Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 2, Issue 2, 2024 pp. 1184-1192 http://urj.uin-malang.ac.id/index.php/mij/index

Manajemen risiko dalam keamanan informasi dan perlindungan data

Valentyno Damya
Program Studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang
e-mail: valentyno.damya@gmail.com

Kata Kunci:
cybersecurity; kepatuhan; kebocoran data; ancaman siber; penilaian risiko

Keywords:
cybersecurity; obedience; data leakage; cyber threats; risk assessment

A B S T R A K

Dalam era digital yang terus berkembang, keamanan informasi dan perlindungan data menjadi krusial bagi perusahaan di seluruh dunia. Artikel ini membahas pentingnya kesadaran cybersecurity dalam konteks manajemen risiko perusahaan, menyoroti berbagai jenis ancaman dan tantangan yang dihadapi dalam mengelola risiko keamanan informasi. Melalui tinjauan literatur, penelitian ini menemukan bahwa perusahaan-perusahaan di Indonesia dan luar negeri memiliki tingkat kesadaran yang bervariasi terhadap ancaman cybersecurity. Regulasi yang ketat, investasi dalam teknologi keamanan, dan budaya organisasi yang memperhatikan privasi dan keamanan data menjadi faktor kunci dalam meningkatkan kesadaran tersebut. Namun, tantangan tetap ada, terutama dalam menghadapi ancaman yang semakin berkembang dan kompleks. Diperlukan upaya kolaboratif antara pemerintah, industri, dan lembaga terkait untuk meningkatkan kesadaran cybersecurity melalui edukasi, pelatihan, dan adopsi praktik terbaik dalam manajemen risiko cybersecurity. Hanya dengan langkah-langkah preventif yang tepat dan pendekatan proaktif, perusahaan dapat lebih siap menghadapi ancaman cyber dan melindungi keamanan informasi mereka secara efektif.

A B S T R A C T

In the rapidly evolving digital era, information security and data protection are crucial for companies worldwide. This article discusses the importance of cybersecurity awareness in the context of corporate risk management, highlighting various types of threats and challenges faced in managing information security risks.Through literature review, this research finds that companies in Indonesia and abroad exhibit varying levels of awareness regarding cybersecurity threats. Stringent regulations, investments in security technologies, and organizational cultures emphasizing privacy and data security are key factors in enhancing this awareness. However, challenges persist, particularly in addressing increasingly sophisticated and complex threats.Collaborative efforts between governments, industries, and relevant institutions are necessary to enhance cybersecurity awareness through education, training, and adoption of best practices in cybersecurity risk management. Only with the right preventive measures and a proactive approach can companies be better prepared to face cyber threats and effectively safeguard their information security.

Pendahuluan

Perkembangan teknologi informasi membawa dampak besar bagi kehidupan. Saat ini penggunaan internet terus mengalami peningkatan namun, masih banyak yang belum paham akan perlindungan data termasuk perusahaan kelas menengah kebawah. Lebih dari 30% pengguna internet belum sadar akan hal itu. Perlunya penjagaan data pribadi maupun perusahaan agar aman dari serangan dan retasan. (Hidayat et al., 2023)

Keamanan suatu hal yang penting dalam system informasi dan menjadi pusat manajemen resiko bagi perusahaan. Pentingnya penjagaan agar tidak disalah gunakan. Dengan perkembangan digital yang begitu pesat perlunya penanganan yang berlaka juga. Ada beberapa keamanan informasi bagi perusahaan yang diantaranya seperti keamanan fisik, keamanan pribadi, keamanan operasional, keamanan komunikasi dan keamanan jaringan. Hal ini perlu diperhatikan bagi perusahaan agar dapat mengatasi dari ancaman direncanakan dan ancaman yang tidak terencana. (Nasher, 2020)

Dalam konteks keamanan informasi dan perlindungan data, organisasi menghadapi berbagai jenis risiko yang dapat mengancam integritas dan kerahasiaan informasi perusahaan. Ancaman meliputi kebocoran data yang disebabkan oleh pelanggaran keamanan, serangan malware yang dapat merusahan atau mencuri informasi penting, serta pencurian identitas yang dapat menimbulkan kerugian finansial dan reputasi organisasi. Dengan meningkatnya interkoneksi digital dan penggunaan teknologi informasi, risiko ini akan semakin kompleks dan membutuhkan perhatian yang lebih besar dari organisasi untuk menerapkan langkah perlindungan yang lebih efektif.

pengelolaan risiko keamanan informasi, organisasi dihadapkan pada sejumlah tantangan yang kompleks. Evolusi teknologi yang cepat menciptakan celah baru yang dapat dieksploitasi oleh penyerang, sementara ketidakpastian dalam regulasi mengharuskan organisasi untuk tetap up-to-date dengan persyaratan yang berubah secara teratur. Ancaman yang terus berkembang, seperti serangan siber yang semakin canggih dan seringkali sulit dideteksi, juga menambah tingkat kompleksitas dalam pengelolaan risiko keamanan informasi. Pada saat yang sama, organisasi dihadapkan pada tantangan untuk mengintegrasikan pendekatan yang holistik dalam manajemen risiko, menggabungkan aspek teknis, proses, dan kebijakan yang berlaku.(Makbull Rizki, 2022).

Manajemen risiko adalah bidang penting untuk mengurangi risiko dan membuat keputusan yang efektif dan mengkomunikasikan hasilnya secara proaktif dalam organisasi untuk menemukan masalah manajerial dan teknis yang mungkin terjadi dapat dilakukan untuk mengurangi kemungkinan dan konsekuensi masalah tersebut (Ihyak et al., 2023; Qulyubi et al., 2023; Syadali et al., 2023). Organisasi memerlukan sistem manajemen risiko keamanan siber yang komprehensif untuk menangani ancaman keamanan siber yang meningkat. Sistem ini harus dapat mengidentifikasi ancaman keamanan siber pada komponen fisik yang dapat terjadi. Oleh karena itu, penelitian ini membahas potensi peristiwa ancaman yang dapat mengakibatkan kerugian atau dampak negatif terhadap bisnis. Misalnya, serangan phishing dapat

terjadi pada perangkat perusahaan yang terhubung, seperti laptop atau ponsel pintar perusahaan, dan malware mengganggu proses bisnis organisasi.(Nurain et al., 2024)

Pendekatan proaktif dalam manajemen risiko keamanan informasi menjadi semakin penting dalam menghadapi ancaman cyber yang terus berkembang (Fatah et al., 2023; Wafie & Segaf, 2023). Organisasi perlu tidak hanya bersifat responsif terhadap insiden yang terjadi, tetapi juga proaktif dalam mengidentifikasi potensi risiko dan mengambil langkah-langkah pencegahan yang sesuai . Dengan adopsi pendekatan proaktif, organisasi dapat lebih efektif mengurangi kemungkinan terjadinya pelanggaran keamanan dan dampak negatif yang mungkin timbul. Hal ini termasuk dalam pengembangan kebijakan keamanan yang ketat, pelaksanaan kontrol akses yang tepat, dan peningkatan kesadaran keamanan di antara semua anggota organisasi. Dengan demikian, pendekatan proaktif ini memungkinkan organisasi untuk lebih siap menghadapi ancaman cyber dan melindungi keamanan informasi mereka secara lebih efektif.

Tinjauan Pustaka

Manajemen Risiko Cybersecurity

Pada perkembangan teknologi, keamanan sangat penting dan menjadi konsentrasi atau focus utama diri penyedia layanan. Hal ini dipengaruhi karena setiap layanan menyimpan informasi yang bersifat rahasia. Informasi dapat berupa data diri. Hal ini harus dijaga oleh penyedia layanan agar tidak ada penyalahguna oleh pihak yang tidak bertanggung jawab (Tan & Soewito, 2022).

NIST *Cybersecurity Framework* adalah kerangka kerja untuk melindungi Organisasi atau instansi terhadap ancaman dari siber. NIST menyediakan bahasa yang umum untuk memahami, mengelola, serta mengungkapkan risiko keamanan siber baik kepada pemangku kepentingan atau *stockholder* internal maupun eksternal (Putri et al., 2022).

Tantangan dan ancaman terkini

Penguatan manajemen risiko perlu di pertimbangkan sebagai keamanan dari ancaman yang akan datang pada organisasi. Keamanan perlu dilakukan berlapis dengan berbagai cara. Memperhatikan aspek ini sangat penting untuk menjaga data dan reputasi organisasi atau perusahaan tetap aman. Hal ini untuk mencegah ancaman yang datang secara tiba-tiba ataupun yang sudah di antisipasi oleh perusahaan. Melakukan beberapa back up data perusahaan juga perlu dilakukan untuk kemanan dari perusahaan (Kurniawan & Solihin, 2022).

Penerapan teknologi

Penerapan teknologi harus dilakukan perusahaan sebagai usaha menjaga kemanan data yang dimiliki. Beberapa hal yang bisa dilakukan oleh perusahaan atau organisasi dengan memahami AI dan *Cybersecurity*. Hal ini dapat mengurangi ancaman yang akan datang pada perusahaan. Pemahaman seperti ini juga harus ada peningkatan setiap saat agar dapat mengantisipasi kecanggihan teknologi dalam peretasan pada perusahaan (Viyanto et al., 2013).

Kebijakan dan kepatuhan

Permen No.82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik berbicara tentang standar sistem manajemen keamanan informasi dan mengharuskan lembaga penyelenggaraan publik untuk menetapkan tata kelola keamanan informasi yang andal dan aman, serta tanggung jawab yang sesuai dengan permen tersebut. Tatakelola teknologi informasi adalah upaya untuk memastikan bahwa manajemen teknologi informasi mendukung atau selaras dengan strategi bisnis yang dilakukan oleh pemimpin instansi (Sundari & Wella, 2021).

Kesadaran Pengguna

Kesadaran yang dimiliki oleh Perusahaan pada dewasa ini sudah sangat pesat. Beberapa perusahaan besar sudah melakukan pengamanan bisnis mereka dengan kemanan berlapis dan salah satunya sektor perbankan (Wafie & Segaf, 2023). Dari hal ini kita dapat ambil kesimpulan kuatnya kemanan yang dilakukan setiap perusahaan berdampak baik dan dapat menjaga reputasi perusahaan (Ramadhani & Pratama, 2020).

Pembahasan

Metode analisis risiko fmea dan FTA

FMEA (Failure Mode and Effect Analysis)

FMEA adalah teknik rekayasa yang digunakan untuk menemukan, mengidentifikasi, dan menghilangkan kesalahan, masalah, error, dan jenisnya dari sistem, desain, proses, atau jasa sebelum mencapai konsumen. Definisi FMEA di atas lebih mengacu pada kualitas. Dalam konteks kesehatan dan keselamatan kerja (K3), kegagalan yang dimaksudakan dalam definisi di atas adalah suatu bahaya dalam suatu proses (Hanif et al., 2015). FMEA dikelompokkan berdasarkan dampak yang diberikan terhadap kesuksesan suatu misi sistem. Secara umum, FMEA didefinisikan sebagai sebuah teknik yang mengidentifikasi tiga hal: 1. Penyebab kegagalan yang mungkin terjadi pada sistem, desain, produk, dan proses selama siklus hidupnya; 2. Efek dari kegagalan tersebut; dan 3. Tingkat kekritisan dampak kegagalan terhadap fungsi sistem, desain, produk, dan proses.

FTA (Fault Tree Analysis)

Metode ini adalah suatu teknik yang digunakan untuk mengidentifikasi resiko yang berperan untuk mengidentifikasi risiko yang menyebabkan suatu kegagalan. Metode ini dilakukan dengan pendekatan yang bersifat top down yang berawal kegagalan dari kejadian puncak dan merinci sebab suatu top event sampai pada suatu kegagalan dasar (Hanif et al., 2015). Dalam analisis gerbang kegagalan (FTA), gerbang logika terdiri dari gerbang AND dan OR. Sebuah gerbang logika menunjukkan keadaan komponen sistem (keadaan dasar), dan hubungan antara keadaan dasar dan keadaan atas menunjukkan keterhubungan dalam gerbang logika. Langkah-langkah FTA adalah sebagai berikut

1. Identifikasi Event Top Level: Pada tahap ini, jenis kerusakan (undesired event) yang terjadi diidentifikasi untuk mengidentifikasi kesalahan sistem. Mempelajari semua informasi tentang sistem memungkinkan Anda memahaminya.
2. Membuat Diagram Pohon Kesalahan: Diagram pohon kesalahan menunjukkan bagaimana peristiwa jaringan tingkat tinggi dapat muncul.
3. Menganalisa Pohon Kesalahan: Analisa pohon kesalahan digunakan untuk mendapatkan data yang jelas dari suatu sistem dan perbaikan yang digunakan.

Tantangan dalam Mengelola Risiko Cybersecurity

Dalam era pesatnya teknologi, keamanan data menjadi suatu keharusan yang tak terelakkan. Hal ini karena kompleksitas ancaman cybersecurity semakin meningkat seiring dengan kemajuan teknologi. Oleh karena itu, penting untuk memahami berbagai jenis ancaman yang ada guna melindungi data pribadi dan korporat. Di bawah ini, disajikan penjelasan yang lebih detail mengenai tujuh jenis ancaman cybersecurity yang harus diwaspadai

Ransomware

Jenis malware yang mengenkripsi file korban dan meminta tebusan dalam bentuk cryptocurrency sebagai syarat untuk mendapatkan kembali akses ke data tersebut. Penyebarannya biasanya melalui lampiran email, iklan berbahaya, atau jaringan yang telah terinfeksi (Person, 2014).

Malware

Perangkat lunak berbahaya yang mencakup berbagai bentuk seperti virus, worm, dan trojan. Virus merusak atau mengubah data tanpa izin, sementara worm menyebar melalui jaringan dan trojan menyamar sebagai perangkat lunak yang sah namun melakukan aktivitas berbahaya di latar belakang.

Phishing

Metode penipuan yang menggunakan email atau pesan palsu untuk mengelabui korban dan mendapatkan informasi pribadi seperti kata sandi atau nomor kartu kredit. Pelaku sering kali meniru lembaga keuangan atau layanan online untuk menimbulkan rasa percaya pada korban.

Spoofing

Tindakan menyamar sebagai entitas lain untuk memperoleh kepercayaan korban. Ini bisa dilakukan melalui pembuatan alamat email atau situs web palsu yang menyerupai yang asli, atau bahkan dengan mengirimkan paket data palsu dalam jaringan.

Social Engineering

Teknik manipulasi interaksi manusia untuk mendapatkan informasi sensitif seperti kata sandi atau akses ke sistem. Penipuan dilakukan dengan membangun kepercayaan pada korban, yang akhirnya mau memberikan informasi atau akses yang tidak semestinya.

Pencurian Data

Ancaman yang melibatkan akses ilegal dan pengambilan data pribadi atau korporat seperti informasi keuangan, data pelanggan, atau rahasia perdagangan. Serangan dapat terjadi melalui serangan siber, pencurian fisik perangkat, atau kebocoran dari sumber internal.

Man in the Middle

Ancaman yang terjadi ketika penyerang menyusup ke dalam komunikasi antara dua pihak, memungkinkan mereka untuk menyadap atau mencuri data yang ditransmisikan. Ini sering terjadi dalam jaringan yang tidak aman seperti WiFi publik.

Dari penjelasan di atas, terlihat jelas bahwa ancaman cybersecurity merupakan ancaman serius yang dapat membahayakan kelangsungan bisnis dan keamanan data. Untuk melindungi diri dari ancaman-ancaman ini, diperlukan langkah-langkah preventif seperti meningkatkan kesadaran cybersecurity, melakukan pembaruan sistem secara rutin, menggunakan perangkat lunak keamanan yang tepat, serta rutin melakukan backup data.

Implikasi Hukum dan Kepatuhan

Penyusunan naskah akademik RUU tentang Perlindungan Data Pribadi ini mengadopsi metode penelitian hukum yuridis normatif. Langkah-langkahnya melibatkan studi kepustakaan yang terutama menelaah data sekunder, seperti bahan hukum primer (termasuk Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan yang telah diubah dengan Undang-Undang Nomor 24 Tahun 2013, Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik) serta perjanjian internasional yang telah disahkan dan berbagai peraturan perundang-undangan terkait lainnya (Kemenkumham, 2022).

Peran Kesadaran Pengguna

Tingkat kesadaran cybersecurity di perusahaan-perusahaan di Indonesia dan luar negeri menunjukkan variasi yang signifikan. Di Indonesia, masih terdapat tantangan dalam meningkatkan kesadaran secara menyeluruh terhadap ancaman cybersecurity. Meskipun beberapa perusahaan telah menunjukkan pemahaman yang baik dan menerapkan praktik terbaik dalam manajemen risiko, namun ada yang masih perlu meningkatkan pemahaman mereka.

Di sisi lain, di negara-negara seperti Amerika Serikat, Eropa, atau Jepang, perusahaan-perusahaan cenderung memiliki tingkat kesadaran cybersecurity yang lebih tinggi secara keseluruhan. Regulasi yang lebih ketat, investasi besar dalam teknologi keamanan, dan budaya yang memperhatikan privasi dan keamanan data menjadi faktor utama dalam peningkatan kesadaran ini.

Namun, perlu dicatat bahwa kesadaran cybersecurity tidak merata di semua perusahaan, baik di Indonesia maupun di luar negeri. Variasi ini dipengaruhi oleh

berbagai faktor seperti industri, ukuran, dan budaya organisasi masing-masing perusahaan.

Meningkatkan kesadaran cybersecurity tetap menjadi prioritas penting bagi perusahaan di seluruh dunia. Hal ini membutuhkan upaya kolaboratif antara pemerintah, industri, dan lembaga terkait untuk memberikan edukasi, pelatihan, dan mendorong adopsi praktik terbaik dalam manajemen risiko cybersecurity.

Kesimpulan Dan Saran

Pada perkembangan teknologi informasi yang semakin pesat, kesadaran akan pentingnya perlindungan data menjadi sangat penting, terutama bagi perusahaan kelas menengah ke bawah. Sayangnya, masih ada lebih dari 30% pengguna internet yang belum menyadari akan pentingnya hal ini. Keamanan data menjadi fokus utama dalam manajemen risiko perusahaan, mengingat kompleksitas ancaman yang semakin berkembang seiring dengan kemajuan digital. Perlindungan data perusahaan meliputi berbagai aspek seperti keamanan fisik, pribadi, operasional, komunikasi, dan jaringan, yang perlu dihadapi dengan langkah-langkah preventif yang tepat.

Ancaman cybersecurity seperti ransomware, malware, phishing, spoofing, social engineering, pencurian data, dan man in the middle, merupakan tantangan serius bagi keamanan data perusahaan. Untuk menghadapi ancaman tersebut, diperlukan pendekatan proaktif dalam manajemen risiko keamanan informasi, yang melibatkan adopsi kebijakan keamanan yang ketat, implementasi kontrol akses yang tepat, dan peningkatan kesadaran keamanan di seluruh organisasi.

Tingkat kesadaran cybersecurity di perusahaan-perusahaan di Indonesia dan luar negeri bervariasi, dengan beberapa perusahaan menunjukkan pemahaman yang baik sementara yang lain masih perlu meningkatkan pemahaman mereka. Regulasi yang ketat, investasi dalam teknologi keamanan, dan budaya yang memperhatikan privasi dan keamanan data menjadi faktor kunci dalam peningkatan kesadaran cybersecurity di beberapa negara.

Untuk meningkatkan kesadaran cybersecurity, diperlukan upaya kolaboratif antara pemerintah, industri, dan lembaga terkait untuk memberikan edukasi, pelatihan, dan mendorong adopsi praktik terbaik dalam manajemen risiko cybersecurity. Dengan demikian, perusahaan dapat lebih siap menghadapi ancaman cyber dan melindungi keamanan informasi mereka secara lebih efektif.

Daftar Pustaka

Fatah, M. I., Asnawi, N., Segaf, S., & Parmujianto, P. (2023). Case study at KSPPS BMT UGT nusantara Indonesia an analysis of using mobile applications to increase fee-based income. *Enrichment: Journal of Management*, *13*(2), 1182–1191. http://repository.uin-malang.ac.id/16777/

Hanif, R., Rukmi, S. H., & Susanty, S. (2015). Perbaikan Kualitas Produk Keraton Luxury DI PT. X dengan Menggunakan Metode Failure Mode and Effect Analysis (FMEA) dan

Fault Tree Analysis (FTA). *Jurnal Online Institut Teknologi Nasional*, *Vol. 03*(No. 03), 137–147.

Hidayat, A., Samudra, Y., & Andriyanto, L. P. (2023). Sosialisasi Pengenalan Pentingnya Cyber SecurityBagi Siswa Untuk Membangun Keamanan Informasi Dalam Era Digital. *Jurnal Pengabdian Masyarakat*, *2*(5), 450–457.

Ihyak, M., Segaf, S., & Suprayitno, E. (2023). Risk management in Islamic financial institutions (literature review). *Enrichment: Journal of Management*, *13*(2), 1560–1567. http://repository.uin-malang.ac.id/16775/

Kemenkumham. (2022). Naskah Akademik RUU Perlindungan Data Pribadi. *Kementerian Hukum Dan Hak Asasi Manusia*, 121.

Kurniawan, F. A., & Solihin, K. (2022). Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman Cyber Security. *JIOSE: Journal of Indonesian Sharia Economics*, *1*(1), 1–20. https://doi.org/10.35878/jiose.v1i1.360

Makbull Rizki. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Nasher, F. (2020). Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang/Jasa Secara Elektronik (Lpse) Di Dinas Komunikasi Dan Informatika Kabupaten Cianjur Dengan Menggunakan Sni Iso/Iec 27001:2013. *Media Jurnal Informatika*, *10*(1), 1–16. https://doi.org/10.35194/mji.v10i1.465

Nurain, A., Gultom, R. A. G., & Indrajit, R. E. (2024). Manajemen Ketahanan Risiko Siber pada Internet of Things dan Cyber Physical System. *Journal on Education*, *06*(02), 13271–13281.

Person. (2014). Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (Mcda). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika*, *5*(1), 122371.

Putri, T. S., Mutiah, N., & Prawira, D. (2022). Analisis Manajemen Risiko Keamanan Informasi Menggunakan Nist Cybersecurity Framework dan ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat). *Coding : Jurnal Komputer Dan Aplikasi*, *10*(2), 237–248.

Qulyubi, A., Suprayitno, E., Asnawi, N., & Segaf, S. (2023). Effect of company size ownership concentration auditor reputation board of commissioners and risk management committee on disclosure of enterprise risk management. *Enrichment: Journal of Management*, *13*(3), 1851–1860. http://repository.uin-malang.ac.id/16779/

Ramadhani, M. R., & Pratama, A. R. (2020). Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia. *Journal.Uii.Ac.Id*, *1*(2), 1–8.

Syadali, M. R., Segaf, S., & Parmujianto, P. (2023). Risk management strategy for the problem of borrowing money for Islamic commercial banks. *Enrichment: Journal of Management*, *13*(2), 1227–1236. http://repository.uin-malang.ac.id/16771/

Tan, T., & Soewito, B. (2022). *Menggunakan Framework Nist Cybersecurity Di Universitas Zxc*. *6*(2), 411–422. https://doi.org/10.52362/jisamar.v6i2.781

Viyanto, A. R., Latuihamallo, O. S., Tua, F. M., & Gui, A. (2013). *Studi Kasus Pada Perusahaan Jasa*. *4*, 43–54.

Wafie, S., & Segaf, S. (2023). Pemanfaatan Informasi Dan Teknologi Dalam Implementasi Manajemen Pengendalian Risiko Likuiditas Di Bmt Ugt Nusantara. *Jurnal Ilmiah Ekonomi Islam*, 9(3).