

Peran Prinsip Akuntabilitas Sebagai Strategi Mitigasi Risiko Operasional Pada Bank Digital: Studi Kasus SeaBank Indonesia

Zaqiyatin Nabila¹, Resty Rahayu Virnanda², Faradila Desiyanti Yusuf³, Rohmawati Kusumaningtias⁴, Ambar Kusumaningsih⁵

^{1,2,3,4,5} Akuntansi, Universitas Negeri Surabaya

e-mail: zaqiyatin.23428@mhs.unesa.ac.id¹, resty.23383@mhs.unesa.ac.id²,
faradila.23285@mhs.unesa.ac.id³, rohmatikusumaningtias@unesa.ac.id⁴,
ambarkusumaningsih@unesa.ac.id⁵

Abstrak

Transformasi perbankan dari sistem konvensional menuju digital membawa dampak signifikan terhadap efisiensi dan kemudahan akses layanan. Namun, perubahan ini juga meningkatkan potensi risiko operasional seperti kebocoran data, serangan siber, serta penyalahgunaan teknologi digital. Penelitian ini bertujuan untuk menganalisis peran prinsip akuntabilitas sebagai strategi mitigasi terhadap risiko operasional pada SeaBank Indonesia. Metode penelitian yang digunakan adalah pendekatan kualitatif. Hasil penelitian menunjukkan bahwa SeaBank menerapkan prinsip akuntabilitas melalui transparansi pelaporan, pengawasan internal, serta penguatan regulasi perlindungan data. Prinsip akuntabilitas terbukti mampu meminimalkan risiko operasional dan meningkatkan kepercayaan masyarakat terhadap layanan perbankan digital. Kesimpulan dari penelitian ini adalah bahwa akuntabilitas dalam perbankan digital tidak hanya bertujuan untuk memenuhi standar, tetapi juga menciptakan lingkungan keuangan yang aman dan dapat diandalkan serta menjadi strategi penting dalam menghadapi tantangan operasional pada era digital.

Kata kunci: *Akuntabilitas, Risiko Operasional, Bank Digital*

Abstract

The transformation of banking from conventional systems to digital platforms has significantly improved service efficiency and accessibility. However, this shift has also increased the potential for operational risks such as data breaches, cyberattacks, and misuse of digital technology. This study aimed to analyze the role of accountability as a mitigation strategy for operational risks in SeaBank Indonesia. A qualitative approach was used to explore this issue. The results show that SeaBank applies the principle of accountability through transparent reporting, internal supervision, and reinforced data protection regulations. Accountability helps minimize operational risks and strengthens public trust in digital banking services. It is concluded that accountability in digital banking not only fulfills regulatory standards but also creates a secure and reliable financial environment, serving as a crucial strategy in addressing operational challenges in the digital era.

Keywords : *Accountability, Operational Risk, Digital Bank*

PENDAHULUAN

Munculnya Bank digital adalah salah satu bukti perkembangan teknologi digital dalam sektor perbankan. Bank digital menawarkan kemudahan akses, efisiensi layanan, serta integrasi dengan berbagai platform teknologi, sehingga menjadi pilihan populer terutama di kalangan generasi muda, hal ini mendukung penelitian dari (Kitsios & Giatsidis, 2021). **Riset dari Ipsos Digital Solutions** pada Februari 2025 mengungkapkan bahwa mayoritas pengguna aktif Bank digital di Indonesia berasal dari kelompok usia 25-44 tahun, dengan SeaBank, Bank Jago, dan Bank Neo sebagai pilihan teratas mereka. Selain faktor teknologi, ada beberapa faktor dalam penerimaan bank digital, seperti faktor sosial dengan adanya *trend* atau gaya hidup. Kemudian faktor personalitas atau kognitif juga dapat mempengaruhi perilaku orang untuk menggunakan

produk bank digital (Hariwibowo & Setiawan, 2024). Bank digital melaksanakan kegiatan usaha melalui saluran elektronik tanpa kantor fisik selain KP sebagaimana dimaksud pada ayat (2) pasal 23 dalam (Komisioner & Jasa, 2021), atau dapat menggunakan kantor fisik yang terbatas. Dari sisi lembaga keuangan, digitalisasi mampu mengurangi biaya operasional karena tidak memerlukan banyak kantor fisik dan staf pendukung, ini memungkinkan Bank untuk mengalokasikan sumber daya secara lebih optimal ke arah inovasi dan pengembangan produk. Digitalisasi perbankan diperkirakan akan terus berkembang, dengan harapan semua Bank bertransformasi menjadi digital 10-20 tahun ke depan. Di samping membawa peluang yang dapat dimanfaatkan oleh industri perbankan, transformasi digital memunculkan tantangan yang perlu diwaspadai. **Menurut Otoritas Jasa Keuangan**, beberapa tantangan tersebut mencakup perlindungan data pribadi dan risiko kebocoran data, risiko investasi teknologi yang tidak sesuai dengan strategi bisnis, risiko penyalahgunaan teknologi *artificial intelligence*, risiko serangan siber, serta risiko alih daya. Selain itu, tantangan lainnya mencakup literasi keuangan digital yang masih rendah, infrastruktur teknologi informasi yang belum merata di Indonesia, dan perlunya dukungan kerangka regulasi yang adaptif terhadap inovasi digital.

Dalam konteks risiko-risiko tersebut, prinsip akuntabilitas menjadi salah satu pondasi penting dalam menjaga keberlanjutan dan kepercayaan publik terhadap Bank digital. Akuntabilitas juga erat kaitannya dengan prinsip tata kelola perusahaan yang baik (*Good Corporate Governance*), yang berperan strategis dalam memitigasi risiko operasional serta memastikan Bank beroperasi secara etis dan profesional. Akuntabilitas tidak hanya mencakup kewajiban untuk mempertanggungjawabkan setiap keputusan dan aktivitas keuangan, tetapi juga menjadi landasan dalam membangun kepercayaan publik, menjaga transparansi, dan mencegah potensi kegagalan sistem. Prinsip akuntabilitas melibatkan komitmen untuk menjelaskan serta mempertanggungjawabkan tindakan kepada pihak-pihak yang memiliki hak dan kepentingan. Dalam konteks bank digital, yang seluruh proses dan pelaporannya bergantung pada teknologi, akuntabilitas berbasis sistem informasi menjadi semakin penting. Oleh karena itu, integrasi teknologi dengan prinsip-prinsip akuntabilitas menjadi strategi kunci dalam memitigasi risiko keuangan serta menjaga keberlanjutan dan kepercayaan publik terhadap insitusi perbankan digital. Penerapan teknologi informasi dalam sistem akuntansi bank dapat meningkatkan transparansi dan akuntabilitas laporan keuangan, (Michalle & Sisdianto, 2024).

Salah satu Bank digital yang berkembang pesat di Indonesia adalah SeaBank, bagian dari ekosistem Sea Group yang juga menaungi Shopee dan Garena. Sebagai Bank digital yang terhubung erat dengan platform *e-commerce*, SeaBank mengelola volume transaksi besar setiap harinya. Kondisi ini menuntut adanya sistem manajemen risiko keuangan yang andal, bukan hanya dari sisi teknologi, tetapi juga dari sisi tata kelola perusahaan yang baik. **Upaya Seabank Indonesia** dalam memenuhi regulasi dan kepercayaan publik telah membuahkan penghargaan dalam bidang kepatuhan hukum pada tahun 2024. Melalui studi kasus pada SeaBank, artikel ini akan mengeksplorasi bagaimana penerapan prinsip akuntabilitas digunakan sebagai strategi mitigasi risiko keuangan dalam praktik perbankan digital. Diharapkan penelitian ini dapat memberikan kontribusi terhadap pemahaman akademik dan praktis mengenai tata kelola risiko di era perbankan digital.

Akuntabilitas dalam Lembaga Keuangan

Akuntabilitas dalam konteks modern, termasuk juga perbankan digital yang dibahas dalam penelitian ini merujuk pada kewajiban untuk mempertanggungjawabkan setiap keputusan. Akuntabilitas merupakan salah satu prinsip dalam *Good Corporate Governance* (GCG), prinsip ini sangat penting dalam tata kelola perusahaan. Akuntabilitas sendiri merupakan komponen utama dalam sektor keuangan yang digunakan untuk menjaga kepercayaan, integritas dan juga stabilitas sistem perbankan. Akuntabilitas sendiri merupakan konsep terkait dengan mekanisme pertanggungjawaban dari satu pihak ke pihak lainnya. Istilah akuntabilitas berasal dari bahasa Inggris *accountability* yang berarti pertanggungjawaban (Mursalim & Junaid, 2022). Akuntabilitas sendiri sangat dibutuhkan agar setiap lembaga negara melaksanakan tugasnya secara bertanggung jawab.

Risiko Operasional dalam Bank Digital

Seiring berkembangnya digitalisasi, industri perbankan menghadapi jenis risiko baru yang berbeda dengan risiko tradisional. Bank digital adalah industri perbankan yang harus mampu merespon berbagai risiko mendasar yang bisa berdampak pada performa operasionalnya (Kurniawan et al., 2021). Di antara berbagai risiko operasional yang muncul dalam bank digital antara lain:

Risiko Kebocoran Data

Risiko pertama yang paling rawan dalam bank digital adalah risiko kebocoran data, risiko ini sangat rawan karena seperti yang kita semua tahu untuk mendaftarkan diri dan menggunakan bank digital butuh data diri nasabah seperti NIK, NPWP dan nomor rekening, data diri inilah yang harus sangat dijaga dan diperhatikan agar tidak bocor dan disalahgunakan. Kebocoran data nasabah khususnya nasabah bank digital bisa menimbulkan kesalahan yang sangat fatal yang menimbulkan hilangnya kepercayaan dan juga rasa aman nasabah kepada bank (Michalle & Sisdiyanto, 2024).

Risiko Siber

Risiko siber ini merupakan tantangan yang sangat besar bagi bank digital yang saat ini berkembang sangat pesat di Indonesia. Bank digital yang kinerjanya fokus dibawah teknologi maka seharusnya sudah mampu untuk menghalau serangan siber dengan teknologi terbarunya (Harahap, 2025). Bank digital sangat rentan terhadap ancaman siber seperti peretasan, malware dan serangan lainnya. Serangan ini dapat menyebabkan gangguan operasional, pencurian data nasabah, hingga menyebabkan kerugian finansial.

Risiko Penyalahgunaan Teknologi *Artificial Intelligence* (AI)

Dalam era digital, sangat penting bagi pengguna layanan atau nasabah untuk memahami cara kerja aplikasi dan sistem digital yang digunakan. kurangnya pemahaman terkait hal seringkali dimanfaatkan oleh pihak pihak yang tidak bertanggung jawab, salah satunya adalah penggunaan teknologi *artificial intelligence* (AI) oleh pelaku kejahatan siber. AI telah banyak digunakan pada bidang manufaktur, perbankan, kesehatan dan transportasi guna meningkatkan efisiensi kinerja perusahaan (Sulistyowati et al., 2023), akan tetapi meski demikian di zaman yang semakin modern dan digital AI seringkali digunakan untuk kegiatan yang dapat merugikan, contohnya saat ini teknologi AI dapat menciptakan serangan yang canggih seperti *deep fake voice* atau *automated identity theft*, hal ini membuat data pribadi seperti *password*, PIN dan kode OTP menjadi sangat rentan apabila pengguna tidak berhati hati. Sangat penting bagi nasabah untuk menjaga data pribadinya dan tidak membagikannya pada pihak lain.

Akuntabilitas sebagai Strategi Mitigasi Risiko

Perkembangan teknologi digital dalam sektor perbankan membawa dampak besar terhadap kompleksitas risiko yang dihadapi, terutama oleh bank digital seperti SeaBank. Risiko-risiko modern seperti serangan siber, kebocoran data nasabah hingga penyalahgunaan teknologi *Artificial Intelligence* (AI) menuntut adanya strategi mitigasi risiko yang adaptif dan berbasis teknologi. Strategi tersebut tidak hanya bersifat reaktif terhadap serangan, tetapi juga proaktif, pendekatan proaktif menekankan pada langkah yang harus diambil sebelum risiko dengan tujuan utama mencegah ancaman atau meminimalkan peluang terjadinya risiko. Selain itu, penerapan prinsip akuntabilitas juga menjadi aspek penting dalam mitigasi risiko. Transparansi dalam pelaporan insiden keamanan, penunjukan pihak atau unit yang memiliki tanggung jawab langsung atas perlindungan data, serta penyusunan prosedur tanggap darurat yang sistematis menunjukkan komitmen terhadap perlindungan data nasabah dan tata kelola digital yang baik. Bank digital dituntut untuk tidak hanya mengandalkan sistem keamanan teknologi, tetapi juga memperkuat nilai-nilai kelembagaan, salah satunya melalui prinsip akuntabilitas. Akuntabilitas merupakan prinsip yang mengatur keselarasan aturan yang berlaku dengan kinerja lapangan. Prinsip ini menekankan setiap entitas, baik individu maupun organisasi harus mempertanggungjawabkan kinerjanya sesuai dengan ketentuan yang telah ditetapkan baik yang sudah diterapkan secara umum maupun yang diatur dalam perundang undangan (Nisak & Riza, 2023).

Melalui akuntabilitas, bank digital tidak hanya bersifat responsif ketika risiko terjadi, tetapi juga menunjukkan komitmen jangka panjang terhadap tata kelola yang baik (*good governance*). Akuntabilitas menciptakan budaya organisasi yang peduli terhadap keamanan data dan integritas

operasional. Dalam konteks bank digital seperti SeaBank, akuntabilitas mendorong perusahaan untuk selalu memenuhi standar perlindungan konsumen serta keamanan informasi yang ditetapkan oleh otoritas keuangan

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur yang bertujuan untuk mengeksplorasi secara mendalam bagaimana prinsip akuntabilitas diterapkan sebagai strategi mitigasi risiko operasional dalam konteks perbankan digital, dengan fokus pada studi kasus SeaBank Indonesia. Pendekatan ini dipilih karena permasalahan yang dikaji bersifat konseptual dan normatif, serta erat kaitannya dengan dinamika tata kelola perusahaan berbasis teknologi. Objek utama dalam penelitian ini adalah prinsip akuntabilitas sebagai bagian dari pilar tata kelola perusahaan yang baik (Good Corporate Governance), dengan fokus pada penerapannya dalam mengelola risiko digital seperti kebocoran data, serangan siber, dan penyalahgunaan teknologi informasi. Definisi operasional akuntabilitas dalam konteks ini merujuk pada komitmen institusi untuk secara terbuka mempertanggungjawabkan keputusan, proses, dan hasil kepada publik serta regulator, sebagai bentuk transparansi dan integritas. Melalui pendekatan ini, penelitian diharapkan dapat memberikan gambaran konseptual yang utuh mengenai bagaimana akuntabilitas dijalankan secara nyata dalam mendukung keberlanjutan dan keamanan operasional bank digital.

Ruang lingkup penelitian dibatasi pada kajian dokumen sekunder, termasuk jurnal akademik, laporan industri, regulasi dari Otoritas Jasa Keuangan (OJK), serta publikasi resmi dari SeaBank Indonesia. Tempat penelitian bersifat non-lokasi karena seluruh data dikumpulkan secara daring. Populasi penelitian terdiri dari dokumen dan sumber digital yang relevan, sementara unit analisis adalah isi literatur yang dipilih berdasarkan kriteria keterkinian (maksimal 5 tahun terakhir), relevansi terhadap topik, dan kredibilitas sumber. Teknik pengumpulan data dilakukan melalui eksplorasi referensi digital, termasuk Google Scholar, portal jurnal institusional, situs resmi OJK dan ISO, serta website perusahaan. Data dianalisis menggunakan pendekatan analisis isi (content analysis), yaitu dengan membaca dan menginterpretasi isi dokumen, mengelompokkan informasi berdasarkan tema seperti risiko keuangan dan tata kelola, serta menyusun hasil dalam bentuk narasi tematik.

Untuk memperkaya perspektif dan menambahkan data lapangan, peneliti juga melakukan wawancara informal secara daring dengan salah satu pegawai SeaBank Indonesia dari divisi kepatuhan dan manajemen risiko. Wawancara dilakukan secara semi-terstruktur untuk mendapatkan gambaran nyata mengenai bagaimana prinsip akuntabilitas diimplementasikan dalam operasional sehari-hari. Dari hasil wawancara, diketahui bahwa setiap keputusan strategis yang menyangkut pengelolaan risiko di SeaBank harus melewati proses pelaporan internal yang ketat dan terdokumentasi, termasuk pelaporan potensi insiden keamanan. Pegawai menjelaskan bahwa SeaBank menerapkan sistem berbasis teknologi untuk memantau aktivitas tidak wajar (anomaly detection), dan bahwa tiap unit kerja diwajibkan membuat log tanggung jawab sebagai bagian dari sistem audit internal. Pegawai tersebut juga menambahkan bahwa budaya pelaporan dan keterbukaan sangat dijaga dalam organisasi, dan setiap pelanggaran SOP langsung ditindak sesuai prosedur.

Dengan menggabungkan pendekatan studi literatur dan wawancara ini, penelitian ini memberikan gambaran menyeluruh mengenai bagaimana akuntabilitas tidak hanya menjadi kerangka normatif, tetapi juga dijalankan secara operasional sebagai strategi nyata untuk memitigasi risiko keuangan di bank digital seperti SeaBank. Hasil kajian menunjukkan bahwa akuntabilitas diterapkan melalui sistem pengawasan internal yang aktif, transparansi pelaporan, dan struktur tanggung jawab yang jelas di setiap level organisasi. Temuan dari wawancara juga menguatkan bahwa budaya akuntabilitas di SeaBank tidak hanya bersifat formal, tetapi tertanam dalam proses kerja harian pegawai. Penerapan prinsip ini terbukti mendukung respons cepat terhadap potensi risiko, sekaligus memperkuat kepercayaan nasabah terhadap keamanan layanan digital yang diberikan. Dengan demikian, akuntabilitas menjadi landasan penting dalam menciptakan tata kelola yang adaptif dan berkelanjutan dalam era perbankan digital.

HASIL DAN PEMBAHASAN

Penerapan Prinsip Akuntabilitas di SeaBank

SeaBank menerapkan prinsip akuntabilitas sebagai bagian integral dari tata kelola perusahaan yang baik (*Good Corporate Governance*). Akuntabilitas di sini tidak hanya mencakup pertanggungjawaban formal kepada regulator dan pemegang saham, tetapi juga meluas pada pengelolaan risiko operasional dan perlindungan kepentingan nasabah. Dalam laporan tahunan dan keberlanjutan (SeaBank, 2024), dijelaskan bahwa SeaBank berkomitmen terhadap lima prinsip utama GCG, yaitu: transparansi, akuntabilitas, pertanggungjawaban, independensi, dan kewajaran. SeaBank menyatakan bahwa prinsip-prinsip tersebut diterapkan secara konsisten dalam seluruh aktivitas bisnis dan operasionalnya untuk memastikan adanya pertanggungjawaban yang jelas di seluruh jenjang organisasi. Penerapan akuntabilitas juga ditunjukkan melalui sistem pengawasan dan evaluasi internal. SeaBank menjalankan pengawasan melekat melalui audit internal yang bertanggung jawab langsung kepada Dewan Komisaris. Setiap hasil audit menjadi dasar evaluasi dan perbaikan prosedur untuk meningkatkan efisiensi serta mencegah terjadinya penyimpangan. Selain itu, rapat koordinasi dan pelaporan berkala kepada Direksi serta unit kerja terkait menjadi bagian dari mekanisme pertanggungjawaban yang berkelanjutan.

SeaBank juga secara aktif menerapkan sistem manajemen risiko terintegrasi, termasuk pelaporan insiden operasional dan pengukuran eksposur terhadap risiko. Mekanisme ini bertujuan untuk memastikan bahwa setiap unit kerja bertanggung jawab dalam mengidentifikasi dan menangani risiko yang mungkin timbul, terutama dalam konteks perbankan digital yang sangat rentan terhadap gangguan teknologi dan siber. Untuk menjamin keamanan data dan integritas informasi, SeaBank telah memperoleh sertifikasi **ISO 270001** yang menunjukkan kepatuhan terhadap standar internasional dalam pengelolaan keamanan informasi. Hal ini merupakan bentuk konkret akuntabilitas dalam menjaga kerahasiaan dan keandalan sistem digital mereka. SeaBank juga menyediakan akses publik terhadap informasi kinerja keuangan, tata kelola, dan kepatuhan regulasi melalui situs resminya. Ini mencerminkan keterbukaan dalam mempertanggungjawabkan seluruh aktivitas bisnis kepada para pemangku kepercayaan masyarakat terhadap entitas perbankan digital. Secara keseluruhan, penerapan prinsip akuntabilitas di SeaBank telah terbukti menjadi pondasi utama dalam mendukung pengelolaan risiko operasional secara efektif, menjaga kepercayaan publik, serta menciptakan sistem pengawasan internal yang terukur dan dapat dievaluasi secara berkala.

Identifikasi Risiko Operasional pada Bank Digital SeaBank

SeaBank yang merupakan perbankan digital di Indonesia telah mengalami perkembangan pesat dalam beberapa tahun terakhir. Dengan adopsi teknologi canggih seperti *Artificial Intelligence (AI)*, *cloud computing*, dan layanan perbankan berbasis aplikasi, SeaBank berupaya meningkatkan efisiensi operasional dan pengalaman nasabah. Namun, transformasi digital ini juga membawa tantangan baru, khususnya dalam risiko operasional yang berkaitan dengan keamanan data dan teknologi. Meski demikian beberapa risiko baru muncul dan SeaBank tetap mengalami tantangan yang cukup signifikan dalam mengelola risiko operasionalnya terutama yang berkaitan dengan:

Risiko Kebocoran data

Sebagai bank digital, SeaBank mengelola data pribadi dan juga data finansial nasabah secara elektronik pastinya sehingga sangat rentan terhadap kebocoran data. Dampak yang sangat signifikan seperti kerugian finansial, turunnya kepercayaan nasabah hingga sanksi regulasi dari Otoritas Jasa Keuangan (OJK). Risiko ini muncul karena adanya pengunggahan data pribadi yang sensitif seperti NIK dan NPWP, risiko ini adalah bentuk kegagalan sistem keamanan (Sheren et al., 2023). Data pribadi dan finansial nasabah yang tersimpan dalam server bank menjadi target empuk bagi peretas. Kebocoran ini tidak hanya berdampak pada reputasi, tetapi juga berpotensi melanggar UU Perlindungan Data Pribadi. Pihak SeaBank menyatakan bahwa mereka menerapkan enkripsi end-to-end dan audit sistem berkala sebagai langkah mitigasi risiko kebocoran data.

Risiko Siber

SeaBank yang beroperasi sepenuhnya berbasis teknologi sangat bergantung pada sistem informasi, internet dan aplikasi digital untuk menjalankan seluruh aktivitas bisnisnya. Ketergantungan ini yang menjadikan risiko siber sebagai salah satu ancaman yang dapat mengganggu operasional dan kepercayaan nasabah. Berdasarkan hasil studi kasus yang dilakukan terhadap SeaBank Indonesia, ditemukan bahwa terdapat beberapa jenis risiko siber yang dihadapi oleh bank digital, yaitu:

Ancaman Malware dan Phishing

Berdasarkan penelitian yang ditulis oleh (Hafizh et al., 2025) Serangan phishing melibatkan upaya penipuan untuk memperoleh informasi sensitif seperti kredensial login login atau data keuangan melalui email atau situs web yang menipu. Malware seperti trojan, spyware, dan ransomware dapat menyerang sistem perbankan, merusak data atau mencuri informasi sensitif.

Serangan DDoS (Distributed Denial of Service)

Serangan DDoS dapat menyebabkan layanan perbankan digital tidak dapat diakses oleh pengguna. Hal ini sangat merugikan karena akan mengganggu kepercayaan nasabah dan menurunkan performa layanan. Dalam beberapa momen high traffic (seperti saat promo), SeaBank harus meningkatkan sistem proteksi server untuk mencegah potensi overload dan serangan dari pihak luar. Berdasarkan artikel resmi SeaBank Indonesia (2025), bank ini menyoroti pentingnya edukasi kepada nasabah dalam mengenali modus penipuan digital yang semakin canggih. Beberapa modus yang diangkat antara lain undian palsu, investasi bodong, toko online palsu, hingga ajakan mengunduh aplikasi tidak resmi (SeaBank Indonesia, 2025).

Risiko Penyalahgunaan Teknologi *Artificial Intelligence* (AI). Seperti sebelumnya yang dijelaskan SeaBank sangat bergantung pada teknologi seperti *cloud computing* dan juga AI untuk operasionalnya, nah dibalik ketergantungan itu terdapat risiko yang harus dihadapi oleh SeaBank seperti Penyalahgunaan data oleh pihak ketiga, terutama dalam kerja sama dengan vendor teknologi dan Eksploitasi celah keamanan dalam sistem cloud, yang memungkinkan akses tidak sah ke data nasabah. Untuk mengatasi risiko ini, SeaBank telah memperoleh sertifikasi ISO27001, yang menunjukkan komitmen mereka terhadap perlindungan data dan keamanan informasi (SeaBank Indonesia, 2025). Dengan berhasil meraih ISO27001 yang merupakan standar internasional, sistem tersebut dipakai untuk melindungi semua data dan informasi dengan memperhatikan aspek perlindungan nasabah, khususnya keamanan yang berhubungan dengan privasi nasabah di SeaBank. SeaBank juga mengakui bahwa penipuan berbasis AI semakin marak terjadi, termasuk penggunaan teknologi *deepfake* dan *voice cloning* untuk mencuri data nasabah. SeaBank juga telah memberikan edukasi kepada nasabah terkait bagaimana cara menghindari penipuan ini (SeaBank Indonesia, 2025).

Peran Akuntabilitas dalam Mitigasi Risiko Operasional pada SeaBank

SeaBank Indonesia menjalankan prinsip akuntabilitas sebagai bagian inti dari tata kelola perusahaan yang baik (Good Corporate Governance). Akuntabilitas tidak hanya diwujudkan dalam bentuk pelaporan formal kepada regulator seperti OJK, tetapi juga menjadi dasar dalam pengelolaan risiko operasional. Melalui penerapan lima prinsip GCG yaitu transparansi, akuntabilitas, pertanggungjawaban, independensi, dan kewajaran, mengharuskan SeaBank memastikan adanya tanggung jawab yang jelas di seluruh lapisan organisasi. Hal ini diperkuat dengan audit internal rutin yang dilaporkan langsung ke Dewan Komisaris, serta pelaporan berkala dari setiap unit kerja kepada manajemen puncak (**SeaBank Indonesia, 2024**). Dalam praktiknya, SeaBank juga mengimplementasikan sistem manajemen risiko terintegrasi, di mana setiap insiden operasional harus dilaporkan dan ditangani sesuai prosedur. Komitmen ini diperkuat dengan diperolehnya sertifikasi ISO 27001, sebagai bukti kepatuhan terhadap standar internasional dalam pengelolaan keamanan informasi. Selain itu, SeaBank menyediakan akses publik terhadap informasi kinerja dan tata kelola melalui situs resmi sebagai bentuk transparansi dan pertanggungjawaban kepada publik (**SeaBank Indonesia, 2024**).

Namun, sebagai bank digital, SeaBank juga dihadapkan pada sejumlah risiko operasional yang khas. Risiko kebocoran data menjadi perhatian utama, mengingat seluruh data pribadi

nasabah disimpan dan dikelola secara elektronik. SeaBank mengatasi hal ini dengan menerapkan sistem enkripsi end-to-end dan audit berkala (**Angellica, 2023**). Di sisi lain, risiko siber seperti phishing, malware, dan serangan DDoS juga mengancam operasional harian. SeaBank menanggapi ancaman ini dengan meningkatkan perlindungan sistem serta mengedukasi nasabah agar lebih waspada terhadap modus penipuan digital (**SeaBank Indonesia, 2025**). Selain itu, pemanfaatan teknologi kecerdasan buatan (AI) dan cloud computing juga menghadirkan potensi risiko baru, seperti penyalahgunaan data dan eksploitasi celah keamanan oleh pihak ketiga. Sertifikasi ISO 27001 yang dimiliki SeaBank menjadi bukti komitmen terhadap keamanan data dan perlindungan privasi nasabah. Bank ini juga menyadari ancaman teknologi seperti deepfake dan voice cloning, dan secara aktif melakukan edukasi terhadap nasabah sebagai bentuk mitigasi risiko teknologi berbasis AI (**SeaBank Indonesia, 2025**). Secara keseluruhan, SeaBank menunjukkan bahwa akuntabilitas bukan hanya prinsip normatif, tetapi dijalankan secara sistematis dan operasional dalam rangka meminimalkan risiko dan meningkatkan kepercayaan publik terhadap bank digital. Upaya ini menjadikan akuntabilitas sebagai fondasi utama dalam membangun ketahanan dan keberlanjutan operasional perbankan digital di era modern.

SIMPULAN

Penelitian ini menunjukkan bahwa prinsip akuntabilitas memiliki peran krusial dalam mitigasi risiko operasional di SeaBank, terutama dalam aspek keamanan data, risiko siber, dan penyalahgunaan teknologi AI. Melalui penerapan tata kelola perusahaan yang baik (GCG), audit internal, serta sertifikasi ISO 27001, SeaBank memastikan adanya pertanggungjawaban yang jelas di seluruh lapisan organisasi. Saran untuk manajemen agar SeaBank terus menjaga dan meningkatkan proteksi data serta edukasi nasabah untuk menghadapi ancaman digital yang berkembang. Otoritas Jasa Keuangan juga diharapkan memperkuat regulasi perlindungan data bagi bank digital untuk mencegah potensi kebocoran informasi yang merugikan nasabah.

DAFTAR PUSTAKA

- Deloitte. (2023). *The global risk management survey: 12th edition*. Deloitte Insights. https://www2.deloitte.com/content/dam/insights/articles/US103959_Global-risk-management-survey-12ed/DI_Global-risk-management-survey-12ed.pdf
- Hafizh, M. A., Arsyadona, Riski, A. A., Diningrat, T. N., & Sinuraya, A. B. Y. (2025). *Cyber Risk Management Dalam Industri Perbankan Digital*. 15(2), 1–15.
- Harahap, A. M. (2025). *ANALISIS RISIKO DALAM DIGITALISASI PERBANKAN SYARIAH: 10*(204), 686–705.
- Hariwibowo, I. N., & Setiawan, W. Y. (2024). : *Reviu Akuntansi Kontemporer Indonesia BANK : PERILAKU DAN RISIKO FINANSIAL*. 5(2). <https://doi.org/10.30595/ratio.v5i2.21116>
- International Organization for Standardization. (2021). *ISO 37301:2021 – Compliance management systems — Requirements with guidance for use*. ISO. <https://www.iso.org/standard/75080.html>
- Kitsios, F., & Giatsidis, I. (2021). Digital Transformation and Strategy in the Banking Sector: Evaluating the Acceptance Rate of E-Services. *JOITMC*, 7(3), 204. <https://doi.org/10.3390/joitmc7030204>
- Komisioner, D., & Jasa, O. (2021). *PERATURAN OTORITAS JASA KEUANGAN REPUBLIK INDONESIA*.
- Kurniawan, A., Rahayu, A., Wibowo, L. A., & Indonesia, U. P. (2021). *PENGARUH TRANSFORMASI DIGITAL*. 10(2).
- Mentari, M., & Sisdianto, H. (2024). *Teknologi Informasi dan Akuntabilitas Bank Digital*. *Jurnal Akuntansi Digital*, 3(1), 45–58.
- Mursalim, Y., & Junaid, A. (2022). *YUME: Journal of Management Pengaruh Akuntabilitas Keuangan , Pengawasan Keuangan dan Transparansi Anggaran terhadap Pengelolaan Keuangan*. 5(2), 477–494. <https://doi.org/10.37531/yume.vxix.344>
- Nisak, K., & Riza, S. (2023). *Pentingnya Trasparansi Keuangan Negara Dalam Meningkatkan Integritas dan Meminimalisir Tindak Pidana Korupsi di Suatu Negara*. 1, 223–231.
- Otoritas Jasa Keuangan. (2021). *Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021*

tentang Bank Umum. <https://www.ojk.go.id/id/regulasi/Documents/Pages/Bank-Umum/POJK%2012%20-%2003%20-2021.pdf>

SeaBank. (2024). *Laporan Tahunan dan Keberlanjutan 2024 PT Bank Seabank Indonesia (SeaBank)*. 254–451.

SeaBank Indonesia. (2025, April 16). *Wawancara Presdir SeaBank: Rahasia di balik cetak laba dan kejar keberlanjutan*. SeaBank Blog. <https://www.seabank.co.id/blog/wawancara-presdir-seabank-rahasia-di-balik-cetak-laba-dan-kejar-keberlanjutan>

Sheren, A., Sirait, R., Kamalia, A. S., Diska, A., & Legowo, M. B. (2023). *MANAJEMEN RESIKO KEBOCORAN DATA NASABAH DAN SERANGAN SIBER MENGGUNAKAN NIST-RISK*. 144–151.

Sulistiyowati, Rahayu, Y. S., & Naja, C. D. (2023). *PENERAPAN ARTIFICIAL INTELLIGENCE SEBAGAI INOVASI DI ERA DISRUPSI*. 7(2), 117–142.