**Economic and Business Management International Journal**
**Mei 2024 | Vol. 6 | No. 2**
**E-ISSN : 2715-3681**
**DOI: 10.556442**

# Penggunaan Token Bank Sebagai Peningkatan Keamanan Transaksi Perbankan di PT Petrokimia Gresik

**[1]Parwanti Nuryoko Putri, [2]Fajar Syaiful Akbar**
[1,2]Universitas Pembangunan Nasional "Veteran" Jawa Timur, Jl. Rungkut Madya No. 1, Gn. Anyar, Kec. Gn. Anyar, Surabaya, Jawa Timur 60294
Email : [1]21013010323@student.upnjatim.ac.id, [2]fajarsyaiful@staff.upnjatim.ac.id

**Abstrak**

Artikel ini membahas penggunaan token bank sebagai upaya peningkatan keamanan transaksi perbankan di PT Petrokimia Gresik. PT Petrokimia Gresik adalah produsen pupuk terbesar di Indonesia yang terlibat dalam berbagai transaksi finansial. Dengan perkembangan teknologi, internet banking menjadi solusi yang mempermudah transaksi, namun juga menimbulkan risiko keamanan seperti peretasan dan pencurian identitas. Oleh karena itu, manajemen risiko yang efektif menjadi penting untuk melindungi transaksi finansial perusahaan. Token bank merupakan teknologi keamanan yang menghasilkan kode dinamis untuk setiap transaksi, sehingga memperkuat perlindungan terhadap akses tidak sah dan penipuan. Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk mengevaluasi efektivitas penggunaan token bank di PT Petrokimia Gresik, melalui observasi langsung dan kajian pustaka. Hasil penelitian menunjukkan bahwa penggunaan token bank dapat meningkatkan keamanan transaksi perbankan, mengurangi risiko fraud, dan memberikan rasa aman bagi pengguna. Meskipun demikian, tantangan seperti kesulitan penggunaan dan risiko kehilangan perangkat token masih ada. Untuk mengatasi ini, perusahaan dapat membuat prosedur tertulis dan menyediakan prosedur cadangan untuk token yang hilang atau rusak. Penelitian ini menyimpulkan bahwa penggunaan token bank di PT Petrokimia Gresik efektif dalam meningkatkan keamanan transaksi perbankan dan merupakan bagian penting dari manajemen risiko perusahaan.
**Kata Kunci :** Internet banking, Manajemen Risiko, Teknologi Keamanan, Token Bank

***Abstract***

*This article discusses the use of bank tokens to increase the security of banking transactions at PT Petrokimia Gresik, Indonesia's largest fertilizer producer. The company engages in various financial transactions, and with technological advancements, internet banking has become a convenient solution. However, it also poses security risks such as hacking and identity theft, making effective risk management essential to protect financial transactions. Bank tokens are a security technology that generates dynamic codes for each transaction, enhancing protection against unauthorized access and fraud. This research uses a descriptive qualitative approach to evaluate the effectiveness of bank token usage at PT Petrokimia Gresik through direct observation and literature review. The results indicate that using bank tokens increases transaction security, reduces fraud risk, and provides users with a sense of security. However, challenges such as usage difficulty and the risk of losing token devices persist. To address this, companies can establish written procedures and provide backup protocols for lost or damaged tokens. This research concludes that using bank tokens at PT Petrokimia Gresik effectively increases banking transaction security and is an integral part of the company's risk management strategy.*
***Keywords :*** *Internet banking, Risk Management, Security Technology, Bank Tokens*

## PENDAHULUAN

Petrokimia Gresik adalah produsen pupuk paling lengkap di Indonesia, memproduksi beragam jenis pupuk dan bahan kimia untuk mendukung solusi agroindustri (Inayah dkk., 2015). PT Petrokimia Gresik menjalankan beragam aktivitas bisnis yang melibatkan transaksi finansial, termasuk pembayaran vendor, penerimaan pembayaran dari pelanggan, dan transaksi keuangan internal lainnya.

Seiring dengan kemajuan zaman, dunia perbankan dituntut untuk meningkatkan pelayanan dan kinerja yang semakin optimal. Kemajuan teknologi yang menghasilkan internet banking menjadi salah satu bentuk layanan yang menguntungkan bagi perbankan, karena internet banking memberikan kemudahan baik bagi nasabah maupun perbankan (Murfi & Suripto, 2020). Internet banking memungkinkan berbagai transaksi dapat dilakukan dengan mudah tanpa perlu mengunjungi bank, cukup dengan satu sentuhan melalui smartphone atau laptop, kapan saja dan di mana saja selama 24 jam. (Wulandari & Novitasari, 2020).

Era digital membawa manfaat besar dalam hal efisiensi dan konektivitas, tetapi juga membawa risiko keamanan yang signifikan. Tentu saja pada setiap proses bisnis memiliki risiko, tidak terkecuali atas proses bisnis pengelolaan kas perusahaan. Risiko merupakan konsekuensi yang timbul akibat adanya ketidakpastian di masa depan, yang dapat mengakibatkan dampak merugikan bagi pelaku usaha. Risiko ini terkait dengan kemungkinan terjadinya kerugian yang tidak diharapkan (Maskhulin dkk., 2024). Terdapat beberapa ancaman yang dapat terjadi pada proses bisnis pengelolaan kas perusahaan seperti peretasan data, pencurian identitas, dan serangan *phishing* (Giri, 2022). Oleh karena itu, PT Petrokimia Gresik harus memprioritaskan manajemen risiko secara efektif untuk melindungi transaksi finansial dan menjaga keamanan sistem keuangan internal.

Manajemen risiko merupakan pendekatan sistematis yang membantu organisasi dalam mengidentifikasi potensi kerugian, baik itu dari faktor internal maupun eksternal. Manajemen risiko memungkinkan perusahaan untuk memahami dan mengevaluasi konsekuensi dari setiap risiko (Zunaedi dkk., 2022). Oleh karena itu, dengan proses perencanaan yang cermat dan perancangan strategi yang tepat, PT Petrokimia Gresik dapat mengurangi kemungkinan terjadinya kerugian atau bahkan menghindarinya sama sekali.

Industri perbankan telah mengembangkan teknologi keamanan yang inovatif, salah satunya adalah token bank. Token bank memberikan lapisan tambahan keamanan dengan menyediakan kode dinamis yang berubah setiap kali transaksi dilakukan (Hendarsyah, 2014). PT Petrokimia Gresik perlu memperkuat strategi keamanan transaksi finansial mereka untuk menghadapi ancaman yang terus berkembang. Penerapan teknologi keamanan seperti token bank merupakan langkah proaktif untuk melindungi perusahaan dan memastikan integritas transaksi finansial sehingga mengurangi risiko akses tidak sah serta penipuan.

Penelitian ini bertujuan untuk memberikan wawasan yang mendalam mengenai bagaimana token bank dapat meningkatkan perlindungan terhadap data nasabah dan mencegah berbagai bentuk kejahatan siber. Peneliti berharap dapat mengidentifikasi faktor-faktor yang mempengaruhi efektivitas penggunaan token bank serta solusi untuk mengatasi tantangan yang mungkin dihadapi. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan rekomendasi yang berguna bagi PT Petrokimia Gresik dalam meningkatkan sistem keamanan transaksinya.

Artikel ini terbagi atas beberapa bagian. Bagian pertama berisi tentang pendahuluan. Pada bagian kedua mendiskusikan tentang metode penelitian. Bagian ketiga berisi hasil dan pembahasan. Penelitian ini diakhiri dengan kesimpulan dan saran untuk PT Petrokimia serta penelitian yang dapat dilakukan selanjutnya.

## TELAAH LITERATUR

a. Pengendalian Internal

"Pengendalian internal adalah proses yang melibatkan dewan komisaris, manajemen, dan personel lainnya untuk memastikan bahwa tujuan entitas tercapai dengan memastikan keandalan efektivitas operasional, kepatuhan terhadap peraturan perundang-undangan pelaporan keuangan, serta perlindungan terhadap aset." (Maruta, 2016).

*Committee of Sponsoring Organizations of the Treadway Commission* (COSO), menegaskan terdapat lima komponen utama pengendalian internal, yaitu:

1. Lingkungan Pengendalian: Mencerminkan nilai dan etika yang melandasi tindakan organisasi.
2. Penilaian Risiko: Proses pengidentifikasian, analisis, dan evaluasi risiko yang dihadapi oleh organisasi.
3. Aktivitas Pengendalian: Prosedur dan kebijakan yang diterapkan untuk menanggapi risiko.
4. Komunikasi dan Informasi: Pengambilan keputusan dan pengendalian didukung secara kritis oleh penyampaian dan distribusi informasi yang signifikan.
5. Pemantauan Aktivitas: Proses evaluasi efektivitas pengendalian internal dan melakukan perbaikan yang diperlukan.

b. Manajemen Risiko

Manajemen risiko adalah proses mengidentifikasi, menganalisis, menilai, dan mengelola risiko yang dihadapi organisasi (Berliana dkk., 2020). Tujuan utama manajemen risiko untuk meminimalisir dampak negatif dari risiko dan meningkatkan peluang keberhasilan organisasi. Proses manajemen risiko terdiri dari beberapa langkah, seperti merencanakan risiko yang belum teratasi, mengidentifikasi risiko baru yang mungkin muncul, memastikan implementasi rencana manajemen risiko berjalan dengan baik, dan secara terus-menerus mengevaluasi efektivitasnya dalam mengurangi dampak risiko (Lokobal dkk., 2014).

c. Perbankan

Bank merupakan sebuah badan usaha yang bertujuan untuk memenuhi kebutuhan kredit, baik melalui alat pembayaran miliknya sendiri maupun dengan menggunakan dana dari pihak lain (Ibrahim, 2022). Proses menerima dan menahan dana yang dimiliki oleh orang atau badan lain dapat diartikan sebagai perbankan (Leviani & Wiyono, 2023). Dana dari masyarakat dihimpun oleh bank dengan berbagai produk simpanan jangka pendek, kemudian menyalurkannya sebagai pembiayaan, yang sebagian besar berjangka panjang. (Farid & Azizah, 2021). Di Indonesia, terdapat dua jenis perbankan yang beroperasi, yaitu bank syariah dan bank konvensional. Bank tersebut menerapkan karakteristik dan prinsip yang berbeda dalam sistem pendanaannya. Bank syariah beroperasi berdasarkan prinsip bagi hasil dan tidak menggunakan sistem bunga, sementara bank konvensional menjalankan operasinya berdasarkan prinsip bunga (Berlian dkk., 2023).

Menurut Fatriani (2018) penghimpunan dana yang tersedia di bank konvensional dan bank syariah mempunyai kesamaan. Kedua jenis bank ini mengumpulkan dana dari masyarakat melalui produk simpanan. sebagai berikut:

1. Giro adalah jenis simpanan yang memungkinkan penarikan dana kapan saja melalui bilyet giro, cek, instrumen pembayaran lainnya, atau pemindahbukuan.
2. Tabungan merupakan jenis simpanan yang hanya dapat ditarik sesuai dengan ketentuan yang telah disepakati, namun tidak memungkinkan penarikan menggunakan bilyet giro, cek, atau instrumen serupa.
3. Deposito merupakan jenis simpanan di bank yang penarikannya hanya dapat dilakukan setelah jangka waktu tertentu yang telah disepakati antara bank dan nasabah penyimpan.

Perkembangan teknologi yang melaju pesat mendorong sektor perbankan untuk meningkatkan layanan melalui pengembangan perbankan digital. Layanan perbankan digital adalah aktivitas perbankan yang menggunakan teknologi elektronik dari bank melalui platform digital nasabah untuk melakukan transaksi secara mandiri (Mutiasari, 2020). Layanan perbankan memegang peranan vital karena tidak hanya berfungsi sebagai sistem pembayaran yang efisien tetapi juga sebagai sarana bagi pelanggan untuk mengakses produk tabungan, uang tunai, dan fasilitas kartu kredit.

d. Internet Banking

*Internet banking* adalah penggunaan teknologi internet sebagai platform untuk melaksanakan transaksi yang terkait dengan aktivitas perbankan. memanfaatkan infrastruktur

jaringan internet sebagai saluran komunikasi antara nasabah dan lembaga perbankan (Wulandari & Novitasari, 2020).

Pengguna internet banking dapat memanfaatkan layanan tersebut secara fleksibel di berbagai lokasi dan waktu, asalkan tersedia akses internet untuk berkomunikasi dengan pihak bank. Salah satu keunggulan fasilitas ini adalah kemampuan bagi nasabah untuk mengakses rekening mereka setiap saat, sepanjang minggu (Wijanarto, 2020).

e. Keamanan pada Internet Banking

*Internet banking* telah menjadi salah satu layanan perbankan yang populer di Indonesia. Layanan ini menawarkan kemudahan serta kenyamanan bagi nasabah untuk melakukan berbagai transaksi perbankan, seperti cek saldo,pembayaran tagihan, dan transfer dana(Ava Dianta & Zusrony, 2019). Kemudahan ini juga diiringi dengan potensi risiko keamanan yang perlu diwaspadai.

Lingkungan *internet banking* tidak luput dari berbagai ancaman keamanan yang dapat membahayakan baik nasabah maupun pihak bank. Menurut Giri (2022) ada beberapa ancaman yang perlu diwaspadai antara lain:

1. *Phishing*: Teknik penipuan daring yang bertujuan untuk mencuri informasi pribadi nasabah, seperti *username,* kata sandi, dengan menyamar sebagai situs atau email resmi bank.
2. *Malware*: Perangkat lunak berbahaya yang dirancang untuk menyusup, merusak dan mengganggu komputer atau perangkat digital lainnya.
3. *Man-in-the-middle attack*: Serangan yang menyasar komunikasi antara nasabah dan bank, memungkinkan pihak ketiga untuk menyadap, memodifikasi, atau mencuri data transaksi.
4. *Social engineering*: Teknik manipulasi psikologis bertujuan untuk menipu nasabah agar memberikan informasi rahasia atau melakukan tindakan yang merugikan, seperti transfer dana ke rekening penipu.

f. Upaya Peningkatan Keamanan Internet Banking

Menyadari potensi risiko keamanan yang signifikan, berbagai upaya telah dilakukan untuk memperkuat keamanan *internet banking*. Safitri dkk. (2020) menegaskan, ada beberapa upaya untuk meingkatkan keamanan *internet banking* di antaranya:

1. Penerapan *Multi-Factor Authentication* (MFA): Meminta nasabah untuk memverifikasi identitasnya melalui beberapa faktor, seperti kombinasi *username*, *password*, dan OTP (*One Time Password*) yang unik dan dinamis, untuk mengakses *internet banking*.
2. Peningkatan edukasi kepada nasabah: Memberikan pelatihan serta edukasi kepada nasabah mengenai praktik aman dalam menggunakan layanan internet banking, mengenali modus penipuan daring, dan menjaga kerahasiaan informasi pribadi.
3. Peningkatan teknologi keamanan: Bank terus berinovasi serta mengembangkan teknologi keamanan terkini untuk melindungi *internet banking* dari berbagai ancaman, seperti enkripsi data yang kuat, sistem deteksi intrusi, dan pemantauan aktivitas mencurigakan secara *real-time*.

g. Token Bank

"Token bank, dikenal sebagai OTP (*One Time Password*) biasanya digunakan sebagai verifikasi tambahan yang dapat diminta secara sporadis. Jenis perangkat menghasilkan data otentikasi yang efektif dalam melawan serangan keamanan dengan menggunakan password yang dinamis atau berubah-ubah, di mana setiap password hanya bisa digunakan sekali" (Hendarsyah, 2014).

Token atau perangkat keamanan fisik, telah menjadi salah satu alat penting dalam meningkatkankeamanan transaksi perbankan, khususnya di era digital. Maraknya modus penipuan daring dan serangan *cyber*, token bank hadir pengaman tambahan yang penting untuk mengamankan dana dan data nasabah. Token bank umumnya berbentuk perangkat kecil seperti

kalkulator atau *flash drive USB*. Perangkat ini dilengkapi dengan tombol-tombol angka dan layar untuk menampilkan kode OTP.

## METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk mengkaji penggunaan token bank sebagai sarana peningkatan keamanan transaksi perbankan di PT Petrokimia Gresik. Pendekatan kualitatif deskriptif mengacu pada studi yang menganalisis interaksi sosial alami, menekankan bagaimana individu menafsirkan dan memahami pengalaman mereka untuk mendapatkan pemahaman yang mendalam tentang realitas sosial, memungkinkan mereka untuk mengatasi masalah mereka sendiri. Pendekatan kualitatif deskriptif dipilih karena memungkinkan peneliti untuk menggambarkan secara rinci dan komprehensif pengalaman dan persepsi karyawan terhadap penggunaan token bank dalam transaksi perbankan (Yuliani, 2018).

Sumber data penelitian terdiri dari data primer dan data sekunder. Data primer diperoleh melalui observasi. Observasi adalah teknik pengumpulan data yang melibatkan pengamatan langsung terhadap konteks dan partisipan yang terlibat dalam fenomena penelitian (Ardiansyah dkk., 2023). Observasi dilakukan di lokasi PT Petrokimia Gresik untuk melihat bagaimana token bank digunakan dalam transaksi sehari-hari, termasuk interaksi antara karyawan dan sistem token bank. Data sekunder diperoleh melalui kajian pustaka. Kajian pustaka mencakup pengumpulan informasi dari berbagai sumber tertulis seperti artikel jurnal, buku, laporan, dan dokumen kebijakan yang relevan dengan penggunaan token bank dan keamanan transaksi perbankan.

## HASIL DAN PEMBAHASAN

a. Praktik Keamanan Transaksi Perbankan yang Diterapkan di PT Petrokimia Gresik

Pada saat menjalankan kegiatan magang di PT Petrokimia Gresik, peneliti berkesempatan untuk mempelajari proses pengunduhan mutasi rekening melalui internet banking. Kegiatan ini bertujuan untuk memantau arus kas perusahaan, yaitu dengan melacak pergerakan dana masuk dan keluar setiap hari di berbagai rekening bank yang dimiliki PT Petrokimia Gresik. Setiap platform internet banking memiliki tampilan dan metode autentikasi yang berbeda, mulai dari autentikasi *password-based*, hingga *Multi-Factor Authentication* (MFA) yang lebih canggih.

Keamanan autentikasi merupakan hal yang krusial, meskipun beberapa platform masih menggunakan metode autentikasi *password-based*, namun dengan adanya *Multi*-Factor *Authentication* (MFA) seperti token bank telah membawa peningkatan yang signifikan dalam tingkat keamanan. Sistem autentikasi *password-based* ini memiliki beberapa kelemahan yang perlu diperhatikan yaitu rentan untuk ditebak, *username* dan *password* dapat dengan mudah diprediksi atau ditebak oleh penjahat *cyber* melalui berbagai metode, seperti *phishing* dan *brute force attack.*

Autentikasi *password-based* rentan terhadap peretasan karena informasi login seperti *username* dan *password* dapat diretas oleh penjahat *cyber* dengan menggunakan teknik *malware* atau *social* engineering. Metode autentikasi *password-based* juga meningkatkan risiko *fraud*, penjahat *cyber* dapat menggunakan informasi tersebut untuk melakukan transfer dana ke rekening yang tidak sah.

b. Manfaat Penggunaan Token Bank untuk Meningkatkan Keamanan Transaksi Perbankan

Penggunaan token bank dapat memberikan beberapa manfaat, yaitu meningkatkan keamanan, meminimalisir risiko penyalahgunaan dana serta kebocoran data. Token bank memperkuat keamanan transaksi dengan menghasilkan kode unik yang hanya berlaku dalam waktu singkat, sehingga sulit bagi penjahat *cyber* untuk melakukan transaksi perbankan secara tidak sah.

Token bank dapat digunakan untuk verifikasi transaksi yang dianggap penting atau sensitif, misalnya, untuk transfer dana besar atau pembayaran ke pihak ketiga baru. Pengguna perlu

memasukkan kode dari token bank untuk menyelesaikan transaksi agar membantu memastikan bahwa transaksi tersebut sah dan diotorisasi oleh pemilik akun sehingga mengurangi risiko *fraud*.

c. Tingkat Evektivitas Penggunaan Token Bank

Tingkat efektivitas penggunaan token bank untuk meningkatkan keamanan transaksi perbankan dapat dirasakan oleh pengguna karena token bank memberikan lapisan keamanan tambahan dalam proses login dan otorisasi transaksi perbankan. Token bank tidak terhubung ke internet, sehingga tidak bisa diakses oleh *malware* yang dapat mencuri *username* dan *password* pengguna. *Malware* yang tertanam di perangkat pengguna tidak memiliki cara untuk mendapatkan kode unik dari token bank, sehingga akun pengguna terlindungi dari serangan *cyber* jenis ini.

Penggunaan token bank dapat meningkatkan kepercayaan pengguna terhadap layanan perbankan online karena mengetahui bahwa akun mereka terlindungi dengan baik, sehingga pengguna merasa nyaman dan aman saat melakukan transaksi online. Melalui autentikasi dua faktor yang melibatkan penggunaan token bank, risiko penipuan atau aktivitas tidak sah lainnya dapat dikurangi, selain itu dapat membantu dalam mendeteksi aktivitas mencurigakan pada transaksi perbankan. Jika terjadi upaya akses yang tidak sah atau percobaan pengunduhan yang tidak biasa, token bank dapat memberikan lapisan perlindungan tambahan dan memicu peringatan kepada pengguna atau administrator sistem.

d. Tantangan Menggunakan Token Bank

Penggunaan token bank dapat meningkatkan keamanan transaksi perbankan, namun sejumlah tantangan mungkin akan timbul bagi pengguna saat mengimplementasikan dan menggunakan token bank. Pengguna harus mempelajari cara kerja token serta proses autentikasi dua faktor, yang mungkin menimbulkan kebingungan atau ketidaknyamanan penggunaan. Token bank, kebanyakan berupa perangkat fisik, harus selalu dibawa atau disimpan oleh pengguna, sehingga jika hilang, rusak, atau tidak tersedia dapat menghambat kemampuan untuk melakukan transaksi. Kesulitan dalam mengakses token bank, terutama di tempat yang jauh dari perangkat, juga dapat mengakibatkan penundaan atau bahkan ketidakmampuan untuk mengakses layanan perbankan secara langsung.

e. Mitigasi Risiko Penggunaan Token Bank

Token bank menawarkan banyak manfaat dalam meningkatkan keamanan transaksi perbankan akan tetapi tidak ada sistem yang sempurna. Oleh karena itu, untuk mengurangi risiko terkait dengan penggunaan token bank perusahaan bisa membuat prosedur tertulis bagi pengguna mengenai cara menggunakan token bank dengan benar, termasuk proses autentikasi dua faktor dan tindakan keamanan yang diperlukan sehingga dapat mengurangi kesalahan serta kebingungan dalam penggunaan token.

Pengguna harus memiliki prosedur cadangan serta penggantian untuk token bank hilang, rusak, atau dicuri sehingga dapat membantu mengurangi dampak negatif, misalnya bank memberikan opsi agar menonaktifkan token yang hilang dan mengaktifkan token pengganti. Pengguna juga harus memastikan token bank dalam kondisi baik dan terjaga keandalannya melalui pemeliharaan rutin serta perbaikan jika diperlukan sehingga dapat mengurangi risiko kegagalan perangkat yang dapat menghambat akses pengguna terhadap layanan perbankan.

## SIMPULAN

Pemanfaatan token bank di PT Petrokimia Gresik telah terbukti efektif dalam meningkatkan keamanan transaksi perbankan. Penggunaan token bank dapat membantu meminimalisir risiko penyalahgunaan dana dan kebocoran data, serta mengurangi risiko *fraud* yang disebabkan oleh peretasan informasi login. Penggunaan token bank juga dapat menimbulkan beberapa tantangan, seperti kebingungan awal dalam penggunaan dan kemungkinan kehilangan

atau kerusakan perangkat. Oleh karena itu untuk mengatasi ini, perusahaan dapat membuat prosedur tertulis bagi pengguna mengenai cara menggunakan token bank dengan benar, serta memberikan prosedur *backup* dan penggantian yang baik untuk mengurangi dampak negatif dari kehilangan atau kerusakan token, sehingga penggunaannya dapat menjadi langkah efektif dalam meningkatkan keamanan transaksi perbankan di PT Petrokimia Gresik.

## SARAN

Penulis menyarankan kepada PT Petrokimia untuk mengusulkan kepada pihak perbankan yang masih menggunakan autentikasi password-based, agar memiliki fitur Multi-Factor Authentication (MFA) pada internet banking untuk meningkatkan tingkat keamanan secara menyeluruh. Pemanfaatan token bank di PT Petrokimia Gresik tidak hanya meningkatkan keamanan transaksi perbankan tetapi juga merupakan bagian integral dari manajemen risiko dan pengendalian internal. Oleh karena itu, dengan menggunakan token bank dapat memastikan perusahaan beroperasi dengan lebih aman dan efisien, melindungi asetnya dari ancaman cyber, serta memenuhi kewajiban regulasi dengan lebih baik.

## DAFTAR PUSTAKA

Ardiansyah, Risnita, & Jailani, M. S. (2023). Teknik Pengumpulan Data Dan Instrumen Penelitian Ilmiah Pendidikan Pada Pendekatan Kualitatif dan Kuantitatif. *Jurnal IHSAN : Jurnal Pendidikan Islam*, *1*(2), 1–9. https://doi.org/10.61104/ihsan.v1i2.57

Ava Dianta, I., & Zusrony, E. (2019). Analisis Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking. *INTENSIF*, *3*(1), 2549–6824.

Berlian, D., Andri, & Apriana, A. (2023). Perbandingan Pemberian Kredit Antara Bank Konvensional dan Pembiayaan Bank Syariah Kepada Usaha Kecil dan Menengah. *Jurnal Perbankan Syariah Indonesia)*, *2*(2), 62–72.

Berliana, M., Sajjad, A., Salsabila, U. J., Kalista, D., Jember, U., Zidan, M., & Christian, J. (2020). ANALISIS MANAJEMEN RISIKO BISNIS (Studi pada Cuanki Asoy Jember). Dalam *Jurnal Akuntansi Universitas Jember* (Vol. 18, Nomor 1).

Farid, M., & Azizah, W. (2021). Manajemen Risiko dalam Perbankan Syariah. *Jurnal Akuntansi dan Keuangan Islam*, *3*(2), 67–80.

Fatriani, R. (2018). Bentuk Bentuk Produk Bank Konvensional dan Bank Syariah di Indonesia. *Ensiklopedia of Journal*, *1*(1), 218–224. http://jurnal.ensiklopediaku.org

Giri, B. E. (2022). PENERAPAN KRIPTOGRAFI DENGAN METODE RSA PADA INTERNET BANKING (STUDI KASUS: SECURITY TOKEN DAN SMART CARD). Dalam *Manajemen Komputer dan Rekayasa Sistem Cerdas* (Vol. 1, Nomor 1).

Hendarsyah, D. (2014). *KEAMANAN LAYANAN INTERNET BANKING DALAM TRANSAKSI PERBANKAN*.

Ibrahim, Y. (2022). Bank Syariah dan Konvensional (Suatu Analisis Perbedaan dan Prinsip-prinsipnya). *SYARAH: Jurnal Hukum Islam*, *11*(1), 1–15.

Inayah, F., Zainul, I., & Yulianto, A. E. (2015). ANALISIS STRATEGI PEMASARAN UNTUK MENINGKATKAN VOLUME PENJUALAN EKSPOR" (Studi pada PT Petrokimia Gresik). *Jurnal Administrasi Bisnis (JAB)*, *24*(1).

Leviani, N., & Wiyono, S. (2023). PENGARUH MOBILE BANKING, INTERNET BANKING, NON PERFORMING LOAN DAN BIAYA OPERASIONAL PENDAPATAN OPERASIONAL TERHADAP PROFITABILITAS RETURN ON ASSET BANK PADA PERUSAHAAN PERBANKAN YANG TERDAFTAR DI BEI TAHUN 2017 – 2021. *Jurnal Ekonomi Trisakti*, *3*(1), 1613–1622. https://doi.org/10.25105/jet.v3i1.16213

Lokobal, A., Pascasarjana, A., Sam, U., Marthin, R., Sumajouw, D. J., & Sompie, B. F. (2014). MANAJEMEN RISIKO PADA PERUSAHAAN JASA PELAKSANA KONSTRUKSI

DI PROPINSI PAPUA (Study Kasus di Kabupaten Sarmi). *Jurnal Ilmiah Media Engineering*, *4*(2), 109–118.

Maruta, H. (2016). Pengendalian Internal Dalam Sistem Informasi Akuntansi. *IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita*, *5*(1), 16–28.

Maskhulin, P. I. A., Setyawan, W. P., Andarini, S., & Kusumasari, I. R. (2024). Memahami dan Mengelola Risiko Bisnis dalam Perencanaan dan Pengembangan Bisnis. *NERACA: Jurnal Ekonomi, Manajemen, dan Akuntansi*, *194*(4), 194–203. http://jurnal.kolibi.org/index.php/neraca

Murfi, R., & Suripto, T. (2020). Analisa Minat Mahasiswa terhadap Penggunaan Layanan Internet Banking Bank BNI Syariah. *Jurnal Ekonomi Syariah Indonesia*, *10*(1), 55–61.

Mutiasari, A. I. (2020). Perkembangan Industri Perbankan di Era Digital. *Ekonomi Bisnis dan Kewirausahaan*, *9*(2), 31–41. www.aptika.kominfo.go.id,

Safitri, E. M., Larasati, A. S., & Hari, S. R. (2020). Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi dan Robotika*, *2*(1), 12–16.

Wijanarto, A. L. (2020). Peran Penggunaan Internet Banking terhadap Kepuasan Nasabah Bank BCA (Studi pada Nasabah Pengguna Fasilitas M-BCA di Kota Depok). *Jurnal Ekonomi, Manajemen, dan Perbankan*, *6*(1), 1–12.

Wulandari, S., & Novitasari, N. (2020). Pengaruh Internet Banking, Risiko Kredit dan Ukuran Perusahaan Terhadap Kinerja Keuangan Perbankan Yang Terdaftar Di Bursa Efek Indonesia Periode 2017 - 2019. *Jesya (Jurnal Ekonomi & Ekonomi Syariah)*, *4*(1), 166–177. https://doi.org/10.36778/jesya.v4i1.327

Yuliani, W. (2018). METODE PENELITIAN DESKRIPTIF KUALITATIF DALAM PERSPEKTIF BIMBINGAN DAN KONSELING. *QUANTA: Jurnal Kajian Bimbingan dan Konseling dalam Pendidikan*, *2*(2), 83–91. https://doi.org/10.22460/q.v2i2p83-91.1641

Zunaedi, B. N. F., Annisa, H. R., & Dewi, M. (2022). Fungsi Internal Audit dan Manajemen Risiko Perusahaan: Sebuah Tinjauan Literatur. *Jurnal Bisnis dan Akuntansi*, *24*(1), 59–70. http://jurnaltsm.id/index.php/JBA