TANTANGAN PENGENDALIAN SISTEM INFORMASI DALAM MENJAGA KEAMANAN DATA PADA KANTOR AKUNTAN PUBLIK

Dinda Wulandari[1], Rahma Nurulhida[2*]

AFILIASI
[1,2] Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Kudus

***Korespondensi:** Email : rahmanurulhida899@gmail.com

DOI: 10.22219/jafin.v5i1.15493

SEJARAH ARTIKEL
Diterima:
7 Februari 2026
Direview:
10 Februari 2026
Direvisi:
4 Maret 2026
Diterbitkan:
17 Maret 2026

Kantor :
Jurusan Akuntansi, Fakultas Ekonomi
Universitas Wahid Hasyim
Jl. Menoreh Tengah X/22
Sampangan, Semarang 50236
Central Java, Indonesia.

P-ISSN : 2963-1076
E-ISSN : 2962-9861

Abstrak

Perkembangan teknologi informasi (TI) yang pesat telah mendorong transformasi digital pada berbagai sektor, termasuk Kantor Akuntan Publik (KAP). Pemanfaatan sistem informasi berbasis digital dalam pengelolaan data keuangan tidak hanya meningkatkan efisiensi, tetapi juga menghadirkan risiko baru terkait keamanan data. Penelitian ini bertujuan untuk mengidentifikasi tantangan serta upaya penguatan pengendalian sistem informasi pada KAP Kumalahadi, Sugeng Pamudji & Rekan Cabang Semarang. Metode penelitian yang digunakan adalah kualitatif dengan pendekatan deskriptif, melalui wawancara mendalam dengan auditor dan tim teknologi informasi, serta observasi langsung terhadap praktik pengendalian sistem informasi. Hasil penelitian menunjukkan bahwa KAP menghadapi berbagai kendala, seperti keterbatasan infrastruktur, ketergantungan pada media fisik dan platform pihak ketiga, lemahnya manajemen file, serta meningkatnya ancaman keamanan siber. Selain itu, keterbatasan kompetensi teknis auditor dalam bidang TI juga menjadi hambatan signifikan. Meski demikian, KAP telah melakukan sejumlah langkah penguatan, antara lain penggunaan email khusus berkapasitas besar, pembatasan akses data, penyusunan pedoman tata kelola data, hingga perekrutan SDM dengan kompetensi TI. Penelitian ini menyimpulkan bahwa pengendalian sistem informasi di KAP tidak hanya merupakan isu teknis, melainkan juga strategis yang membutuhkan integrasi teknologi, investasi infrastruktur, serta budaya kepatuhan untuk menjaga integritas dan kerahasiaan data klien.

Kata Kunci: keamanan data, sistem informasi, teknologi informasi, pengendalian internal, Kantor Akuntan Publik.

Abstract

The rapid development of information technology (IT) has driven digital transformation in various sectors, including Public Accounting Firms (KAP). The use of digital-based information systems in financial data management not only increases efficiency but also presents new risks related to data security. This study aims to identify challenges and efforts to strengthen information system controls at the Semarang Branch of KAP Kumalahadi, Sugeng Pamudji & Rekan. The research method used was qualitative with a descriptive approach, through in-depth interviews with auditors and the information technology team, as well as direct observation of information system control practices. The results show that the KAP faces various obstacles, such as limited infrastructure, reliance on physical media and third-party platforms, weak file management, and increasing cybersecurity threats. Furthermore, the limited technical competence of auditors in the IT field is also a significant obstacle. Nevertheless, the KAP has taken several strengthening measures, including the use of special large-capacity email, limiting data access, developing data governance guidelines, and recruiting human resources with IT competencies. This study concludes that information system controls at KAP are not only a technical issue, but also a strategic one that requires technology integration, infrastructure investment, and a culture of compliance to maintain the integrity and confidentiality of client data.

***Keyword**: data security, information systems, information technology, internal control, Public Accounting Firm.*

PENDAHULUAN

Perkembangan teknologi informasi (TI) yang pesat telah mendorong transformasi digital di berbagai sektor bisnis (Nurhayati & Yanti, 2024). Pemanfaatan sistem berbasis digital dalam pengelolaan data keuangan meningkatkan efisiensi sekaligus menimbulkan risiko baru terkait keamanan informasi. Data keuangan yang bersifat sensitif memiliki implikasi besar terhadap kredibilitas serta keberlangsungan entitas apabila mengalami kebocoran atau manipulasi (Cremer dkk., 2022). Risiko seperti kegagalan sistem, lemahnya pengendalian internal berbasis teknologi, maupun akses tidak sah dapat memengaruhi kualitas laporan keuangan dan menurunkan tingkat kepercayaan pemangku kepentingan (Nurwanah, 2024).

Dalam konteks pengelolaan organisasi dan audit, pengendalian internal menjadi komponen penting untuk menjaga efektivitas, efisiensi, keandalan pelaporan keuangan, serta kepatuhan terhadap regulasi (Hamed, 2023). Menurut kerangka kerja COSO, pengendalian internal terdiri dari lima komponen utama, yaitu lingkungan pengendalian, penilaian risiko, aktivitas pengendalian, informasi dan komunikasi, serta pemantauan (Saputra & Novita, 2023). Seluruh komponen ini berperan penting dalam memastikan setiap proses organisasi, termasuk sistem informasi, berjalan sesuai prinsip kehati-hatian dan keamanan yang memadai.

Seiring meningkatnya kompleksitas sistem berbasis digital, Information Technology (IT) menjadi tulang punggung bagi operasional bisnis modern. IT mencakup perangkat keras, perangkat lunak, jaringan, serta sumber daya manusia yang digunakan untuk mengolah, menyimpan, dan menyebarkan informasi secara cepat dan akurat (Li, 2021). Penerapan TI memungkinkan integrasi proses bisnis dan pengambilan keputusan berbasis data, sekaligus meningkatkan produktivitas organisasi (Indra Rizki Hasibuan & Rahmi Syahriza, 2025). Namun, ketergantungan tinggi terhadap TI juga membawa konsekuensi meningkatnya risiko keamanan data yang harus diantisipasi melalui sistem pengendalian yang kuat.

Dalam bidang audit, kemajuan teknologi juga mendorong munculnya konsep teknologi audit, yaitu pemanfaatan perangkat lunak, sistem informasi, dan aplikasi berbasis digital untuk mendukung proses audit mulai dari pengumpulan data hingga analisis bukti audit. Teknologi audit modern memanfaatkan big data, kecerdasan buatan (AI), dan machine learning (ML) untuk meningkatkan efisiensi, akurasi, serta kemampuan deteksi risiko (Putri dkk., 2022). Dengan demikian, auditor dituntut tidak hanya memiliki kompetensi akuntansi, tetapi juga pemahaman terhadap risiko teknologi dan sistem informasi yang digunakan oleh klien (Nasruddin dkk., 2023).

Kantor Akuntan Publik (KAP) sebagai lembaga profesional yang memperoleh izin resmi dari Menteri Keuangan berdasarkan Undang-Undang Nomor 5 Tahun 2011 memiliki tanggung jawab besar dalam menjaga integritas dan kerahasiaan data klien (Rofikah & ., 2022). KAP tidak hanya berperan dalam memberikan opini atas kewajaran laporan keuangan, tetapi juga memiliki kewajiban untuk memastikan bahwa proses audit dilakukan secara aman dan sesuai dengan standar profesional (Arda, 2024). Dalam era digital, tantangan bagi KAP semakin besar karena harus memastikan sistem informasi yang digunakan baik oleh auditor maupun klien berada dalam kondisi aman dan terkendali.

Namun, di Indonesia, penerapan praktik pengamanan sistem informasi di KAP masih menghadapi berbagai kendala, mulai dari keterbatasan sumber daya manusia, infrastruktur teknologi, hingga regulasi yang belum sepenuhnya

mengakomodasi kebutuhan tersebut (Priardhina & Sari, 2025). KAP memiliki tanggung jawab menjaga kerahasiaan dan integritas data klien, tetapi upaya pengendalian internal berbasis teknologi masih terbatas dan belum terstandar secara menyeluruh (Ningsih & Abdurahman, 2024). Kondisi ini menimbulkan celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab dan berpotensi menurunkan kepercayaan publik terhadap profesi auditor.

Penelitian terdahulu menunjukkan pentingnya peran pengendalian sistem informasi dalam proses audit. Berdasarkan penelitian yang dilakukan (Apriyanto dkk., 2024) menyoroti pentingnya kerangka berbasis risiko dan kompetensi auditor dalam mengurangi risiko sistem informasi. Penelitian yang dilakukan (Susanto & Soepriyanto, 2024) menemukan bahwa tingkat pengungkapan risiko teknologi berhubungan dengan biaya audit, sementara (Kurniawan & Mulyawan, 2023) menekankan bahwa kolaborasi auditor dengan tim IT serta tata kelola TI klien menjadi faktor kunci dalam meningkatkan keamanan data.

Namun, penelitian yang secara spesifik menyoroti bagaimana KAP, khususnya di tingkat cabang, menghadapi tantangan dalam menjaga keamanan sistem informasi masih jarang ditemukan. Oleh karena itu, penelitian ini memiliki kebaruan pada fokusnya terhadap praktik pengendalian sistem informasi dan keamanan data di Kantor Akuntan Publik Kumalahadi, Sugeng Pamudji & Rekan Cabang Semarang. Penelitian ini tidak hanya menyoroti tantangan umum yang dihadapi auditor dalam menjaga kerahasiaan data, tetapi juga menggali secara mendalam upaya konkret penguatan sistem yang dilakukan oleh KAP tersebut. Penelitian ini bertujuan untuk mengidentifikasi tantangan dalam pengendalian sistem informasi pada Kantor Akuntan Publik dan menganalisis upaya yang dilakukan dalam memperkuat keamanan data klien.

Berdasarkan uraian diatas, maka penelitian ini berjudul "Pengendalian Sistem Informasi di Kantor Akuntan Publik: Tantangan dan Upaya Penguatan Keamanan Data pada KAP Kumalahadi, Sugeng Pamudji & Rekan Cabang Semarang" guna mengidentifikasi dan menganalisis tantangan yang dihadapi dalam menjaga keamanan data berbasis sistem informasi serta menggali upaya penguatan prosedur pengendalian internal yang dilakukan auditor dalam menghadapi potensi ancaman digital.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif (Villamin dkk., 2025). Pendekatan ini dipilih karena penelitian bertujuan untuk memahami secara mendalam tantangan yang dihadapi Kantor Akuntan Publik (KAP) Kumalahadi, Sugeng Pamudji & Rekan Cabang Semarang dalam menjaga keamanan data berbasis sistem informasi, serta untuk menggali upaya penguatan prosedur pengendalian intesrnal yang telah dilakukan.

Sumber data dalam penelitian ini terdiri dari data primer dan sekunder. Data primer diperoleh melalui wawancara mendalam dengan auditor dan tim teknologi informasi (TI) KAP, serta observasi langsung terhadap praktik pengendalian sistem informasi yang diterapkan dalam proses audit. Sementara itu, data sekunder diperoleh dari literatur berupa buku, jurnal ilmiah, regulasi terkait akuntan publik, serta publikasi resmi dari Ikatan Akuntan Indonesia (IAI) yang relevan dengan isu pengendalian sistem informasi dan keamanan data (Dewi dkk., 2025).

Teknik analisis data dilakukan dengan model analisis interaktif yang mencakup reduksi data, penyajian data, dan penarikan kesimpulan/verifikasi (Mezmir, 2020). Analisis ini digunakan untuk mengidentifikasi pola, tantangan, serta strategi penguatan keamanan data yang dilakukan oleh KAP. Oleh karena itu, hasil penelitian diharapkan mampu memberikan gambaran menyeluruh tentang bagaimana KAP mengantisipasi risiko digital sekaligus menjaga integritas dan kerahasiaan data klien.

HASIL DAN PEMBAHASAN

This study centers on PT Unilever Indonesia Tbk, a publicly traded enterprise operating in the fast-moving consumer goods industry. Its business scope covers personal Penelitian ini berfokus pada tantangan dan upaya yang dilakukan oleh KAP Kumalahadi, Sugeng Pamudji & Rekan Cabang Semarang dalam upaya pengendalian keamanan data klien. Penulis memilih dua narasumber yaitu satu tim IT dan satu akuntan publik yang diharapkan dapat mendapatkan dua sudut pandang berbeda terkait dengan pengendalian keamanan data klien.

Berdasarkan hasil wawancara dua narasumber, bisa dilihat bahwa kedua pihak menekankan pentingnya tanggung jawab akuntan publik dalam menjaga kerahasiaan serta keamanan data klien. Narasumber pertama menegaskan bahwa managemen harus menjaga kerahasiaan data klien dan sudah diatur secara formal dalam Surat Perjanjian Kerja (SPK) dan Surat Perikatan Audit (SPA), sehingga setiap data yang diterima harus dikelola dengan prosedur tertentu. Akses data juga dibatasi hanya untuk pihak-pihak yang berkepentingan, baik melaluimedia fisik (flashdisk atau SSD portable) maupun platform daring seperti Google Drive. Hal serupa juga diungkapkan oleh narasumber kedua yang menekankan bahwa akuntan public memiliki tanggung jawab besar dalam memastikan data klien tersimpan denga naman dan hanya bisa diakses oleh pihak yang memiliki kepentingan.

Terkait tantangan utama, kedua narasumber memiliki pandangan yang relatif sama. Narasumber pertama menyoroti kendala teknis seperti kerentanan media fisik (mudah rusak atau tercecer), serta kurangnya manajemen penamaan file pada cloud storage. Sementara itu, narasumber kedua menekankan pada tantangan yang lebih strategis, yaitu ancaman keamanan siber yang semakin canggih, pengelolaan akses data yang aman, serta kepatuhan seluruh pihak (Akuntan Publik, Staf Auditor, Personel Support & Klien) terhadap kebijakan keamanan serta pengamanan data.

Dari sisi koordinasi, narasumber pertama meyampaikan bahwa di internal KAP sudah memiliki system email khusus berkapasitas 100GB untuk menampung data klien, serta kewajiban ketua tim audit untuk membuat folder setiap entitas yang akan diaudit agar file lebih terorganisir. Narasumber kedua menambahkan bahwa koordinasi era tantara akuntan public dengan tim IT maupun auditor internal sangat penting. Hal ini dilakukan untuk memastikan pengendalian internal memadai sekaligus menajaga system keamanan data agar tetap efektif dan mutakhir.

Dalam jalannya suatu system, tentu memiliki kendala. Kendala yang pernah terjadi disampaikan oleh narasumber yang mana menuturkan pengalaman saat proses audit sebuah Perusahaan sistem konvesional yang baru bermigrasi ke sistem syariah, dimana pada kasus ini Pihak KAP KSP Cabang Semarang telah sedini mungkin mengantisipasi tata kelola data-data digital secara tertib dan aman, sehingga ketika

terjadi penyampaian oleh Pihak Klien melalui petugas yang tidak menguasai tata kelola database secara baik & benar yang pada akhirnya menimbulkan kesalahpahaman dimana terjadi pergeseran data secara signifikan antara data asli versi petugas Pemeriksa Internal dgn Petugas TI sehingga menimbulkan perbedaan sajian yg signifikan dengan klien, , maka Pihak KAP KSP Cabang Semarang dapat segera memetakan serta memitigasi masalah tersebut dengan cepat & akurat.

Dalam beberapa kasus lain Pihak KAP KSP Cabang Semarang melalui unit kerja DevPro (Development Program) juga mampu membantu Auditor utk mendalami lingkungan TI (Teknologi Informasi) sederhana guna Risk Audit Assesment dan juga mampu mendeteksi adanya ketidakstabilan sandi, parameter serta anomali perhitungan & hasil penghitungan (Mathic Environment) pada suatu CBusS (Core Bussines System) yang digunakan dengan memanfaatkan serta mengoptimalisasi fungsi-fungsi perumusan pada MS Excell (Audit Berbasis Komputer). Dari kasus tersebut, muncul kesadaran bersama, terutama bg Pihak Klien, bahwa pengelolaan data memerlukan sumber daya yang mahir dalam tata kelola database, CBusS juga memerlukan pengawasan & pemeliharaan yg rutin & konsisten oleh Pihak Pemangku Kepentingan. Adapun Sementara itu keterampilan tersebut masih belum banyak yang diajarkan dalam Pendidikan akuntansi formal.

Jika dilihat dari kekuatan system pengendalian internal, kedua narasumber sepakat bahwa kondisinya masih jauh dari kata ideal dan masih perlu terus didorong pengembangannya. Narasumber pertama menyoroti keterbatasan sarana prasarana, termasuk ketergantungan pada media fisik dan platform pihak ketiga seperti Google Drive. Narasumber kedua melalui Tim DevPro menjelaskan bahwa butuh investasi besar untuk memperkuat system, namun sejumlah Langkah sudah ditempuh, aantara lain seperti penyusunan pedoman tata kelola data, perancangan berbagai tools plan, tools audit & tools audit report serta penerapan management security access, penggunaan layanan pihak ketiga berbayar untuk meningkatkan pengamanan terhadap firewall system serta data encription, merekrut SDM jurusan Akuntansi atau Keuangan Plus (mahir dalam pengelolaan dasar berbagai database serta mampu melakukanb optimalisasi MS Office) hingga nantinya dapat merekrut SDM dengan kompetensi IT.

Maka terlepas dari hal-hal tersebut, terkait dengan pandangan dan harapan ke depan,narasumber pertama berharap adanya SOP spesifik agar tercipta alur kerja yang lebih jelas, terutama bagi karyawan baru. Narasumber kedua menekankan pentingnya menciptakan lingkungan teknologi informasi yang khas dan sesuai dengan kebutuhan industry KAP, sehingga mampu mendukung keamanan data klien secara lebih efektif dan berkelanjutan.

KESIMPULAN

Penelitian ini menyoroti tantangan dan Upaya penguatan pengendalian system informasi di KAP Kumalahadi, Sugeng Pamudji & Rekan Cabang Semarang. Hasil penelitian menunjukkan bahwa meskipun kesadaran akan pentingnya menjaga kerahaisaan dan keamanan data klien sudah cukup tinggi, praktik dilapangan masih menghadapi berbagai kendala. Tantangan yang ditemukan antara lain keterbatasan sarana prasarana, ketergantungan pada media fisik maupun platform pihak ketiga, lemahnya manajemen file, serta meningkatnya ancaman keamanan siber. Selain itu,

kurangnya kompetensi teknis auditor dalam bidang teknologi informasi juga bisa menjadi hambatan tersendiri dalam mengelola risiko digital secara optimal.

Walaupun demikian, manajemen telah melakukan sejumlah langkah penguatan, seperti penggunaan email khusus berkapasitas besar, pembatasan akses data, penyusunan pedoman tata Kelola data, hingga perekrutan SDM dengan kompetensi teknologi. Langkah-langkah ini menunjukkan adanya komitmen dalam menjaga integritas dan kerahasiaan data klien. Namun, berdasarkan perspektif narasumber kondisi pengendalian internal masih jauh dari kata ideal dan membutuhkan investasi besar baik dalam aspek infrastruktur, kebijakan, maupun peningkatan kapasitas SDM**.**

Dengan demikian, dapat disimpulkan bahwa keamanan system informasi di KAP Kumalahadi, Sugeng Pamudji & Rekan Cabang Semarang bukan hanya sekedar isu teknis melainkan juga strategis. Untuk menjamin keberlanjutan dan kredibilitas, KAP perlu mengintegrasikan pendekatan berbasis risiko, teknologi mutakhir, serta peningkatan budaya kepatuhan dalam pengelolaan data klien.

Terkait dengan keberlanjutan sistem keamanan data manajemen, terdapat beberapa saran penulis diantaranya perlunya Menyusun dan menerapkan Standar Operasional Prosedur (SOP) yang lebih rinci terkait pengelolaan data, termasuk mekanisme penyimpanan, pengarsipan,dll. SOP ini sangat penting terutama bagi karyawan baru atau tenaga magang agar dapat meminimalisir potensi kelalaian. Perlunya investasi yang lebih besar pada infrastruktur teknologi, misalnya pengadaan server internal dengan enkripsi kuat atau system cloud berlisensi resmi dengan tingkat keamanan tinggi. Hal ini dapat mengurangi ketergantungan pada platform pihak ketiga yang rawan kebocoran data. System pengendalian internal yang sudah diterapkan perlu dievaluasi secara berkala.

Pemantauan secara berkala dapat membantu KAP mengidentifikasi kelemahansejak dini dan memperbaikinya sebelum menimbulkan dampak yang signifikan terhadap keamanan data klien. Saran untuk penulis, penelitian ini masih terbatas pada satu kantor cabang. Untuk penelitian berikutnya diharapkan penulis dapat memperluas objek ke lebih dari satu KAP atau menbandingkan antar cabang, sehingga hasilnya lebih komprehensif dan dapat diperbandingkan.

DAFTAR PUSTAKA

Apriyanto, A., Mudawanah, S., Sutanto, E., Purnomo, A. D., & Murniawan, M. W. (2024). Auditing in the Era of Cybersecurity: Challenges and Solutions. *Journal Markcount Finance*, *2*(2), 285–295. https://doi.org/10.70177/jmf.v2i2.1291

Arda, D. P. (2024). Peran Akuntan Publik Dalam Penerapan Good Governance Di Pasar Modal (Tinjauan Standar Audit). *Jurnal Akuntansi, Keuangan, Pajak Dan Informasi (JAKPI)*, *4*(1), 12–24. https://doi.org/10.32509/jakpi.v4i1.4087

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Dewi, A. K., Sibarani, B. K., Saputra, E., Norazlina, N., Susanti, S., Syafira, Y., & Munakalla, Y. (2025). Strategi Efektif Pengendalian Internal dalam Keamanan Sistem Informasi Akuntansi untuk Perlindungan Data Keuangan. *Jurnal Ilmiah Raflesia Akuntansi*, *11*(1), 138–148. https://doi.org/10.53494/jira.v11i1.838

Hamed, R. (2023). *The Role of Internal Control Systems in Ensuring Financial Performance Sustainability*. *15*(13).

Indra Rizki Hasibuan, & Rahmi Syahriza. (2025). Peran Teknologi Informasi Dalam Meningkatkan Efisiensi Administrasi Di Bpjs Kesehatan Cabang Padang Sidiempuan. *Jurnal Review Pendidikan Dan Pengajaran*, *8*, 1757–1760.

Kurniawan, Y., & Mulyawan, A. N. (2023). The Role of External Auditors in Improving Cybersecurity of the Companies through Internal Control in Financial Reporting. *Journal of System and Management Sciences*, *13*(1), 485–510. https://doi.org/10.33168/JSMS.2023.0126

Li, H. (2021). *Optimization of the Enterprise Human Resource Management Information System Based on the Internet of Things*. https://doi.org/10.1155/2021/5592850

Mezmir, E. A. (2020). Qualitative Data Analysis: An Overview of Data Reduction, Data Display and Interpretation. *Research on Humanities and Social Sciences*, *10*(21), 15–27. https://doi.org/10.7176/rhss/10-21-02

Nasruddin, N. A., Pomtoh, G. T., & Kusumawati, A. (2023). The Role of Technology in Detecting Cyber Risk and Improving Internal Audit: A Systematic Review. *Jurnal Akuntansi*, *18*(2), 173–183. https://doi.org/10.37058/jak.v18i2.7675

Ningsih, R. Y., & Abdurahman. (2024). Peran dan Potensi Implementasi Audit TI dalam Transformasi Digital Berkelanjutan pada Sektor Publik di Indonesia. *Indonesian Journal of Auditing and Accounting (IJAA) 2024*, *1*(1), 120–139. www.jurnal.iapi.or.id

Nurhayati, M., & Yanti, S. N. (2024). Peran Teknologi Informasi Dalam Transformasi Bisnis Dan Ekonomi. *Jurnal Review Pendidikan Dan Pengajaran*, *7*(3), 10008–10012.

Nurwanah, A. (2024). Cybersecurity in Accounting Information Systems: Challenges and Solutions. *Advances in Applied Accounting Research*, *2*(3), 157–168. https://doi.org/10.60079/aaar.v2i3.336

Priardhina, I., & Sari, R. (2025). (2025). *Current Challenges in the Digital Era : the Moderating Role of*. *6*(2), 301–315.

Putri, O. A., Hariyanti, S., & Kediri, I. (2022). Review Artikel: Transformasi Digital Dalam Bisnis Dan Manajemen. *Proceedings of Islamics Economics, Business, and Philantrhropy*, *1*(1), 135–166. https://jurnalfebi.iainkediri.ac.id/index.php/proceedings

Rofikah, S., & . N. (2022). Pengaruh Pertimbangan Pasar Kerja, Penghargaan Finansial, Dan Nilai Intrinsik Pekerjaan Terhadap Minat Pemilihan Karier Sebagai Akuntan Publik (Studi Empiris Pada Mahasiswa Akuntansi Universitas Wiraraja Madura). *Journal of Accounting and Financial Issue (JAFIS)*, *3*(1), 50–70. https://doi.org/10.24929/jafis.v3i1.2042

Saputra, M. A., & Novita. (2023). Sistem Pengendalian Internal Berdasarkan COSO Framework Pada Perusahaan Konstruksi. *Jurnal Riset Akuntansi Politala*, *6*(1), 197–210. http:jra.politala.ac.id/indexx.php/JRA/index

Susanto, & Soepriyanto, G. (2024). Cybersecurity disclosure and audit fees: An empirical study of listed companies on the Indonesia stock exchange. *Edelweiss Applied Science and Technology*, *8*(6), 6090–6104. https://doi.org/10.55214/25768484.v8i6.3328

Villamin, P., Lopez, V., Thapa, D. K., & Cleary, M. (2025). A Worked Example of Qualitative Descriptive Design: A Step-by-Step Guide for Novice and Early Career Researchers. *Journal of Advanced Nursing*, *81*(8), 5181–5195. https://doi.org/10.1111/jan.16481