang, Z., & Li, W. (2021). The Role of Board of Directors in Cyber Risk Oversight. Journal of Cybersecurity and Privacy, 1(3), 412-428.

Humphreys, E. (2021). Implementing the ISO/IEC 27001:2013 ISMS Standard. Norwood: Artech House.

ISO/IEC 27001. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization.

Janicke, H., & Jones, K. (2024). Cyber Governance for Non-Technical Managers: Bridging the Gap. Computers & Security, 136, 103-118.

Jurnal & Artikel Ilmiah

Karanja, E. (2022). The Role of the Chief Information Security Officer in Non-Technical Firms. Journal of Management Information Systems, 39(1), 210-235.

Maheshwari, S. (2023). Human Factors in Cybersecurity: Defensive Social Engineering Training for Employees. IEEE Transactions on Engineering Management, 70(4), 1450-1462.

National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg: U.S. Department of Commerce.

Nuseir, M. T. (2021). Digital Transformation and Cybersecurity Governance: A Study on Non-Technical Firms in Emerging Markets. Sustainability, 13(21), 118-132.

Posthumus, S., & von Solms, R. (2018). A Framework for the Governance of Information Security. Computers & Security, 23(3), 191-201.

Purnawan, Y., Mayanta, H., & Purba, B. S. P. (2025). Kerangka Tata Kelola Risiko Siber untuk Perusahaan Non-Teknis. Pematangsiantar: Universitas Efarina.

Radziwill, N. M., & Benton, M. C. (2020). Cybersecurity Management for Quality Professionals. Software Quality Professional, 22(4), 4-15.
Setiawan, A., & Ramli, K. (2023). Analisis Tata Kelola Keamanan Informasi pada Sektor Non-TI Menggunakan Indeks KAMI. Jurnal Sistem Informasi, 19(1), 12-28.
Susskind, L., & Field, P. (2023). Defensive Social Engineering: Non-Technical Cybersecurity Strategies for Modern Leadership. Cambridge: MIT Sloan Management Review.
Tounsi, W. (2024). Cybersecurity for Business Leaders: A Non-Technical Guide. New York: Springer.
von Solms, B., & von Solms, R. (2018). Cybersecurity and Information Security: What Every Board Member Needs to Know. Computers & Security, 78, 10-17.
Widyanto, R. A., & Widjajarto, A. (2022). Designing Cyber Risk Management for Non-IT SMEs: A Qualitative Approach. Procedia Computer Science, 197, 560-568.
Buku & Laporan Institusi (Standard Internasional).