

Implementasi enterprise risk management (erm) dalam mengelola risiko digital di perbankan syariah era industri 4.0

Muhammad Arifky Wahyudi

Program studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang
e-mail: arifkywahyudi@gmail.com

Kata Kunci:

Enterprise Risk Management, risiko digital, perbankan syariah, industri 4.0, keamanan siber

Keywords:

Enterprise Risk Management, digital risk, Islamic banking, Industry 4.0, cybersecurity

ABSTRAK

Era Industri 4.0 telah mendorong transformasi besar di sektor perbankan, khususnya perbankan syariah, dengan meningkatnya adopsi teknologi digital yang menghadirkan peluang sekaligus risiko baru. Artikel ini bertujuan untuk menganalisis pentingnya penerapan Enterprise Risk Management (ERM) dalam menghadapi risiko digital di perbankan syariah. Dengan menggunakan pendekatan konseptual dan studi pustaka, artikel ini menyoroti bagaimana ERM mampu membantu bank syariah dalam mengidentifikasi, menilai, dan merespons berbagai risiko digital seperti serangan siber, pelanggaran data, hingga tantangan kepatuhan terhadap prinsip syariah. Implementasi ERM berbasis

kerangka COSO mencakup delapan komponen utama yang dapat memperkuat manajemen risiko digital secara menyeluruh dan terintegrasi. Hasil kajian ini menunjukkan bahwa penerapan ERM secara optimal dapat meningkatkan ketahanan operasional, menjaga kepercayaan nasabah, serta memastikan keberlanjutan dan daya saing bank syariah di era digital yang semakin kompleks dan dinamis.

ABSTRACT

The Industrial 4.0 era has driven a massive transformation in the banking sector, especially Islamic banking, through increased adoption of digital technologies that present both opportunities and emerging risks. This article aims to analyze the significance of implementing Enterprise Risk Management (ERM) in addressing digital risks in Islamic banking. Using a conceptual analysis approach combined with literature review, this study highlights how ERM helps Islamic banks identify, assess, and respond to various digital threats, such as cyberattacks, data breaches, and compliance challenges with sharia principles. ERM implementation based on the COSO framework involves eight key components that strengthen digital risk management in an integrated and comprehensive manner. The study concludes that optimal ERM implementation enhances operational resilience, maintains customer trust, and ensures the sustainability and competitiveness of Islamic banks in an increasingly complex and dynamic digital environment.

Pendahuluan

Era keempat (4.0) yang dimulai pada awal abad ke-21 mengintegrasikan teknologi digital, fisik, dan biologis. Kehadiran Internet of Things (IoT), kecerdasan buatan (AI), machine learning, big data, dan berbagai teknologi canggih lainnya telah mendorong transformasi besar dalam industri dan kehidupan masyarakat. Industri 4.0 menyatukan sistem fisik dan digital untuk menciptakan 'pabrik pintar' serta mengoptimalkan proses produksi dan pengelolaan sumber daya (Rafidah & Maharani, 2024). Teknologi



This is an open access article under the [CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/) license.

Copyright © 2023 by Author. Published by Universitas Islam Negeri Maulana Malik Ibrahim Malang.

memainkan peran penting dalam setiap lini kehidupan. Era industri 4.0 ditandai dengan proses digitalisasi, yaitu pemanfaatan teknologi secara menyeluruh. Menurut (Anis et al., 2022) Industri 4.0 mencakup lima aspek utama, yaitu Artificial Intelligence (AI), Internet of Things (IoT), antarmuka manusia-mesin, teknologi robotik dan sensor, serta teknologi percetakan tiga dimensi (3D). Kelima teknologi tersebut menunjukkan bahwa industri di era ini mulai memasuki dunia virtual dan mengandalkan mesin-mesin otomatis yang terintegrasi dengan internet

Era Industri 4.0 membawa transformasi besar yang memengaruhi hampir seluruh aspek kehidupan, terutama dalam industri perbankan yang mengandalkan teknologi digital dan koneksi internet (Tambunan & Padli Nasution, 2022). Pemanfaatan teknologi telah membawa perubahan besar dalam industri perbankan. Ada empat aspek utama yang mendorong pergeseran lanskap perbankan di masa depan. Pertama, ekspektasi konsumen kini lebih tinggi karena mereka menginginkan layanan yang praktis, aman, personal, dan mengikuti tren. Kedua, penggunaan big data memungkinkan bank menciptakan layanan yang lebih tepat sasaran dan membuka peluang bisnis baru. Ketiga, munculnya kemitraan dengan perusahaan besar dan start-up digital menciptakan ekosistem baru di mana kolaborasi dengan fintech dan bigtech membantu bank menjangkau lebih banyak nasabah dan mengembangkan layanan. Keempat, bank dituntut bertransformasi menjadi digital sepenuhnya agar bisa lebih efisien, menjangkau masyarakat luas, dan tetap kompetitif dan berkelanjutan di tengah persaingan industri keuangan yang kian ketat (Ngamal & Maximus Ali Perajaka, 2021).

Transformasi digital di sektor perbankan kini menjadi respons atas hadirnya fintech dan revolusi Industri 4.0. Perkembangan ini menandai masuknya perbankan ke era layanan digital yang bertujuan memperluas inklusi keuangan dan memudahkan akses layanan tanpa batas waktu dan tempat. Awalnya hanya menawarkan fitur dasar, perbankan digital kini mencakup berbagai layanan seperti pembukaan rekening, investasi, tarik tunai tanpa kartu, hingga belanja. Digitalisasi ini penting untuk meningkatkan kepuasan nasabah, yang menjadi kunci dalam industri perbankan. Jika ekspektasi mereka tidak terpenuhi nasabah bisa berpindah ke bank lain. Oleh karena itu, bank syariah harus terus berinovasi agar tetap relevan di era digital (Husni Shabri, 2022). Enterprise Risk Management (ERM) dan transformasi digital berperan penting dalam keberlanjutan perbankan, karena keduanya membantu mengelola risiko dan mendukung kelangsungan jangka Panjang (Wahyuningsih et al., 2024). ERM dapat membantu dalam mengidentifikasi, mengendalikan, dan meminimalkan risiko agar tidak melebihi kapasitas yang dimiliki, sehingga keberlangsungan operasional tetap terjaga. Mengingat masa depan penuh ketidakpastian, pengelolaan risiko yang baik sangat dibutuhkan terutama dalam perbankan syariah. Hal ini agar perbankan syariah dapat menghadapi tantangan dengan bijak dan menjaga kepercayaan dengan nasabah (Naibaho et al., 2024)

Artikel ini bertujuan untuk memberikan pemahaman yang komprehensif mengenai pentingnya penerapan Enterprise Risk Management (ERM) sebagai strategi utama dalam memperkuat manajemen risiko digital di sektor perbankan syariah. Seiring dengan pesatnya perkembangan teknologi pada era Industri 4.0 dan semakin meluasnya digitalisasi layanan keuangan bank syariah dituntut untuk tidak hanya

berinovasi, tetapi juga mampu mengantisipasi dan mengelola berbagai risiko digital yang muncul.

Metode analisis yang digunakan pada artikel ini adalah pendekatan analisis konseptual yang dikombinasikan dengan studi pustaka. Analisis konseptual digunakan untuk memahami secara lebih mendalam tentang konsep Enterprise Risk Management (ERM) dan risiko digital dalam dunia perbankan Syariah khususnya di era digital seperti sekarang. Pendekatan ini membantu penulis menelaah bagaimana ERM dapat menjadi strategi penting dalam menghadapi berbagai tantangan digital. Sementara itu, studi pustaka dilakukan dengan membaca dan mengkaji berbagai referensi, seperti jurnal, buku, dan laporan penelitian yang relevan. Dengan menggabungkan kedua pendekatan ini, artikel ini berusaha memberikan gambaran yang jelas dan menyeluruh mengenai pentingnya penguatan manajemen risiko digital di perbankan syariah melalui penerapan ERM.

Pembahasan

Konsep Enterprise Risk Management

Enterprise Risk Management (ERM) adalah pendekatan manajemen yang dijalankan secara sistematis dan menyeluruh untuk mengelola berbagai risiko yang mungkin muncul. Tujuannya adalah memberikan keyakinan bahwa operasional perusahaan berjalan aman dan terkendali sehingga terhindar dari potensi kerugian yang bisa mengganggu stabilitas dan keberlanjutan usaha. Dengan ERM perusahaan dapat lebih siap menghadapi ketidakpastian dan mengambil keputusan secara lebih bijak (Saputra et al., 2023). ERM juga dapat dikatakan suatu proses yang melibatkan manajemen, dewan direksi, dan seluruh elemen organisasi. Proses ini dijalankan sebagai bagian dari perumusan strategi dan mencakup seluruh aspek dalam organisasi. Tujuan utamanya adalah untuk mengenali berbagai peristiwa yang berpotensi menimbulkan risiko, mengelola risiko tersebut secara terarah, serta memberikan keyakinan yang cukup bahwa tujuan organisasi dapat tercapai. Dengan penerapan ERM, organisasi dapat lebih proaktif dalam menghadapi ketidakpastian dan menjaga stabilitas operasional secara berkelanjutan (Iswajuni et al., 2018).

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) merilis edisi terbaru dari Enterprise Risk Management Integrated Framework pada Juni 2016 melalui tahap public exposure. Kerangka ini menekankan bahwa setiap aktivitas bisnis pasti mengandung ketidakpastian yang berpotensi menimbulkan risiko. Oleh karena itu, pengelolaan risiko perlu dilakukan secara menyeluruh dan terintegrasi dan bukan secara terpisah. Contohnya risiko hukum yang dihadapi perusahaan tidak hanya berdampak secara langsung tetapi juga dapat merusak reputasi perusahaan yang pada akhirnya mempengaruhi nilai sahamnya di pasar modal (Saputra et al., 2023). Menurut COSO ERM (2004), manajemen risiko mencakup delapan komponen utama yang saling berkaitan dan membentuk proses terpadu. Berikut penjelasan tiap komponennya:

Lingkungan Internal (Internal Environment)

Organisasi membentuk lingkungan internal yang memberikan warna serta arah terhadap cara pandang seluruh anggotanya dalam menghadapi risiko. Dalam komponen

ini, manajemen menetapkan filosofi manajemen risiko, risk appetite, nilai etika, integritas, serta menciptakan lingkungan operasional yang mendukung semuanya.

Penetapan Tujuan (Objective Setting)

Manajemen harus terlebih dahulu menetapkan tujuan organisasi sebelum mereka dapat mengidentifikasi potensi kejadian yang memengaruhi pencapaian tujuan tersebut. Melalui ERM, manajemen memastikan proses penetapan tujuan selaras dengan misi perusahaan dan sesuai dengan risk appetite yang telah ditentukan. Tujuan ini mencakup tujuan strategis, operasional, dan pelaporan.

Identifikasi Risiko (Event Identification)

Manajemen mengidentifikasi kejadian-kejadian potensial baik dari lingkungan internal maupun eksternal yang dapat memengaruhi strategi atau pencapaian tujuan organisasi. Kejadian tersebut bisa berdampak positif (peluang) atau negatif (risiko). Identifikasi dapat dilakukan dengan menganalisis tren atau kejadian historis.

Penilaian Risiko (Risk Assessment)

Manajemen menilai sejauh mana suatu kejadian dapat berdampak terhadap pencapaian tujuan. Mereka menganalisis besar kecilnya risiko berdasarkan risiko melekat (inherent) dan risiko tersisa (residual), dengan mempertimbangkan dua aspek utama: kemungkinan (likelihood) dan dampak (consequence). Besarnya risiko dihitung dengan mengalikan kedua aspek tersebut.

Perlakuan Risiko (Risk Response)

Setelah menilai risiko, manajemen menentukan langkah yang tepat sebagai tanggapan. Tanggapan tersebut dapat berupa: 1) Avoidance, menghentikan aktivitas yang menyebabkan risiko; b) Reduction, mengurangi kemungkinan atau dampak risiko; c) Sharing, membagi risiko dengan pihak lain; d) Acceptance, menerima risiko terutama jika risikonya kecil dan tidak memerlukan tindakan khusus.

Aktivitas Pengendalian (Control Activities)

Manajemen menyusun kebijakan dan prosedur untuk memastikan tanggapan risiko dapat terlaksana secara efektif. Mereka menciptakan lingkungan pengendalian yang mencakup nilai integritas dan etika, kompetensi, kebijakan SDM, budaya organisasi, filosofi kepemimpinan, struktur organisasi, serta pembagian wewenang dan tanggung jawab.

Informasi dan Komunikasi (Information and Communication):

Manajemen menyampaikan informasi yang relevan kepada pihak-pihak terkait melalui saluran komunikasi yang sesuai. Mereka memastikan kualitas informasi, arah komunikasi (horizontal maupun vertikal), serta efektivitas media komunikasi yang digunakan.

Pemantauan (Monitoring)

Manajemen melakukan pemantauan secara berkelanjutan (ongoing) dan periodik (separate evaluation). Mereka menjalankan aktivitas seperti supervisi, rekonsiliasi, serta pengawasan rutin lainnya untuk menilai efektivitas seluruh komponen ERM. Setiap

komponen memiliki pernyataan yang menjelaskan fungsinya dalam kerangka ERM secara keseluruhan, dengan total 108 pernyataan yang digunakan sebagai acuan penilaian.

Penerapan ERM memberikan panduan menyeluruh bagi seluruh elemen organisasi dalam mengelola risiko secara terintegrasi khususnya dalam menghadapi masa depan yang penuh ketidakpastian. Dengan penerapan ERM yang optimal perusahaan memiliki peluang besar untuk meningkatkan kinerja keuangannya secara signifikan. Bagi perbankan syariah di tengah arus disrupsi dan tantangan digital yang terus berkembang diperlukan strategi yang tidak hanya melindungi kelangsungan usaha tetapi juga tetap selaras dengan prinsip-prinsip syariah. Di sinilah peran penting ERM muncul sebagai sistem yang tidak hanya mengelola risiko tetapi juga menjaga agar seluruh langkah bank tetap berada di jalur yang baik secara bisnis maupun nilai-nilai Islam (Hidayat & Mukhlisin, 2019).

Metode tradisional dalam manajemen risiko tidak lagi memadai untuk menghadapi karakteristik risiko yang terus berkembang. Maka dari itu, dengan menerapkan ERM perusahaan secara aktif membangun ketahanan terhadap kegagalan sistematis dan memantau berbagai peluang untuk mengurangi risiko secara menyeluruh (Shad et al., 2019). Para ahli meyakini bahwa penerapan ERM secara optimal mampu mendorong peningkatan kinerja, yang pada akhirnya akan meningkatkan nilai serta memperpanjang umur perusahaan (Phan et al., 2020). Para peneliti dan praktisi mulai memanfaatkan Enterprise Risk Management (ERM) sebagai solusi untuk mengatasi kelemahan dalam manajemen risiko tradisional. Meskipun penelitian tentang efektivitas dan manfaat ERM masih terbatas, minat terhadap konsep ini terus meningkat. Saat ini, mereka secara aktif mengeksplorasi cara-cara baru dan lebih efektif dalam mengelola risiko serta menggali manfaat yang dapat diperoleh dari penerapan ERM (Sitinjak & Nibras Anny Khabibah, 2023).

Peneliti, seperti Indra Saputra et al. (2023), telah banyak meneliti penerapan Enterprise Risk Management (ERM) di sektor keuangan. Mereka menemukan bahwa ERM berpengaruh positif dan signifikan terhadap penilaian keberlanjutan perbankan. Artinya, bank secara aktif menerapkan ERM sebagai strategi utama untuk mendukung keberlanjutan. Hal ini sejalan dengan peta jalan keuangan berkelanjutan yang dirancang oleh Otoritas Jasa Keuangan (OJK). Dalam konteks era digital, penerapan ERM juga membantu perbankan menghadapi risiko digital, seperti serangan siber, kebocoran data, dan gangguan sistem teknologi, sehingga menjadikan sistem keuangan lebih tangguh dan berkelanjutan.

Risiko Digital dalam Perbankan Syariah

Dalam era digital, sektor perbankan mengalami transformasi signifikan melalui adopsi teknologi informasi. Namun, kemajuan ini juga menimbulkan berbagai tantangan dan risiko digital yang kompleks. Terdapat beberapa risiko digital dalam perbankan syariah:

Risiko keamanan cyber (cybersecurity risk)

Kejahatan siber terus mengancam perbankan syariah di era digital. Pelaku memanfaatkan teknologi dan jaringan komputer untuk mencuri data, meretas sistem,

melakukan penipuan online, dan menyebarkan malware. Tindakan ini merugikan bank maupun nasabah. Oleh karena itu, bank syariah perlu memahami jenis-jenis kejahatan siber agar dapat melindungi sistem dan menjaga integritas informasi keuangan (Jakobsson, 2020). Pencurian data merupakan salah satu kejahatan siber yang umum terjadi. Pelaku biasanya menyasar informasi sensitif seperti nomor kartu kredit, data keuangan, dan identitas pribadi nasabah untuk melakukan penipuan atau menjualnya ke pihak tak bertanggung jawab. Kejahatan ini bisa merusak reputasi bank syariah dan merugikan nasabah secara finansial. Selain itu, peretas juga sering membobol sistem perbankan dengan keahlian teknis mereka untuk mencuri dana, memanipulasi transaksi, atau merusak infrastruktur digital. Serangan ini dapat mengganggu layanan perbankan dan memperburuk kepercayaan publik (Faizal et al., 2023).

Pelaku siber menggunakan jaringan komputer atau telekomunikasi untuk meluncurkan ancaman yang menyasar berbagai elemen, seperti situs web, sistem komputer, dan perangkat pribadi. Pelaku serangan siber sering menyasar spionase industri dan target-target pemerintah, yang memicu kekhawatiran serta ketegangan akibat risiko kebocoran data pribadi dan aset berharga. Selain itu, mereka juga memanfaatkan serangan siber sebagai alat politik di dunia maya maupun sebagai instrumen dalam konteks ekonomi. Pihak yang tidak bertanggung jawab sering mencoba mengakses, merusak, atau mencuri data dan informasi penting dari sistem perbankan digital, sehingga menimbulkan risiko keamanan siber (Fatmala Putri & Ratna Sari, 2023). Gani (2023) menambahkan bahwa serangan siber secara nyata mengancam stabilitas keuangan. Serangan siber yang berhasil mengganggu fungsi operasional lembaga keuangan, merusak integritas data, dan pada akhirnya mengikis kepercayaan masyarakat terhadap sistem perbankan.

Risiko pelanggaran data dan pencurian identitas nasabah

Pelanggaran data dapat terjadi karena serangan siber, kebocoran, atau penyalahgunaan oleh pihak internal. Penyerang sering mengeksploitasi celah sistem atau menggunakan phishing dan malware untuk mencuri data sensitif nasabah. Kesalahan manusia, seperti kehilangan perangkat atau kelalaian dalam mengelola data, juga bisa menyebabkan kebocoran. Dampaknya meliputi kerugian finansial, rusaknya reputasi bank syariah, dan pelanggaran privasi. Sementara itu, pencurian identitas terjadi saat pelaku memakai data pribadi seperti nama atau nomor identitas untuk penipuan. Mereka kerap menggunakan email atau situs palsu untuk menipu nasabah, atau memanfaatkan malware serta kebocoran data dalam sistem bank (Faizal et al., 2023). Jika terjadi pencurian data nasabah maka sebagaimana yang diatur dalam Pasal 4 UUPK yang di dalamnya memberikan hak kepada nasabah yang dirugikan untuk menuntut kompensasi, ganti rugi, atau penggantian atas layanan yang tidak sesuai dengan janji. Pelanggaran ini mencerminkan bentuk risiko digital dalam perbankan syariah, khususnya terkait ancaman terhadap keamanan data akibat serangan siber. UUPK Pasal 7 huruf D dan G juga mewajibkan bank untuk menjamin mutu layanan sesuai standar yang berlaku dan memberikan ganti rugi atas kerugian yang dialami nasabah. Oleh karena itu, bank syariah harus melaksanakan standarisasi keamanan digital secara optimal sebagai bentuk tanggung jawab dalam menghadapi risiko digital (Fatmala Putri & Ratna Sari, 2023).

Risiko Kepatuhan (Compliance)

Risiko digital dalam perbankan syariah dapat muncul ketika bank tidak mematuhi regulasi yang berlaku, baik dari regulator seperti Bank Indonesia maupun prinsip-prinsip syariah. Ketidakpatuhan ini bisa terjadi jika bank syariah menerapkan teknologi digital atau sistem informasi yang tidak sejalan dengan nilai-nilai syariah. Ketika sistem digital yang digunakan bertentangan dengan prinsip syariah, hal ini dapat menimbulkan ketidakseimbangan dalam proses operasional dan menurunkan kepercayaan nasabah. Selain itu, ketidakpatuhan juga memperbesar potensi terjadinya berbagai risiko digital lainnya, seperti penyalahgunaan data, pelanggaran etika syariah, dan kerugian sistemik yang mempengaruhi stabilitas layanan perbankan (Rianto, 2013)

Risiko Operasional

Risiko digital dalam perbankan syariah di bidang operasional dapat terjadi akibat kesalahan manusia maupun kegagalan sistem. Pegawai atau pihak tidak bertanggung jawab bisa saja melakukan tindakan kejahatan digital seperti peretasan (hacking), penyebaran spyware, cracking, hingga sabotase (Rahmawati, 2017). Di sisi lain, sistem juga bisa mengalami gangguan seperti kesalahan jaringan, error pada perangkat lunak, atau gangguan koneksi internet. Untuk mengatasi hal ini, bank syariah perlu memperkuat sistem operasional digital mereka guna meminimalisir potensi kejahatan digital dan mencegah kegagalan sistem yang dapat mengganggu layanan kepada nasabah (Rianto, 2013).

Tantangan Perbankan Syariah di Era Industri 4.0 dalam Menghadapi Risiko Digital

(Restika & Sonita, 2023) menyebutkan terdapat beberapa tantangan yang di hadapi perbankan syariah dalam menghadapi risiko digital, yaitu:

Serangan phishing and social engineering

Pelaku kejahatan siber sering kali melancarkan serangan phishing dan social engineering dengan memanipulasi psikologis nasabah atau karyawan untuk mendapatkan informasi rahasia. Ketika serangan ini berhasil, reputasi bank bisa rusak dan dana nasabah berisiko hilang.

Malware dan Ransomware

Serangan malware dan ransomware yang terus mengintai ini dapat mencuri data keuangan, mengunci sistem operasional, dan bahkan memaksa bank membayar tebusan untuk memulihkan akses. Ketiga, bank syariah harus menjaga keseimbangan antara menjaga keamanan siber dan mematuhi prinsip syariah. Jika bank melanggar prinsip-prinsip ini, kepercayaan nasabah bisa terganggu dan stabilitas keuangan terancam.

Tantangan kepatuhan syariah

Bank syariah harus menjaga keseimbangan antara menjaga keamanan siber dan mematuhi prinsip syariah. Ketika bank melanggar norma dan etika Islam, mereka berisiko merusak citra lembaga dan kehilangan kepercayaan nasabah yang menjadi fondasi utama stabilitas keuangan syariah.

Ketidakpastian hukum dan regulasi

Bank syariah juga harus menyesuaikan diri dengan regulasi yang terus berubah. Ketika bank terlambat mematuhi standar keamanan siber yang berlaku, mereka bisa terkena sanksi hukum dan kehilangan reputasi.

Kurangnya kesadaran keamanan

Kurangnya pemahaman terhadap risiko siber dari pihak internal maupun eksternal memperbesar potensi pelanggaran keamanan. Karyawan dan nasabah yang belum teredukasi bisa menjadi celah bagi pelaku kejahatan untuk menyusup ke sistem bank.

Pengelolaan identitas dan akses yang tidak efektif

Bank yang tidak mengelola identitas dan akses secara efektif membuka peluang bagi pihak tidak berwenang untuk masuk ke dalam sistem dan mencuri data penting. Akses ilegal ini bisa menyebabkan pencurian identitas, penipuan, atau pengambilalihan dana nasabah.

Tantangan teknologi finansial

Bank syariah yang berupaya berintegrasi dengan layanan fintech modern sering menghadapi risiko baru terkait keamanan siber. Jika proses integrasi tidak dilakukan dengan aman, kebocoran data atau kegagalan sistem dapat terjadi dan mengancam kepercayaan publik terhadap bank.

Implementasi ERM di Perbankan Syariah dalam Menghadapi Risiko Digital

Implementasi ERM pada bank syariah dalam menghadapi risiko digital dapat dilakukan dengan beberapa cara. Menurut COSO ERM (2004) terdapat delapan komponen yang dapat dijadikan sebagai dasar implementasi ERM dalam perbankan syariah, khususnya dalam menghadapi risiko digital, yaitu:

Membangun Lingkungan Internal yang Kuat

Manajemen bank syariah menetapkan filosofi manajemen risiko yang berlandaskan prinsip syariah. Mereka membangun budaya kerja yang menjunjung integritas, serta menetapkan selera risiko (risk appetite) yang mencakup risiko teknologi seperti cyber risk, risiko data breach, dan gangguan sistem layanan digital. Risk appetite akan berperan dalam membantu bank membuat keputusan yang lebih baik (Putri, 2023).

Menetapkan Tujuan Strategis dan Operasional

Manajemen menetapkan tujuan strategis yang mencakup transformasi digital, keamanan sistem IT, dan peningkatan pelayanan digital. Mereka memastikan bahwa tujuan-tujuan tersebut sejalan dengan misi syariah dan berada dalam batas risiko yang dapat diterima (risk appetite)

Mengidentifikasi Risiko Digital

Tim manajemen risiko secara aktif mengidentifikasi potensi risiko digital dari lingkungan internal seperti kesalahan sistem, dan eksternal seperti serangan siber. Mereka memanfaatkan tren historis, audit teknologi, dan hasil evaluasi insiden sebelumnya untuk mengenali berbagai bentuk ancaman digital

Melakukan Penilaian Risiko secara Menyeluruh

Manajemen menganalisis kemungkinan dan dampak dari setiap risiko digital. Mereka menghitung besarnya risiko berdasarkan tingkat kemungkinan serangan siber dan dampaknya terhadap layanan seperti mobile banking, internet banking, dan integritas data nasabah.

Merancang Tanggapan Risiko yang Efektif

Setelah melakukan penilaian, manajemen menentukan langkah mitigasi. Mereka menghindari penggunaan teknologi yang rentan (avoidance), mengimplementasikan firewall dan sistem deteksi intrusi (reduction), mengasuransikan infrastruktur digital (sharing), atau menerima risiko kecil dengan monitoring ketat (acceptance).

Menerapkan Aktivitas Pengendalian Manajemen

Menyusun kebijakan keamanan data dan prosedur IT untuk mengurangi risiko digital. Mereka menetapkan kontrol akses, otorisasi transaksi digital, serta pemisahan fungsi antara pengembangan sistem dan operasional harian. Prosedur ini dituangkan dalam kebijakan keamanan informasi syariah.

Meningkatkan Informasi dan Komunikasi Risiko

Bank syariah mengembangkan saluran komunikasi dua arah antara manajemen, karyawan, dan pihak regulator. Mereka menyebarluaskan informasi mengenai risiko digital dan kebijakan penanganannya secara cepat dan transparan. Selain itu, pelaporan insiden digital dilakukan secara berkala kepada pimpinan.

Melaksanakan Pemantauan Berkala

Tim audit internal dan divisi manajemen risiko secara rutin memantau efektivitas kontrol digital. Mereka mengevaluasi prosedur keamanan informasi, melakukan uji coba simulasi serangan siber, dan memperbarui sistem berdasarkan rekomendasi audit serta perubahan teknologi.

Kesimpulan

Perbankan syariah harus secara proaktif menghadapi risiko digital yang muncul akibat transformasi teknologi di era Industri 4.0. Enterprise Risk Management (ERM) berperan sebagai strategi utama dalam memperkuat sistem manajemen risiko digital secara menyeluruh dan terintegrasi. Dengan menerapkan delapan komponen ERM berdasarkan kerangka COSO, bank syariah dapat menetapkan tujuan strategis, mengidentifikasi risiko, menilai dampaknya, serta merancang respons yang tepat terhadap ancaman seperti serangan siber, pencurian data, dan pelanggaran prinsip syariah. Penerapan ERM juga mampu meningkatkan efisiensi operasional, menjaga integritas layanan digital, dan membangun kepercayaan nasabah. Oleh karena itu, membangun budaya risiko yang kuat, meningkatkan literasi keamanan digital, dan memperkuat koordinasi lintas fungsi menjadi langkah penting agar perbankan syariah dapat bertahan dan bersaing secara berkelanjutan di tengah disrupsi teknologi.

Daftar Pustaka

- Anis, M. Z. A., Mardiani, F., & Fathurrahman, F. (2022). Digital History dan Kesiapan Belajar Sejarah di Era Revolusi 4.0. *Fajar Historia: Jurnal Ilmu Sejarah Dan Pendidikan*, 6(1), 29–42. <https://doi.org/10.29408/fhs.v6i1.4375>
- COSO. (2004). Enterprise Risk Management – Integrated Framework. Komite Nasional Kebijakan Governance (KNKG). Pedoman Penerapan Manajemen Risiko Berbasis Governance. 2011.
- 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>
- Fatmala Putri, D., & Ratna Sari, W. (2023). Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *Jurnal Ilmiah Ekonomi Dan Manajemen*, 1(4), 173–181. <https://doi.org/10.61722/jiem.v1i4.331>
- Gani, T. A. 2023. “Kedaulatan Data Digital Untuk Integritas Bangsa.” Yiah Kuala University Press
- Hidayat, E. K. P., & Mukhlisin. (2019). Studi Sektor Perbankan Tentang Enterprise Risk Management, It Governance, Financial Performance Dan Firm Value. *Prosiding Working Papers Series In Management*, 11(2), 85–104. <https://doi.org/10.25170/wpm.v11i2.4507>
- Husni Shabri. (2022). Transformasi Digital Industri Perbankan Syariah Indonesia. *El-Kahfi | Journal of Islamic Economics*, 3(02), 1–7. <https://doi.org/10.58958/elkahfi.v3i02.88>
- Indra Saputra, Etty Murwaningsari, & Yvonne Augustine. (2023). The Role of Enterprise Risk Management And Digital Transformation On Sustainable Banking In Indonesia. *Neo Journal of Economy and Social Humanities (NEJESH)*, 2(1).
- Iswajuni, I., Soetedjo, S., & Manasikana, A. (2018). Pengaruh Enterprise Risk Management (Erm) Terhadap Nilai Perusahaan Pada Perusahaan Manufaktur Yang Terdaftar Di Bursa Efek. *Journal of Applied Managerial Accounting*, 2(2), 275–281. <https://doi.org/10.30871/jama.v2i2.942>
- Jakobsson, M., & Myers, S. (2020.). Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft. www.swsec.
- Naibaho, D., Sipayung, F., Simbolon, B. A. J., Ratna, R., & Simanjuntak, D. (2024). Analisis Implementasi Enterprise Risk Management dan Nilai Perusahaan. *Journal of Economics and Business UBS*, 13(2), 689–700. <https://doi.org/10.52644/joeb.v13i2.1582>
- Ngamal, Y., & Maximus Ali Perajaka. (2021). Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, 2(2), 59–74. <https://doi.org/10.33541/mr.v2iiv.4099>

- Putri, L. T. (2023). Analisis pengaruh kemelekan keuangan syariah dan Risk Appetite terhadap minat mahasiswa untuk berinvestasi : Studi pada mahasiswa Kota Malang. 1(4), 505–511.
- Phan, T. D., Dang, T. H., Nguyen, T. D. T., Ngo, T. T. N., & Hoang, T. H. Le. (2020). The effect of enterprise risk management on firm value: Evidence from Vietnam industry listed enterprises. *Accounting*, 6(4). <https://doi.org/10.5267/j.ac.2020.4.011>
- Rafidah, A. S., & Maharani, H. N. (2024). Inovasi dan Pengembangan Produk Keuangan Syariah: Tantangan dan Prospek Era Revolusi Industri 4.0. *Jurnal Ilmiah Edunomika*, 8(1), 1–14. <https://jurnal.stie-aas.ac.id/index.php/jie/article/view/11649>
- Rahmawati, I. (2017). The analysis of cyber crime threat risk management to increase cyber defense analisis manajemen risiko ancaman kejahatan siber (cyber crime) dalam peningkatan cyber defense. | *Journal of Defense & State Defense*, 7(2), 55–70.
- Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital. *Krigan: Journal of Management and Sharia Business*, 1(2), 25. <https://doi.org/10.30983/krigan.v1i2.7929>
- Rianto, R. B. (2013). *Manajemen Risiko Perbankan Syariah di Era Digital*. 2(5), 444.
- Saputra, E. A., Widya Pitaloka, S., & Hanesti, E. M. (2023). Analisis Penerapan Enterprise Risk Management Terhadap Risiko Produk Halal Dimsho Tiga Naga Merr. *JEB 17 Jurnal Ekonomi & Bisnis*, 8(2), 161–174.
- Shad, M. K., Lai, F. W., Fatt, C. L., Klemeš, J. J., & Bokhari, A. (2019). Integrating sustainability reporting into enterprise risk management and its relationship with business performance: A conceptual framework. *Journal of Cleaner Production*, 208. <https://doi.org/10.1016/j.jclepro.2018.10.120>
- Sitinjak, J., & Nibras Anny Khabibah. (2023). Literatur Review Manfaat Dari Enterprise Risk Management Di Indonesia. *Jurnal Ekonomi STIEP*, 8(1), 92–100. <https://doi.org/10.54526/jes.v8i1.137>
- Tambunan, R. T., & Padli Nasution, M. I. (2022). Tantangan dan Strategi Perbankan Dalam Menghadapi Perkembangan Transformasi Digitalisasi di Era 4.0. *Sci-Tech Journal*, 2(2), 148–156. <https://doi.org/10.56709/stj.v2i2.75>
- Wahyuningsih, S., Jasmin, J., & Juwono, E. (2024). Peran Strategi Manajemen Risiko dalam Mengoptimalkan Likuiditas dan Meminimalkan Risiko Kredit di Industri Perbankan di Indonesia. *Sanskara Manajemen Dan Bisnis*, 2(03), 156–167. <https://doi.org/10.58812/smb.v2i03.420>