Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 3, Issue May, 2025 pp. 898-905 http://urj.uin-malang.ac.id/index.php/mij/index

Analisis manajemen risiko berbasis teknologi informasi pada produk E-Banking syariah

Silvia Nazma Zahira
Program Studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang
e-mail: silvianazma@gmail.com

Kata Kunci:
manajemen risiko tii; e-banking syariah; keamanan digital; kepatuhan syariah

Keywords:
IT risk management; Islamic digital banking; cybersecurity; sharia compliance

A B S T R A K

Perkembangan teknologi digital dalam industri perbankan syariah memunculkan peluang besar sekaligus risiko baru, terutama yang berkaitan dengan penggunaan teknologi informasi (TI). Penelitian ini bertujuan untuk mengkaji strategi pengelolaan risiko berbasis TI yang diterapkan pada layanan e-banking syariah guna menjaga keberlangsungan operasional serta memastikan kepatuhan terhadap prinsip-prinsip syariah. Dengan menggunakan metode kualitatif deskriptif melalui studi pustaka, penelitian ini menemukan bahwa pengelolaan risiko TI dalam e-banking syariah mencakup tata kelola TI yang sesuai syariah, penerapan sistem keamanan digital yang kuat, pengawasan terhadap mitra teknologi, serta penguatan kapasitas sumber daya manusia. Selain itu, keterlibatan aktif Dewan Pengawas Syariah (DPS) dan edukasi nasabah menjadi faktor pendukung penting dalam menanggulangi risiko. Temuan ini menegaskan bahwa sistem manajemen risiko yang terintegrasi dan sejalan dengan nilai-nilai Islam sangat diperlukan untuk menjaga keberlanjutan layanan perbankan digital syariah di era teknologi saat ini.

A B S T R A C T

Digital advancements in the Islamic banking sector have brought significant opportunities alongside emerging risks, particularly those related to the use of information technology (IT). This study explores how Islamic banks implement IT-based risk management strategies within their e-banking services to maintain operational reliability and uphold Sharia compliance. Utilizing a descriptive qualitative method through literature analysis, the study finds that effective IT risk management in Islamic e-banking involves key elements such as Sharia-aligned IT governance, strong cybersecurity measures, oversight of third-party service providers, and staff capacity development. Moreover, active participation from the Sharia Supervisory Board (SSB) and ongoing customer education play an essential role in strengthening risk prevention efforts. The results affirm that a Sharia-compliant and integrated risk management system is vital for the resilience and integrity of digital banking operations in the current technological landscape.

Pendahuluan

Kemajuan teknologi informasi telah mengubah secara signifikan bagi ndustri perbankan, termasuk di dalamnya perbankan syariah. Penggunaan teknologi digital seperti layanan e-banking memungkinkan transaksi keuangan dilakukan secara cepat, fleksibel, dan tanpa batasan waktu atau tempat. Melalui fitur seperti internet banking, mobile banking, serta ATM berbasis prinsip syariah, bank dapat menjangkau nasabah dengan lebih luas dan efisien. Meskipun begitu, transformasi digital ini membawa tantangan tersendiri, terutama dalam hal keamanan siber, integritas data, serta

kepatuhan terhadap nilai-nilai syariah (Faizal et al., 2023).

Dalam sistem perbankan syariah, tantangan tersebut tidak hanya berkaitan dengan aspek teknis seperti potensi peretasan atau gangguan sistem, tetapi juga terkait dengan keharusan untuk tetap menjaga kesesuaian terhadap ajaran Islam. Transaksi yang dilakukan secara elektronik tetap harus bebas dari unsur-unsur yang dilarang, seperti riba, ketidakjelasan (gharar), dan perjudian (maysir). Oleh karena itu, sistem pengelolaan risiko berbasis teknologi informasi harus disusun dengan mengedepankan pendekatan yang tidak hanya menjamin keamanan operasional, tetapi juga memenuhi standar etika dan hukum Islam (Buaty et al., 2023).

Manajemen risiko dalam konteks ini mencakup serangkaian proses mulai dari mengenali, menganalisis, hingga merespons berbagai potensi gangguan terhadap sistem e-banking syariah. Proses ini harus dilakukan secara sistematis dan menyeluruh, dengan menanamkan nilai-nilai seperti transparansi, keadilan, serta amanah dalam setiap langkahnya. Peran Dewan Pengawas Syariah (DPS) menjadi sangat penting untuk memastikan bahwa penggunaan teknologi informasi tidak melanggar prinsip-prinsip syariah yang berlaku (Mutafarida, 2017). Berdasarkan urgensi tersebut, artikel ini bertujuan untuk mengevaluasi penerapan manajemen risiko teknologi informasi dalam operasional e-banking syariah. Penelitian ini difokuskan pada cara-cara bank syariah dalam menghadapi tantangan digital dengan tetap menjaga kepatuhan terhadap ajaran Islam. Diharapkan, hasil pembahasan dapat memberikan kontribusi terhadap pengembangan sistem perbankan digital yang aman, berkelanjutan, dan selaras dengan nilai-nilai syariah.

Pembahasan

Untuk memahami bagaimana strategi manajemen risiko diterapkan dalam produk e-banking syariah, terlebih dahulu perlu ditelaah konsep dasar manajemen risiko dan peran teknologi informasi dalam mendukung operasional perbankan syariah. Pemahaman ini menjadi landasan untuk menganalisis lebih dalam strategi mitigasi risiko yang sesuai dengan prinsip-prinsip syariah serta tantangan yang dihadapi dalam implementasinya.

Manajemen Risiko

Manajemen risiko merupakan suatu pendekatan terstruktur yang digunakan untuk mengidentifikasi, menilai, memantau, dan mengendalikan potensi risiko yang dapat mengganggu pencapaian tujuan organisasi. Menurut Utami et al. (2022) manajemen risiko adalah proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko yang dilakukan secara sistematis dan berkesinambungan untuk meminimalisir potensi kerugian dan memastikan tercapainya tujuan organisasi secara efektif dan efisien. Dalam dunia perbankan, khususnya bank syariah, manajemen risiko menjadi aspek penting karena menyangkut keamanan dana masyarakat dan stabilitas sistem keuangan. Risiko tidak bisa dihindari sepenuhnya, namun dengan manajemen risiko yang baik, dampaknya dapat dikurangi. Proses manajemen risiko biasanya mencakup

beberapa tahapan, yaitu identifikasi risiko, analisis risiko, evaluasi risiko, penanganan atau mitigasi risiko, serta pemantauan berkelanjutan (Mutafarida, 2017).

Teknologi Informasi dalam Perbankan Syariah

Perkembangan teknologi informasi (TI) telah membawa perubahan besar dalam sistem kerja dan layanan di industri perbankan. TI menjadi fondasi utama dalam mendukung operasional perbankan modern, mulai dari sistem pencatatan transaksi, pengelolaan data nasabah, hingga pengembangan produk-produk digital yang berbasis aplikasi. Menurut Tahir et al., (2023) digitalisasi perbankan merupakan proses integrasi teknologi dalam semua aspek kegiatan bank, yang bertujuan untuk meningkatkan efisiensi, kenyamanan, serta keamanan dalam pelayanan kepada nasabah.

Namun, kemajuan teknologi juga diiringi dengan tantangan besar, terutama dari sisi keamanan informasi. Serangan siber seperti phishing, malware, hingga peretasan data menjadi ancaman serius bagi industri perbankan digital. Oleh karena itu, sistem keamanan seperti enkripsi data, otentikasi berlapis, serta sistem deteksi ancaman berbasis kecerdasan buatan (AI-based threat detection) menjadi komponen penting dalam menjaga kepercayaan nasabah dan stabilitas sistem keuangan. Menurut Al-Banna (2021) , penerapan manajemen risiko teknologi informasi yang baik serta investasi pada sistem keamanan siber dapat meningkatkan ketahanan digital bank dalam menghadapi risiko eksternal. Teknologi informasi bukan hanya alat bantu, tetapi telah menjadi tulang punggung transformasi industri perbankan ke arah yang lebih canggih, efisien, dan aman.

Konsep E-Banking Syariah

E-banking syariah adalah konsep perbankan berbasis teknologi informasi yang mengintegrasikan prinsip-prinsip syariah dalam pelaksanaan transaksi perbankan secara elektronik. Dalam e-banking syariah, teknologi informasi digunakan untuk mempermudah akses layanan perbankan dengan mematuhi hukum dan etika syariah, yang melarang transaksi yang mengandung unsur riba (bunga), gharar (ketidakpastian), dan maysir (perjudian). E-banking syariah merujuk pada penggunaan teknologi informasi dalam menyediakan layanan perbankan yang mematuhi prinsip-prinsip syariah Islam. Dalam hal ini, bank-bank syariah memanfaatkan platform elektronik seperti internet banking, mobile banking, dan ATM untuk memberikan layanan perbankan yang bebas dari unsur-unsur yang dilarang dalam Islam, seperti riba (bunga), gharar (ketidakpastian), dan maysir (perjudian). Konsep dasar dari e-banking syariah adalah penyediaan layanan yang tidak hanya efisien dan cepat, tetapi juga memenuhi kaidah hukum Islam yang mengatur hubungan keuangan. Menurut Kelvin et al., (2024) e-banking syariah bukan hanya soal transaksi keuangan, tetapi juga mencakup manajemen dan pengelolaan risiko yang sesuai dengan prinsip syariah, serta memastikan transparansi dalam setiap transaksi.

Manajemen Risiko TI dalam Konteks Syariah

Manajemen risiko teknologi informasi (TI) dalam konteks perbankan syariah merupakan proses pengelolaan risiko yang tidak hanya mempertimbangkan aspek teknis dan keamanan, namun juga kesesuaian terhadap prinsip-prinsip syariah. Menurut

Ariana (2016) pendekatan manajemen risiko TI dalam perbankan syariah harus berbasis pada nilai-nilai Islam seperti kejujuran, keadilan, transparansi, dan kehati-hatian. Dalam praktiknya, bank syariah harus dapat mengidentifikasi potensi risiko TI seperti serangan siber, gangguan sistem, hingga kebocoran data, dan menyusun strategi mitigasi yang tidak melanggar prinsip syariah.Bank syariah umumnya menerapkan manajemen risiko TI dengan struktur yang jelas dan melibatkan Dewan Pengawas Syariah (DPS). DPS memiliki peran penting dalam mengawasi kebijakan dan operasional yang berhubungan dengan TI agar sesuai dengan fatwa DSN-MUI. Sebagaimana dijelaskan oleh Tahir et al., (2023) sistem pengelolaan risiko TI pada bank syariah mencakup lima tahap utama: identifikasi risiko, analisis risiko, evaluasi risiko, mitigasi risiko, dan pemantauan berkelanjutan. Dalam konteks syariah, proses ini harus dilandasi dengan nilai tanggung jawab (amanah) dalam menjaga data dan aset nasabah.

Jenis Risiko E-Banking Syariah

- Risiko Operasional

  Risiko operasional dalam e-banking syariah mencakup potensi kerugian yang timbul akibat kegagalan sistem, kesalahan manusia, atau gangguan proses internal. Misalnya, gangguan pada server atau kesalahan dalam pemrosesan transaksi dapat menghambat layanan kepada nasabah dan merusak citra bank. Bank Syariah Indonesia (BSI) telah menghadapi tantangan semacam ini, terutama dalam hal sistem informasi dan teknologi yang digunakan (Faizal et al., 2023)
- Risiko Keamanan Informasi (Cybersecurity)

  Dengan meningkatnya penggunaan teknologi digital, e-banking syariah menghadapi risiko keamanan informasi yang signifikan, seperti serangan siber, malware, dan pencurian data nasabah. Ancaman ini dapat merusak sistem perbankan dan melanggar privasi nasabah . Oleh karena itu, bank syariah perlu mengimplementasikan sistem keamanan yang kuat dan melakukan pemantauan berkala untuk melindungi data nasabah.
- Risiko Kepatuhan Syariah

  Risiko kepatuhan syariah muncul ketika bank syariah tidak mematuhi prinsip-prinsip Islam dalam operasionalnya, termasuk dalam penggunaan teknologi. Misalnya, penggunaan sistem yang tidak sesuai dengan prinsip syariah dapat menimbulkan pelanggaran . Oleh karena itu, pengawasan dari Dewan Pengawas Syariah (DPS) sangat penting untuk memastikan bahwa seluruh proses digital tetap sesuai dengan hukum Islam.
- Risiko Reputasi

  Risiko reputasi terjadi ketika kepercayaan nasabah terhadap bank syariah menurun akibat kejadian negatif, seperti pemberitaan buruk di media massa atau pelanggaran etika bisnis. Hal ini dapat berdampak pada penurunan jumlah nasabah dan kerugian finansial . Bank syariah harus menjaga reputasinya dengan memastikan transparansi dan kepatuhan terhadap prinsip syariah dalam setiap aspek operasionalnya.
- Risiko Teknologi dan Infrastruktur

  Ketergantungan pada teknologi dan infrastruktur dalam e-banking syariah membawa risiko tersendiri, seperti kegagalan sistem atau kurangnya kesiapan

infrastruktur untuk menghadapi gangguan. Bank syariah perlu memiliki sistem pemulihan bencana (disaster recovery) dan pusat data yang andal untuk memastikan kontinuitas layanan (Anggitaningsih, 2024).

- Risiko Literasi Digital Nasabah

  Rendahnya tingkat literasi digital di kalangan nasabah dapat menjadi hambatan dalam adopsi e-banking syariah. Banyak nasabah masih mengandalkan layanan perbankan konvensional dan merasa ragu untuk menggunakan layanan digital . Oleh karena itu, bank syariah perlu melakukan edukasi dan peningkatan kesadaran digital secara berkelanjutan kepada nasabah.

Startegi Manajemen Risiko berbasis TI pada E-Banking Syariah

Strategi manajemen risiko berbasis teknologi informasi dalam e-banking syariah merupakan langkah penting untuk menjaga stabilitas operasional dan kepatuhan terhadap prinsip syariah. Salah satu pendekatan awal adalah menyelaraskan strategi teknologi informasi dengan visi dan misi bank syariah itu sendiri. Artinya, setiap kebijakan dan pengembangan teknologi harus mendukung tujuan bisnis yang halal dan sesuai syariat. Selanjutnya, penerapan tata kelola TI yang baik menjadi pondasi utama. Tata kelola ini meliputi penyusunan kebijakan risiko, batasan risiko, dan integrasi pengendalian internal yang sistematis serta berkelanjutan, sebagaimana diatur dalam pedoman OJK untuk bank syariah (OJK, 2016). Di sisi lain, keamanan informasi menjadi elemen vital dalam mitigasi risiko digital. Implementasi sistem keamanan seperti firewall, enkripsi, dan autentikasi ganda dapat membantu mencegah serangan siber yang berpotensi merugikan nasabah maupun reputasi bank. Selain itu, strategi ini perlu diperkuat dengan pengembangan kapasitas sumber daya manusia. Peningkatan kompetensi staf dalam bidang teknologi serta pemahaman terhadap hukum syariah akan memastikan bahwa pengelolaan risiko berjalan secara profesional dan sesuai nilai Islam (Ningsih & Ismaini, 2025).

Aspek lain yang tidak kalah penting adalah kerja sama dengan pihak ketiga. Bank syariah yang menggunakan jasa penyedia teknologi luar harus memastikan bahwa pihak tersebut memiliki standar keamanan dan manajemen risiko yang sejalan dengan ketentuan yang berlaku. Pengawasan terhadap operasional pihak ketiga sangat diperlukan untuk menghindari celah kerentanan (Hikam et al., 2025). Terakhir, proses evaluasi dan pemantauan secara berkala menjadi kunci agar strategi manajemen risiko tetap relevan. Audit internal, pemantauan sistem berkelanjutan, serta penerapan tindakan korektif terhadap temuan risiko akan membantu menciptakan sistem yang tangguh dan adaptif di era digital (Sari & Khudri, 2024).

Implementasi Bank Syariah terhadap Manajemen Risiko Berbasis Teknologi Informasi pada Produk E-Banking Syariah

Perkembangan teknologi digital menuntut bank syariah untuk menghadirkan layanan yang cepat, efisien, dan tetap sesuai dengan prinsip syariah. E-banking syariah menjadi solusi yang diandalkan, tetapi dalam pelaksanaannya mengandung berbagai risiko, seperti keamanan siber, privasi data nasabah, dan kepatuhan terhadap hukum

Islam (Rachmawati et al., 2025). Oleh karena itu, manajemen risiko teknologi informasi menjadi elemen penting dalam implementasi e-banking syariah. Bank Syariah Indonesia (BSI) dan institusi sejenis perlu mengidentifikasi ancaman yang mungkin timbul dari digitalisasi, seperti peretasan sistem, serangan malware, atau penyalahgunaan data, serta menyusun langkah mitigasi yang tepat. Manajemen risiko tidak hanya mencakup aspek teknis, tetapi juga harus mempertimbangkan nilai-nilai syariah seperti kejujuran (shidq), tanggung jawab (amanah), dan keadilan (adl). Proses ini mencerminkan komitmen bank syariah dalam menjaga integritas serta kepercayaan nasabah terhadap layanan digital yang ditawarkan. Selain itu, evaluasi berkala dan pengawasan oleh Dewan Pengawas Syariah (DPS) menjadi bagian penting dalam menjamin bahwa sistem informasi tidak keluar dari rambu syariat (Lubis et al., 2025).

Strategi manajemen risiko teknologi informasi di bank syariah mencakup penggunaan sistem keamanan mutakhir yang sesuai dengan prinsip Islam. Penerapan teknologi seperti enkripsi data, otentikasi multi-faktor, firewall, dan sistem deteksi intrusi telah menjadi keharusan untuk mengantisipasi berbagai ancaman digital (Shobah et al., 2024) . Tidak hanya sistemnya, tetapi kesiapan sumber daya manusia juga sangat vital—pegawai bank harus dibekali pelatihan dalam hal keamanan TI dan prinsip-prinsip syariah. Selain itu, bank juga harus menyusun kebijakan tata kelola TI yang selaras dengan tujuan syariah, mulai dari perencanaan, pelaksanaan, hingga pengawasan. Kolaborasi dengan penyedia teknologi eksternal pun wajib diawasi secara ketat untuk memastikan mereka tidak membawa sistem atau prosedur yang bertentangan dengan syariat Islam. Dengan manajemen risiko yang terintegrasi seperti ini, bank syariah dapat meminimalisir potensi kerugian dan menjaga reputasinya di tengah kompetisi layanan digital yang semakin ketat (Faizal et al., 2023).

Penerapan manajemen risiko berbasis TI tidak akan optimal tanpa keterlibatan aktif dari nasabah. Banyak risiko justru muncul akibat rendahnya literasi digital dan minimnya kesadaran akan keamanan data dari sisi pengguna. Oleh karena itu, bank syariah perlu mengedukasi nasabah tentang penggunaan layanan e-banking secara aman, seperti tidak membagikan OTP atau PIN kepada pihak lain, serta mengenali tanda-tanda phishing. Edukasi ini penting terutama untuk kalangan muda seperti mahasiswa, yang menjadi pengguna aktif layanan digital namun seringkali kurang memperhatikan aspek keamanan. Peningkatan literasi ini sejalan dengan prinsip ta'lim (pendidikan) dalam Islam. Dengan begitu, tercipta hubungan yang sinergis antara sistem yang aman, petugas yang kompeten, dan nasabah yang sadar risiko. Kombinasi ini memperkuat keberlangsungan e-banking syariah yang andal dan tetap sesuai syariah di era teknologi informasi (Subagyo, 2023).

Kesimpulan dan Saran

Penerapan manajemen risiko berbasis teknologi informasi pada layanan e-banking syariah merupakan upaya strategis yang tidak hanya berorientasi pada penguatan sistem keamanan digital, tetapi juga menekankan kepatuhan terhadap prinsip-prinsip syariah. Manajemen risiko TI mencakup beberapa aspek penting, mulai dari tata kelola sistem yang sesuai dengan nilai-nilai Islam, penggunaan teknologi keamanan mutakhir,

hingga peningkatan kapasitas SDM dan edukasi kepada nasabah. Selain itu, pengawasan internal, termasuk peran aktif Dewan Pengawas Syariah (DPS), menjadi penentu dalam menjamin bahwa seluruh aktivitas digital tetap berada dalam koridor hukum Islam. Dengan pendekatan yang terintegrasi dan responsif terhadap dinamika digital, bank syariah mampu menciptakan sistem layanan e-banking yang aman, terpercaya, dan sesuai dengan tuntunan syariah.

Selain itu, Bank syariah perlu secara konsisten memperkuat sistem manajemen risiko TI melalui peningkatan infrastruktur digital yang adaptif dan aman, serta memperhatikan aspek syariah dalam setiap pengembangan teknologi. Diperlukan kolaborasi yang erat antara tim TI, manajemen risiko, dan Dewan Pengawas Syariah agar proses mitigasi risiko berjalan efektif dan tetap sesuai prinsip Islam. Selain itu, literasi digital nasabah harus menjadi perhatian utama melalui program edukasi berkelanjutan, agar mereka lebih waspada terhadap potensi risiko siber dan mampu menggunakan layanan e-banking secara bijak. Evaluasi berkala serta pembaruan terhadap kebijakan dan sistem keamanan juga harus menjadi agenda rutin demi memastikan layanan digital syariah tetap tangguh di tengah ancaman teknologi yang terus berkembang.

Daftar Pustaka

Al-Banna, H. (2021). *Dasar-Dasar Manajemen Risiko Bank Syariah. Program Studi Perbankan Syariah, Fakultas Ekonomi dan Bisnis Islam, UIN Sunan Kalijaga.* Program Studi Perbankan Syariah, Fakultas Ekonomi dan Bisnis Islam, UIN Sunan Kalijaga. http://digilib.uin-suka.ac.id/id/eprint/57002/

Anggitaningsih, R. (2024). Manajemen Risiko Operasional Pada Bank Syari'ah Indonesia di Jawa Timur. *Multidisciplinary Journal of Education , Economic and Culture*, *2*(2), 879–891. https://doi.org/10.61231/mjeec.v2i2.255

Ariana, R. (2016). *Bank Syariah*. *1*, 1–23.

Buaty, N., Dewi, S. C., Dutasmara, R., & Broto, M. (2023). Manajemen Resiko Teknologi Informasi Pada Industri Perbankan Dengan Iso 31000 : 2018 Framework. *Prosiding Seminar …*, 31–39. https://journal.perbanas.id/index.php/psn/article/view/584%0Ahttps://journal.perbanas.id/index.php/psn/article/download/584/321

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*(2), 87–100. https://doi.org/10.47435/asy-syarikah.v5i2.2022

Hikam, M., Siswanto, & Djalaluddin, A. (2025). *INTEGRATING DIGITAL SERVICES IN ISLAMIC SOCIAL FINANCE : A SERVICE-DOMINANT FRAMEWORK*. *14*(1).

Kelvin, K., Judijanto, L., Rumawak, I., Amadea, I., & ... (2024). *Teknologi Informasi: Teori dan Implementasi Penerapan Teknologi Informasi di Berbagai Bidang* (Issue March). https://books.google.com/books?hl=en&lr=&id=cGkcEQAAQBAJ&oi=fnd&pg=PP3&dq=implementasi+teknologi+informasi&ots=BC5Xo5KKxv&sig=RuFYzXpC1NKpoEVx55SDd3bChus

Lubis, A. M., Jelita, G., Okta, S., & Wirya, V. (2025). *Tantangan dan Keamanan Teknologi Informasi pada Manajemen Bank Syariah*. *1*.

Mutafarida, B. (2017). Macam-Macam Risiko Dalam Bank Syariah. *Wadiah*, *1*(2), 25–40. https://doi.org/10.30762/wadiah.v1i2.1280

Ningsih, A. S., & Ismaini, D. (2025). *Keamanan data nasabah bank syariah*. *2*(1), 651–662.

Otoritas Jasa Keuangan (OJK). (2016). Indonesia Financial Service Authority Regulation 38/POJK.03/2016 Risk Management for IT purposes. *Peraturan OJK*, 61. https://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK MRTI.pdf

Rachmawati, E., Kinasih, L. S., Rahmadani, N., Griana, T. P., Muti'ah, R., Suharti, Azis, D. P. A., & Eni, E. (2025). *Protective effect of fermented vegetable compounds against nonalcoholic fatty liver disease using metabolite profiling , integrated network pharmacology , and molecular docking approach*. https://doi.org/10.4103/JAPTR.JAPTR

Sari, A. M., & Khudri, T. M. Y. (2024). Evaluasi Peran Audit Internal Dalam Manajemen Risiko Reputasi. *Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA)*, *8*(1), 518–527. https://doi.org/10.31955/mea.v8i1.3694

Shobah, W. N., Saputri, A. B., & Fauziyah, N. (2024). *The Influence of Using Mobile Learning " Wordwall " on the Critical Thinking Ability of Social Sciences Education Students at UIN Malang in the World History Course*. *2024*(Majid 2016), 497–501.

Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah: Identifikasi Ancaman dan Tantangan Terkini. *Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*, 2. https://doi.org/https://doi.org/10.47435/asy-syarikah.v5i2.2022

Tahir, R., Harto, B., Rukmana, A. Y., Subekti, R., Waty, E., Situru, A. C., & Sepriano. (2023). Transformasi Bisnis di Era Digital (Teknologi Informasi dalam Mendukung Transformasi Bisnis di Era Digital). In *Sonpedia Publishing* (Issue August).

Utami, L. C., Aqil, M., & Chairina, C. (2022). Studi Literatur Penerapan Manajemen Risiko Pada Bank Syariah. *Jurnal Ekonomika Dan Bisnis (JEBS)*, *2*(3), 742–747. https://doi.org/10.47233/jebs.v2i3.262