ANALISIS BALANCED SCORECARD UNTUK MENDUKUNG PENGENDALIAN CYBER FRAUD DI BANK CIMB NIAGA TAHUN 2022-2024

Umi Solehah[1]; Siti Rodiah[2]; Zul Azmi[3]

Fakultas Ekonomi dan Bisnis, Universitas Muhammadiyah Riau
Jln. Delima, Kec. Tampan, Kota Pekanbaru, Riau 28292
E-mail : 220301043@student.umri.ac.id (Koresponding)

Abstract: This study aims to examine the importance of cyberfraud control as the use of digital services in the banking sector increases, potentially creating cybercrime risks. The focus of this study is the implementation of cyberfraud control at Bank CIMB Niaga using the Balanced Scorecard (BSC) approach, which encompasses financial, customer, internal business process, and learning and growth perspectives. The research method used is qualitative, utilizing secondary data sourced from annual reports and sustainability reports for the 2022–2024 period. The results show that cyberfraud control at Bank CIMB Niaga has gradually strengthened through increased investment in technological security, improvements to internal business processes, and increased organizational readiness for digital transformation. These findings demonstrate that effective cyberfraud control requires technological support, a robust risk management system, and an organizational commitment to maintaining sustainable information security

Keywords: *Balanced Scorecard, Cyber Fraud, Internal Control*

Perkembangan teknologi informasi telah mendorong percepatan transformasi digital di sektor perbankan melalui pemanfaatan layanan berbasis teknologi seperti internet banking dan mobile banking. Digitalisasi tersebut memberikan kemudahan bagi nasabah dalam melakukan transaksi secara cepat dan efisien. Namun, di balik manfaat tersebut, perbankan juga menghadapi peningkatan risiko kejahatan siber (*cyber fraud*) yang dapat mengancam keamanan sistem serta kerahasiaan data nasabah Otoritas Jasa Keuangan (2025). Oleh karena itu, pengendalian *cyber fraud* menjadi aspek penting bagi industri perbankan dalam menjaga stabilitas operasional dan kepercayaan publik. Ancaman *cyber fraud* menunjukkan tren peningkatan secara global maupun nasional. Cyberscurity Ventures (2021) memperkirakan kerugian akibat *cyber crime* secara global mencapai USD 9,5 triliun pada tahun 2024 dan diprediksi meningkat menjadi USD 10,5 triliun pada akhir tahun 2025. Di Indonesia, berbagai modus kejahatan digital seperti *phishing, skimming, malware, hingga social engineering* masih mendominasi serangan terhadap sektor perbankan Otoritas Jasa Keuangan (2025). Berdasarkan data data Badan Siber dan Sandi Negara (2024) mencatat sebanyak 122,79 juta anomali atau serangan siber selama periode Januari-Agustus 2024, yang menunjukkan bahwa sektor perbankan menjadi salah satu target utama kejahatan digital.

Menyikapi kondisi tersebut, Otoritas Jasa Keuangan Otoritas Jasa Keuangan (2025) menekankan pentingnya penerapan strategi anti-fraud berbasis teknologi digital serta penguatan sistem pengendalian internal di lembaga perbankan nasional. Sejalan dengan hal tersebut, sejumlah bank nasional mulai melakukan berbagai upaya penguatan sistem pengendalian untuk memitigasi risiko *cyber fraud.* Salah satu bank yang menunjukkan komitmen dalam menghadapi ancaman tersebut adalah Bank CIMB Niaga melalui berbagai kebijakan dan strategi pengendalian selama periode 2022-2024.

Tabel Data Ancaman *Cyber fraud* Nasional Dan Strategi Pengendalian Bank CIMB Niaga 2022-2024

Tahun	Fenomena *cyber fraud*	Stratgei Pengendalian Bank Bank CIMB Niaga
2022	BSSN mencatat 11,8 juta anomali tarif dari sektor keuangan	Fokus pada penguatan keamanan Siber, peningkatan Sistem Insiden Manajemen, serta mitigasi risiko
2023	Serangan meningkat kerugian gelobal akibat *cyber crime* mencapai USD 8 triliun dan sebagian besar ancaman ini berbentuk *cyber fraud*	Implementasi *zero Tolerance to fraud*, sistem *Whistleblowing System*, dan evaluasi *Anti-fraud Managemen* secara berkala
2024	Diprediksi meningkat menjadi USD 9,5 triliun serta serangan *pishing* dan kebocoran data makin masif (BSSN)	Penerapan *Cyber Defanse*, pengujian serangan dengan *Breach Attack Simulation Tool*, dan *Information Scurity Mnagemen System*

Sumber: Diolah dari BSSN, OJK, dan Laporan Tahunan CIMB Niaga 2022-2024

Berdasarkan Tabel data ancaman tersebut, dapat dilihat bahwa ancaman *cyber fraud* secara nasional menunjukkan kecenderungan meningkat dari tahun ke tahun. Pada saat yang sama, Bank CIMB Niaga secara konsisten melakukan berbagai upaya penguatan sistem pengendalian sebagai respons terhadap meningkatnya risiko kejahatan digital. Kondisi tersebut menunjukkan bahwa pengendalian *cyber fraud* menjadi isu strategis yang memerlukan perhatian serius, tidak hanya dari sisi teknis keamanan, tetapi juga dari aspek manajerial dan pengelolaan kinerja organisasi. Dalam konteks tersebut, diperlukan suatu pendekatan yang mampu mengevaluasi efektivitas pengendalian *cyber fraud* secara menyeluruh. *Balanced Scorecard* (BSC) dinilai relevan karena mampu mengukur kinerja organisasi dari empat perspektif, yaitu keuangan, pelanggan, proses bisnis internal, serta pembelajaran dan pertumbuhan Kaplan and Norton (1996). Penerapan BSC terbukti mampu memberikan gambaran kinerja gambaran kinerja organisasi secara komperhensif karena tidak hanya berfokus pada aspek keuangan, tetapi juga aspek non keuangan. Hal ini situnjukan pada penelitian oleh Azmi et al. (2021) yang menerapkan BSC untuk menilai kinerja organisasi. Penelitian yang dilakukan oleh Rodiah et al. (2019) juga menunjukkan bahwa efektivitas pengendalian internal memiliki peran penting dalam menekan terjadinya berbagai bentuk kecurangan dalam organisasi. Temuan tersebut menunjukkan bahwa pengendalian internal menjadi faktor penting dalam pencegahan risiko fraud, termasuk kejahatan berbasis teknologi informasi (*cyber fraud*) pada sektor perbankan, Sistem pengendalian yang kuat mampu membatasi peluang terjadinya *fraud* melalui peningkatan pengawasan, kepatuhan terhadap prosedur, serta penguatan etika organisasi. Pendekatan ini memungkinkan evaluasi pengendalian risiko tidak hanya berfokus pada aspek finansial, tetapi juga mencakup proses internal dan kesiapan organisasi dalam menghadapi dinamika risiko digital. Basel Committee on Banking Supervision (2023) juga menegaskan bahwa risiko kejahatan siber dapat memengaruhi stabilitas dan kepercayaan terhadap sistem perbankan global, sehingga memerlukan pendekatan pengendalian yang terintegrasi.

Penelitian yang dilakukan oleh Akinbowale et al. (2020) menunjukkan bahwa penerapan *Balanced Scorecard* mampu meningkatkan efektivitas pengendalian risiko *cyber fraud* pada sektor

perbankan melalui integrasi indikator keuangan dan nonkeuangan. Hasil penelitian tersebut menegaskan bahwa keseimbangan antara perspektif keuangan, pelanggan, proses bisnis internal, serta pembelajaran dan pertumbuhan berperan penting dalam memperkuat sistem pengendalian internal terhadap risiko kejahatan digital.Temuan serupa juga disampaikan oleh zerihun (2023) yang menyatakan bahwa *Balanced Scorecard* dapat membantu organisasi jasa keuangan dalam meningkatkan efisiensi operasional sekaligus memperkuat manajemen risiko digital. Dalam penelitiannya, penerapan keempat perspektif *Balanced Scorecard* dinilai mampu memberikan kerangka evaluasi kinerja yang lebih komprehensif dalam menghadapi meningkatnya ancaman *cyber fraud*. Selanjutnya, Abdalla et al. (2022) menekankan bahwa penerapan *Balanced Scorecard* secara konsisten mendorong terciptanya keseimbangan antara pencapaian kinerja finansial dan penguatan tata kelola risiko, sehingga sistem deteksi dan pencegahan *cyber fraud* dapat berjalan lebih efektif. Temuan ini menunjukkan bahwa *Balanced Scorecard* tidak hanya berfungsi sebagai alat pengukuran kinerja, tetapi juga sebagai pendekatan strategis dalam pengendalian risiko digital.

Namun demikian, penelitian yang dilakukan oleh Kwaijtaal (2024) menunjukkan hasil yang berbeda. Penelitian tersebut menemukan bahwa penerapan *Balanced Scorecard* belum sepenuhnya optimal dalam menghadapi kompleksitas kejahatan siber, khususnya akibat lemahnya integrasi antara proses bisnis internal dan sistem keamanan digital. Kondisi ini menyebabkan strategi pengendalian *cyber fraud* yang diterapkan belum memberikan dampak yang maksimal. Perbedaan temuan penelitian tersebut menunjukkan adanya kesenjangan kajian, khususnya terkait efektivitas penerapan *Balanced Scorecard* dalam mendukung pengendalian *cyber fraud* pada sektor perbankan di Indonesia. Oleh karena itu, penelitian ini dilakukan untuk menganalisis pengendalian *cyber fraud* di Bank CIMB Niaga menggunakan pendekatan *Balanced Scorecard* periode 2022-2024. Penelitian ini diharapkan mampu memberikan kontribusi akademik dalam memperkaya kajian manajemen risiko perbankan serta menjadi bahan pertimbangan bagi pihak perbankan dan regulator dalam memperkuat sistem pengendalian internal yang adaptif terhadap dinamika risiko kejahatan digital.

Penelitian ini menggunakan pendekatan *Balanced Scorecard* (BSC) sebagai kerangka analisis kinerja pengendalian *cyber fraud* pada Bank CIMB Niaga. Menurut Kaplan and Norton (1992) Balanced Scorecard merupakan sistem pengukuran kinerja tradisional yang berfokus pada indikator keuangan, ukuran keuangan bersifat retrospektif dan tidak memperhitungkan faktor-faktor yang menentukan keberhasilan organisasi jangka panjang, dan terdapat empat perspektif, yaitu keuangan, pelanggan, proses bisnis internal, serta pembelajaran dan pertumbuhan. Pendekatan ini memungkinkan penilaian pengendalian cyber fraud tidak hanya dari sisi keuangan, tetapi juga dari aspek non-keuangan yang mendukung keberlanjutan operasional bank. Oleh Karena itu, diperlukan sistem pengukuran yang dapat menyeimbangkan perspektif internal dan eksternal organisasi, serta perspektif keuangan dan non-keuangan, dan hasil akhir juga penggerak. Tujuan *Balanced Scorecard* adalah untuk menilai kebutuhan dengan menggunakan metrik terkait kinerja yang secara akurat mengukur banyak aspek operasi organisasi (Kaplan and Norton 1996).

Cyber fraud merupakan bentuk kejahatan siber yang semakin meningkat seiring dengan perkembangan digitalisasi perbankan dan berpotensi menimbulkan risiko operasional, reputasi, serta kerugian finansial (Satrya 2024). Oleh karena itu, pengendalian cyber fraud menjadi bagian penting dalam manajemen risiko perbankan. Selain itu, penelitian ini didukung oleh teori Fraud Triangle yang di kembangkan oleh Cressey (1953) dan

Fraud Pentagon yang dikembangankan oleh Jonathan Marks dari Crowe Horwath tahun 2011. Teori ini banyak digunakan dalam penelitian sebelumnya untuk menganalisis risiko kecurangan (Syavira and Aliyah 2023). Kedua teori tersebut yang menjelaskan faktor-faktor pendorong terjadinya fraud, seperti tekanan, peluang, rasionalisasi, kemampuan, dan arogansi. Teori ini digunakan untuk memperkuat pemahaman mengenai pentingnya penguatan sistem pengendalian internal dalam meminimalkan risiko cyber fraud.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan desain deskriptif. Menurut Sugiyono (2020), penelitian kualitatif bertujuan untuk memahami fenomena secara holistik melalui penyajian data dalam bentuk deskriptif. Pendekatan ini digunakan untuk menganalisis penerapan pengendalian *cyber fraud* di Bank CIMB Niaga menggunakan kerangka *Balanced Scorecard*.

Pengumpulan data dilakukan melalui studi dokumentasi. Menurut Sugiyono (2020), studi dokumentasi merupakan teknik pengumpulan data dengan menelaah dokumen tertulis yang relevan dengan objek penelitian. Data dianalisis secara kualitatif dengan mengelompokkan informasi berdasarkan empat perspektif *Balanced Scorecard*, yaitu keuangan, pelanggan, proses bisnis internal, serta pembelajaran dan pertumbuhan.

HASIL

Ringkasan Hasil Analisis

Perpspektif	Indikator Utama	Temuan
Keuangan	BOPO, Net prorifit, CAR	Kinerja keuangan yang relatif stabil mendukung keberlanjutan pengendalian *cyber fraud* melalui kemampuan bank dalam menjaga efisiensi dan kecukupan modal.
Pelanggan	Kontribusi transaksi digital, NPS, penyelesaian keluhan nasabah	Pengendalian *cyber fraud* berperan dalam menjaga kepercayaan nasabah terhadap keamanan layanan digital perbankan.
Proses Bisnis Internal	Teknologi keamanan, penanganan insiden *cyber fraud*, manajemen risiko oprasional	Penguatan sistem keamanan dan manajemen risiko internal meningkatkan efektivitas pengendalian *cyber fraud*
Pembelajaran dan Pertumbuhan	Adaptasi organisasi terhadap digitalisasi, integrasi strategi digital, struktur organisasi	Kesiapan organisasi dan penguatan sumber daya manusia mendukung keberlanjutan strategi pengendalian risiko digital.

Sumber: Diolah dari Laporan Tahunan Bank CIMB Niaga (2022-2024)

PEMBAHASAN

Perspektif Keuangan

Hasil penelitian menunjukkan bahwa stabilitas kinerja keuangan Bank CIMB Niaga selama periode 2022-2024 menunjukkan pola fluktuatif namun relatif stabil selama periode penelitian, yang mencerminkan efisiensi oprasional masih terjaga. Ini menjadi fondasi penting dalam mendukung efektivitas pengendalian *cyber fraud*. Kinerja keuangan yang relatif terjaga mencerminkan kemampuan bank dalam mempertahankan efisiensi operasional serta kecukupan permodalan di tengah meningkatnya risiko kejahatan digital. Kondisi ini memberikan ruang bagi manajemen untuk mengalokasikan sumber daya keuangan pada penguatan sistem keamanan teknologi. Temuan ini sejalan dengan pandangan Kaplan and Norton (1996) sebagai dasar dalam mendukung pencapaian strategi organisasi secara berkelanjutan. Selain itu Esther Akinbowale

et al. (2022) menegaskan bahwa stabilitas keuangan merupakan faktor penting dalam mendukung investasi keamanan digital sebagai bagian dari mitigasi *cyber fraud* di sektor perbankan.

Perspektif Pelanggan

Pada perspektif pelanggan, temuan penelitian menunjukkan bahwa peningkatan penggunaan layanan digital oleh nasabah tidak diikuti dengan penurunan tingkat kepercayaan terhadap keamanan transaksi. Hal ini mengindikasikan bahwa sistem pengendalian *cyber fraud* yang diterapkan bank mampu menjaga persepsi keamanan. Temuan ini sejalan dengan penelitian Febriana (2024) yang menyatakan bahwa tingkat adopsi layanan digital sangat dipengaruhi oleh persepsi keamanan dan keandalan sistem perbankan. Ketika keamanan digital terjaga, nasabah akan lebih aktif menggunakan layanan berbasis teknologi. Ini merupakan indikator nonkeuangan yang penting dalam menilai efektivitas pengendalian *cyber fraud*. Otoritas Jasa Keuangan (2024) juga menegaskan bahwa keamanan transaksi digital berperan langsung terhadap keberlanjutan hubungan antara bank dan nasabah, terutama dalam era transformasi digital perbankan.

Perspektif Proses Bisnis Internal

Temuan pada perspektif proses bisnis internal menunjukkan bahwa Bank CIMB Niaga melakukan penguatan pengendalian *cyber fraud* melalui peningkatan sistem keamanan, pengelolaan insiden, serta penerapan manajemen risiko operasional yang lebih terstruktur. Upaya tersebut mencerminkan bahwa pengendalian risiko digital telah menjadi bagian dari proses bisnis inti perbankan. Hasil ini sejalan dengan asel Committee on Banking Supervision (2023) yang menekankan bahwa efektivitas pengendalian risiko siber sangat bergantung pada integrasi antara teknologi keamanan dan proses operasional internal. Zul Azmi et al. (2022) menjelaskan bahwa peningkatan kualitas proses internal dan komitmen organisasi terhadap mutu operasional berkontribusi positif terhadap kinerja dan daya saing organisasi. Temuan tersebut menunjukkan bahwa penguatan proses internal merupakan faktor penting dalam mendukung pencapaian tujuan organisasi. Pengendalian internal merupakan elemen penting dalam pencegahan kecurangan fraud karena berfungsi menutup peluang terjadinya penyimpangan dalam proses operasional. Tampubolon and Rodiah (2020) menunjukkan bahwa pengendalian internal yang efektif serta moralitas individu berpengaruh signifikan terhadap kecenderungan terjadinya kecurangan akuntansi. Temuan ini menegaskan bahwa penguatan kontrol internal dan aspek perilaku individu merupakan fondasi utama dalam upaya pencegahan fraud.

Dalam konteks penelitian ini, kondisi tersebut relevan untuk menjelaskan pentingnya penguatan sistem dan proses internal sebagai bagian dari upaya pengendalian risiko digital pada Bank CIMB Niaga Pola tersebut sesuai dengan temuan penelitian yang menegaskan bahwa efektivitas pengendalian *cyber fraud* sangat dipengaruhi oleh kecepatan respon insiden, sistem pelaporan terintegrasi, serta evaluasi keamanan yang dilakukan secara rutin Katuri (2025). Selain itu penelitian Khuluddiyah (2025) juga menunjukkan bahwa penerapan manjemen risiko teknologi informasi yang komperhensif dapat membantu bank dalam menghadapi ancaman *cyber fraud* yang semakin kompleks.

Perspektif Pembelajaran dan Pertumbuhan

Pada perspektif pembelajaran dan pertumbuhan, hasil penelitian menunjukkan bahwa kesiapan organisasi mendukung keberlanjutan pengendalian *cyber fraud*. Temuan ini sejalan dengan Kaplan and Norton (1996) yang menegaskan bahwa perspektif pembelajaran dan pertumbuhan menjadi pendorong utama keberhasilan perspektif lainnya dalam *Balanced Scorecard*. Kesiapan tersebut tercermin melalui peningkatan kesadaran keamanan

informasi, penguatan tata kelola teknologi informasi, serta pengembangan kompetensi pegawai yang berkaitan dengan pengelolaan risiko digital. Kondisi ini menunjukkan bahwa pengendalian *cyber fraud* tidak hanya bergantung pada teknologi, tetapi juga pada kemampuan organisasi dalam membangun kapabilitas internal secara berkelanjutan. Temuan penelitian ini juga sejalan dengan pendapat Solms and Niekerk (2013) yang menyatakan bahwa keamanan informasi harus dipahami sebagai bagian dari budaya organisasi, bukan hanya sebagai aspek teknis teknologi. Dengan demikian, perspektif pembelajaran dan pertumbuhan berperan penting dalam membentuk perilaku, pola kerja, serta kesadaran keamanan yang berkelanjutan dalam mendukung pengendalian *cyber fraud* di sektor perbankan.

SIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa penerapan kerangka *Balanced Scorecard* mampu memberikan gambaran yang komprehensif terhadap efektivitas pengendalian *cyber fraud* di Bank CIMB Niaga selama periode 2022-2024. Pendekatan ini memungkinkan evaluasi pengendalian tidak hanya dilihat dari sisi keuangan, tetapi juga dari perspektif pelanggan, proses bisnis internal, serta pembelajaran dan pertumbuhan organisasi. Dari perspektif keuangan, hasil penelitian menunjukkan bahwa kinerja Bank CIMB Niaga berada pada kondisi yang relatif stabil dengan kecenderungan positif. Indikator efisiensi dan profitabilitas menunjukkan bahwa bank tetap mampu menjaga stabilitas operasional di tengah meningkatnya risiko kejahatan siber. Kondisi ini mengindikasikan bahwa investasi dan kebijakan penguatan keamanan teknologi informasi tidak mengganggu kinerja keuangan, melainkan justru mendukung keberlangsungan operasional dan pengelolaan risiko digital secara berkelanjutan. Pada perspektif pelanggan, peningkatan kontribusi transaksi digital serta tingkat kepuasan dan penyelesaian keluhan nasabah yang tetap terjaga mencerminkan meningkatnya kepercayaan masyarakat terhadap sistem keamanan perbankan. Hal ini menunjukkan bahwa strategi pengendalian *cyber fraud* yang diterapkan tidak hanya berorientasi pada aspek teknis, tetapi juga berdampak langsung terhadap persepsi dan rasa aman nasabah dalam menggunakan layanan digital bank. Selanjutnya, dari perspektif proses bisnis internal, Bank CIMB Niaga secara konsisten memperkuat sistem pengendalian melalui pengembangan teknologi keamanan, peningkatan manajemen insiden, serta penerapan kerangka manajemen risiko operasional. Penggunaan sistem keamanan berlapis, simulasi serangan siber, dan evaluasi anti-fraud management menunjukkan adanya keseriusan bank dalam memitigasi potensi risiko *cyber fraud* yang semakin kompleks dan dinamis. Sementara itu, pada perspektif pembelajaran dan pertumbuhan, hasil penelitian memperlihatkan adanya peningkatan kesiapan organisasi dalam menghadapi tantangan digital.

Penguatan struktur organisasi, integrasi strategi digital, serta peningkatan kesadaran sumber daya manusia terhadap risiko kejahatan siber menjadi faktor pendukung penting dalam membangun sistem pengendalian yang berkelanjutan. Hal ini menegaskan bahwa efektivitas pengendalian *cyber fraud* tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh kesiapan manusia dan budaya organisasi. Secara keseluruhan, penelitian ini menunjukkan bahwa pengendalian *cyber fraud* di Bank CIMB Niaga telah berjalan secara terintegrasi dan mengalami penguatan dari tahun ke tahun. Pendekatan *Balanced Scorecard* terbukti mampu menjadi alat evaluasi strategis yang efektif dalam menilai kesiapan organisasi menghadapi risiko digital secara menyeluruh. Dengan demikian, keberhasilan pengendalian *cyber fraud* tidak hanya bergantung pada aspek teknis keamanan, tetapi juga pada sinergi antara kinerja keuangan, kepercayaan nasabah, efektivitas proses internal, serta kesiapan organisasi dalam menghadapi

perkembangan ancaman siber di sektor perbankan.

DAFTAR RUJUKAN

Abdalla, Yousif Abdelbagi, Abdelrahman Mohamed Ibrahim, Alhashmi Aboubaker Lasyoud, and Mohammed Hersi Warsame. 2022. "Barriers of Implementing the Balanced Scorecard: Evidence From the Banking Sector in the Developing Market." *Journal of Governance and Regulation* 11(2):173–80. doi: 10.22495/jgrv11i2art15.

Akinbowale, Oluwatoyin Esther Heinz Eckart, and Mulatu Fekadu Zerihun. 2020. "Analysis of Cyber-Crime Effects on the Banking Sector Using the Balanced Score Card: A Survey of Literature." *Journal of Financial Crime* 27(3):945–58. doi: 10.1108/JFC-03-2020-0037.

Akinbowale, Oluwatoyin Esther, Polly Mashigo, and Mulatu Fekadu Zerihun. 2023. "Application of Balance Scorecard as a Strategic Management and Performance Measurement Tool for Cyberfraud Mitigation ' Internal Determinants of Bank Deposit Flows under Different Market Conditions in Ghana ."" (August). doi: 10.21511/bbs.19(1).2024.19.

Badan Siber dan Sandi Negara. 2024. "Lanskap Keamanan Siber Indonesia 2024." (70).

Basel Committee on Banking Supervision. 2023. "Basel Committee on Banking Supervision Discussion Paper." *Report* 1(1):1–8.

Cressey, Donald R. 1953. *Other People's Money: A Study in the Social Psychology of Embezzlement*. Glencoe, IL: Free Press (atau Patterson Smith, jika pakai versi reprint 1973).

Cyberscurity Ventures. 2021. "Cybercrime To Cost The World $10.5 Trilion Annually By 2025."

Esther Akinbowale, Oluwatoyin, Heinz, and Mulatu Fekadu Zerihun. 2022. "The Use of the Balanced Scorecard as a Strategic Management Tool to Mitigate Cyberfraud in the South African Banking Industry." *Heliyon* 8(12). doi: 10.1016/j.heliyon.2022.e12054.

Febriana, Vii Cendrik. 2024. "Jurnal Ekonomika Dan Bisnis Islam E-ISSN: 2686-620X Halaman 161-174." 7:161–74.

Kaplan, Robert S., and David P. Norton. 1992. "The Balanced Scorecard - Measures That Drive Performance. (Includes Related Articles)." *Harvard Business Review* 70(1):71.

Kaplan, Robert S., and David P. Norton. 1996. "The BALANCED SCORECARD." Pp. 1–14 in *Sustainability (Switzerland)*. Vol. 11.

Katuri, Sandeep. 2025. "Cybersecurity Threats in Digital Banking : A Comprehensive Analysis." 16(1):1–16.

Khuluddiyah, Zulaikhatul. 2025. "Implementasi Manajemen Risiko Teknologi Informasi Dalam Proses Transformasi Digital Bank Syariah Indonesia." 3:771–75.

Kwaijtaal, Anton. 2024. "Decoding the Dynamics in Liability Law." *SSRN Electronic Journal* 21(2). doi: 10.2139/ssrn.4709302.

OJK. 2024. "Stakeholder Engagement Disclosures in Sustainability Reports: Evidence from Italian Food Companies." *Business Ethics, the Environment and Responsibility* 34(1):260–79. doi: 10.1111/beer.12642.

Otoritas Jasa Keuangan. 2025. "Modus Kejahatan Di Sektor Jasa Keuangan Makin Kompleks." Retrieved (https://keuangan.kontan.co.id/news/modus-kejahatan-di-sektor-jasa-keuangan-makin-kompleks-ojk-upayakan-hal-ini).

Rodiah, Siti, Ika Ardianni, and Aftania Herlina. 2019. "Pengaruh Pengendalian Internal, Ketaatan Aturan Akuntansi, Moralitas Manajemen Dan Budaya Organisasi Terhadap Kecurangan Akuntansi The Effect of Internal Control, Compliance with Accounting Rules, Management Morality and Organization Culture to Accounting Fraud."

Satrya, Ilham Zharfan. 2024. "SERANGAN SIBER DALAM PERKEMBANGAN DIGITAL DI INDONESIA." 9(10).

Solms, Rossouw Von, and Johan Van Niekerk. 2013. "From Information Security to Cyber Security." *Computers & Security* 38:97–102. doi: 10.1016/j.cose.2013.04.004.

Sugiyono. 2020. *Metodologi Penelitian Kuantitatif, Kualitatif Dan R & D*.

Syavira, Cindy, and Siti Aliyah. 2023. "Fraudulent Financial Statement : Pengujian Fraud Pentagon Theory Pada Sektor Industri Dan Barang Konsumsi Yang Terdaftar Di Bursa Efek Indonesia." 20(1):111–32.

Tampubolon, Evelina, and Siti Rodiah. 2020. "Pengaruh Pengendalian Internal Dan Moralitas Individu Terhadap Kecurangan (Fraud) Akuntansi (Studi Eksperimen Pada Mahasiswa Universitas Muhammadiyah Riau)." 4(1):37–42. doi: 10.18196/rab.040151.

Zul Azmi, Nuraima, Fadrul. 2021. "KNOWLEDGE MANAGEMENT AND HOSPITAL PERFORMANCE BASED ON BALANCED SCORECARD IN PEKANBARU." 6(2):213–21.

Zul azmi, Sulistiamdary, Siti Samsiah. 2022. "Apakah Biaya Kualitas Penting Meningkatkan Keunggulan Kompetitif Dan Kinerja Organisasi." 12(2). doi: 10.37859/jae.v12i2.4264.