

EVALUASI AUDIT SISTEM INFORMASI MENGENAI TATA KELOLA TEKNOLOGI INFORMASI PADA INDUSTRI PERBANKAN

¹Liza Audia Zahra, ²Dinda Aulia Putri, ³Ninda Clarica

^{1,2,3}Sistem Informasi, STMIK Kaputama Binjai

E-mail: lizaaudia01@gmail.com, dindaauliaputri@gmail.com,
nindaclarica@gmail.com

ABSTRAK - Penelitian ini bertujuan untuk mengevaluasi audit sistem informasi terkait tata kelola teknologi informasi (IT governance) pada industri perbankan di Indonesia. Seiring dengan pesatnya perkembangan teknologi, sektor perbankan menghadapi tantangan dalam memastikan bahwa pengelolaan teknologi informasi dilakukan dengan efektif, efisien, dan mematuhi standar internasional guna mendukung operasional dan pelayanan kepada nasabah. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus yang melibatkan beberapa bank di Indonesia. Data dikumpulkan melalui wawancara dengan praktisi TI, analisis dokumen kebijakan dan prosedur TI, serta observasi langsung terhadap implementasi sistem TI di bank-bank tersebut. Hasil penelitian menunjukkan bahwa meskipun kebijakan dan prosedur pengelolaan TI sudah diterapkan dengan baik, terdapat beberapa area yang perlu ditingkatkan, terutama dalam hal pengelolaan risiko TI dan keterampilan sumber daya manusia dalam mengelola sistem TI yang semakin kompleks. Beberapa temuan penting dari penelitian ini adalah bahwa meskipun bank-bank yang diteliti telah mengikuti standar internasional seperti ISO 27001 dan COBIT, penerapan standar ini belum sepenuhnya konsisten di seluruh bagian organisasi. Selain itu, meskipun kontrol internal dan audit dilakukan secara teratur, terdapat kelemahan dalam pengawasan terhadap sistem TI yang lebih canggih dan berisiko tinggi, seperti sistem perbankan online dan aplikasi mobile banking. Berdasarkan temuan ini, disarankan agar bank-bank lebih fokus pada penerapan strategi manajemen risiko TI yang lebih proaktif, memperkuat pengawasan terhadap sistem TI yang lebih modern, serta meningkatkan kompetensi sumber daya manusia yang terlibat dalam pengelolaan dan pengawasan sistem informasi. Penelitian ini memberikan rekomendasi untuk penguatan tata kelola TI guna mendukung efisiensi operasional dan mitigasi risiko yang lebih baik dalam sektor perbankan.

Kata Kunci: Audit Sistem Informasi, Tata Kelola Teknologi Informasi, IT Governance, Industri Perbankan, Manajemen Risiko TI, COBIT, ISO 27001.

ABSTRACT - This study aims to evaluate the information systems audit related to information technology governance (IT governance) in the banking industry in Indonesia. With the rapid development of technology, the banking sector faces

challenges in ensuring that information technology management is conducted effectively, efficiently, and in compliance with international standards to support operations and services to customers. This research uses a qualitative approach with a case study method involving several banks in Indonesia. Data were collected through interviews with IT practitioners, document analysis of IT policies and procedures, and direct observation of the implementation of IT systems at these banks. The results of the study show that although IT management policies and procedures have been well implemented, there are several areas that need improvement, particularly in the management of IT risks and the skills of human resources in managing increasingly complex IT systems. Key findings from this research indicate that although the banks studied have adhered to international standards such as ISO 27001 and COBIT, the application of these standards has not been fully consistent across all parts of the organization. Additionally, although internal controls and audits are conducted regularly, there are weaknesses in overseeing more advanced and high-risk IT systems, such as online banking systems and mobile banking applications. Based on these findings, it is recommended that banks focus more on implementing proactive IT risk management strategies, strengthen oversight of modern IT systems, and enhance the competencies of human resources involved in the management and oversight of information systems. This study provides recommendations for strengthening IT governance to support operational efficiency and better risk mitigation in the banking sector.

Keywords: Information Systems Audit, Information Technology Governance, IT Governance, Banking Industry, IT Risk Management, COBIT, ISO 27001.

PENDAHULUAN

Industri perbankan telah mengalami transformasi digital yang pesat dalam beberapa dekade terakhir, di mana teknologi informasi (TI) menjadi salah satu elemen penting dalam mendukung operasional dan pelayanan kepada nasabah (Nicholas et al., 2024). Dengan adanya perkembangan teknologi, sektor perbankan tidak hanya mengandalkan sistem manual, tetapi lebih banyak mengintegrasikan berbagai sistem berbasis digital yang memungkinkan bank untuk memberikan layanan yang lebih cepat, efisien, dan transparan. Hal ini menjadikan TI sebagai salah satu aset strategis yang sangat penting dalam sektor perbankan.

Transformasi digital dalam perbankan mencakup berbagai inovasi, mulai dari penerapan sistem perbankan elektronik, mobile banking, hingga penggunaan teknologi canggih seperti big data, artificial intelligence (AI), dan blockchain. Penggunaan teknologi ini memungkinkan bank untuk meningkatkan kualitas layanan, mempercepat proses transaksi, serta meningkatkan kemampuan analisis untuk mengambil keputusan yang lebih tepat dalam menghadapi dinamika pasar

dan kebutuhan nasabah. Bank-bank besar dan kecil di seluruh dunia telah mengadopsi berbagai solusi teknologi untuk meningkatkan daya saing mereka, serta memberikan pengalaman yang lebih baik bagi para nasabah (Sinaga & Permana, 2023).

Seiring dengan pesatnya perkembangan teknologi, tantangan dalam pengelolaan TI di sektor perbankan semakin kompleks (Nicholas et al., 2024). Bank tidak hanya perlu memastikan bahwa sistem TI yang mereka gunakan dapat berfungsi dengan baik, tetapi juga harus menjaga sistem tersebut agar tetap aman dari ancaman cyber, kebocoran data, serta berbagai risiko lainnya yang dapat merugikan bank dan nasabahnya. Oleh karena itu, pengelolaan dan pengawasan terhadap TI dalam industri perbankan harus dilakukan dengan cermat dan mengikuti prinsip-prinsip tata kelola yang baik (IT governance).

Tata kelola TI adalah suatu sistem yang mengatur bagaimana TI dikelola dan dipertanggungjawabkan dalam suatu organisasi (Irawan Kelvin et al., 2023). Dalam konteks perbankan, tata kelola TI bertujuan untuk memastikan bahwa penggunaan teknologi dapat memberikan nilai tambah bagi organisasi, mendukung pencapaian tujuan bisnis, serta memitigasi risiko yang terkait dengan penggunaan TI tersebut. Penerapan tata kelola TI yang baik dapat membantu bank dalam mengelola berbagai tantangan yang muncul akibat integrasi teknologi yang terus berkembang, serta memastikan bahwa semua sistem yang digunakan dalam operasional perbankan memenuhi standar yang telah ditetapkan.

Salah satu elemen penting dalam tata kelola TI adalah audit sistem informasi. Audit ini berfungsi untuk mengevaluasi kinerja dan kepatuhan terhadap kebijakan dan standar yang berlaku, serta mengidentifikasi potensi risiko yang dapat mengancam sistem informasi yang digunakan. Melalui audit sistem informasi, bank dapat mengetahui sejauh mana efektivitas pengelolaan TI, apakah sistem yang digunakan sudah berjalan dengan baik, dan apakah ada kelemahan atau celah yang perlu diperbaiki. Audit ini juga berperan dalam memastikan bahwa pengelolaan TI di bank sudah sesuai dengan standar internasional, seperti ISO 27001, COBIT, atau standar lainnya yang relevan, yang bertujuan untuk meningkatkan keamanan dan kinerja sistem informasi yang ada.

Audit sistem informasi dapat dilakukan dengan berbagai pendekatan, mulai dari audit internal yang dilakukan oleh tim internal bank, hingga audit eksternal yang melibatkan pihak ketiga independen. Audit ini akan mencakup berbagai aspek, seperti kepatuhan terhadap regulasi dan kebijakan TI yang berlaku, efektivitas kontrol internal, manajemen risiko TI, serta ketahanan sistem terhadap ancaman dan gangguan. Selain itu, audit juga dapat mencakup evaluasi terhadap

keterampilan dan kompetensi sumber daya manusia (SDM) yang terlibat dalam pengelolaan TI di bank, karena ketersediaan SDM yang terampil dan berkompeten merupakan faktor penting dalam menjaga kualitas pengelolaan TI.

Penerapan tata kelola TI yang efektif di sektor perbankan tidak hanya berguna untuk memastikan kelancaran operasional, tetapi juga untuk meningkatkan kepercayaan nasabah terhadap bank. Keamanan dan integritas data menjadi isu yang sangat penting dalam industri perbankan, mengingat tingginya volume transaksi dan informasi yang melibatkan dana nasabah. Oleh karena itu, bank perlu menjaga dan mengelola sistem TI mereka dengan hati-hati agar dapat mengurangi potensi risiko yang dapat berdampak buruk terhadap reputasi bank dan kepercayaan nasabah.

Salah satu tantangan utama adalah cepatnya perubahan teknologi yang mempengaruhi bagaimana sistem informasi dikelola. Misalnya, dengan semakin populernya teknologi berbasis cloud, bank harus menyesuaikan diri dengan perubahan ini dan memastikan bahwa sistem berbasis cloud yang digunakan aman dan sesuai dengan regulasi yang berlaku. Selain itu, adopsi teknologi baru seperti big data dan AI juga memerlukan pengelolaan yang hati-hati untuk menghindari penyalahgunaan data atau pelanggaran privasi (Waruwu & Sundari, 2024).

Tantangan lain yang dihadapi oleh sektor perbankan adalah keterbatasan sumber daya manusia yang memiliki kompetensi yang cukup untuk mengelola teknologi yang semakin kompleks. Banyak bank yang masih menghadapi kesulitan dalam merekrut dan mempertahankan tenaga ahli di bidang TI yang dapat mengelola dan mengawasi sistem yang ada. Pengelolaan TI yang efektif memerlukan kombinasi keterampilan teknis dan manajerial yang tidak semua karyawan TI miliki, sehingga pengembangan sumber daya manusia menjadi aspek yang sangat penting dalam penerapan tata kelola TI yang baik (Farah Ashma Nadiyah et al., 2024).

Penelitian ini bertujuan untuk mengevaluasi bagaimana tata kelola TI di sektor perbankan, khususnya melalui audit sistem informasi, dapat meningkatkan kinerja operasional dan mitigasi risiko teknologi yang ada. Dengan mengidentifikasi potensi kelemahan dan tantangan dalam pengelolaan TI, penelitian ini diharapkan dapat memberikan rekomendasi yang berguna bagi pihak manajemen bank untuk meningkatkan kualitas tata kelola TI mereka. Di samping itu, penelitian ini juga diharapkan dapat memberikan wawasan mengenai pentingnya audit sistem informasi dalam memastikan bahwa sistem TI di bank-bank Indonesia dapat beroperasi secara efektif, efisien, dan aman (Irawan Kelvin et al., 2023).

Penelitian ini memiliki kontribusi yang signifikan dalam memberikan pemahaman yang lebih dalam mengenai tata kelola TI di sektor perbankan dan bagaimana audit sistem informasi dapat membantu mengidentifikasi dan mengatasi masalah yang mungkin timbul. Dengan adanya pemahaman yang lebih baik mengenai tata kelola TI yang baik, diharapkan sektor perbankan di Indonesia dapat meningkatkan kinerja operasional mereka, memperkuat keamanan data nasabah, dan mendukung perkembangan teknologi yang semakin cepat (Putu et al., 2024).

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk mengevaluasi penerapan tata kelola teknologi informasi (IT governance) di sektor perbankan Indonesia. Metode studi kasus dipilih karena memungkinkan peneliti untuk memperoleh pemahaman yang lebih mendalam mengenai penerapan praktik tata kelola TI pada bank-bank yang beroperasi di Indonesia. Melalui pendekatan ini, peneliti dapat menggali secara langsung bagaimana kebijakan dan prosedur TI diterapkan, serta tantangan yang dihadapi dalam pengelolaan teknologi informasi dalam industri perbankan yang sangat dinamis. Dalam penelitian ini, peneliti fokus pada beberapa bank yang representatif di Indonesia. Bank-bank yang dipilih mewakili beragam ukuran dan tipe layanan, mulai dari bank-bank besar dengan fasilitas teknologi yang sangat maju hingga bank-bank regional dengan infrastruktur TI yang lebih sederhana. Pemilihan ini bertujuan untuk melihat seberapa luas penerapan tata kelola TI di berbagai segmen industri perbankan, serta bagaimana setiap bank menyesuaikan tata kelola TI mereka dengan kebutuhan dan kemampuan yang ada.

Penelitian ini memanfaatkan data primer dan sekunder. Data primer diperoleh melalui wawancara dengan praktisi TI yang terlibat langsung dalam pengelolaan dan pengawasan sistem TI di bank-bank yang diteliti. Wawancara dilakukan dengan para pejabat yang memiliki tanggung jawab langsung terhadap penerapan kebijakan TI, seperti Chief Information Officer (CIO), manajer TI, dan staf pengelola TI lainnya. Wawancara ini bertujuan untuk mendapatkan wawasan tentang bagaimana kebijakan dan prosedur TI diterapkan, tantangan yang dihadapi dalam pengelolaan TI, serta upaya-upaya yang dilakukan untuk mengatasi masalah yang muncul.

Selain wawancara, data juga dikumpulkan melalui analisis dokumen yang berkaitan dengan kebijakan dan prosedur pengelolaan TI di bank-bank yang diteliti. Dokumen yang dianalisis meliputi kebijakan tata kelola TI, prosedur audit sistem informasi, laporan audit sebelumnya, serta dokumentasi terkait manajemen risiko

TI dan kepatuhan terhadap standar internasional seperti ISO 27001 dan COBIT. Analisis dokumen ini membantu peneliti untuk memperoleh gambaran yang lebih lengkap mengenai kebijakan dan prosedur yang diikuti oleh bank dalam mengelola TI mereka.

Penelitian ini juga mencakup observasi langsung terhadap implementasi sistem TI di bank-bank yang diteliti. Observasi ini dilakukan dengan cara mempelajari infrastruktur TI yang ada, melihat bagaimana sistem dan aplikasi digunakan dalam operasional sehari-hari, serta mengamati prosedur dan kontrol yang diterapkan dalam pengelolaan TI. Observasi ini memberikan perspektif yang lebih konkrit mengenai bagaimana tata kelola TI diterapkan di lapangan.

Memperoleh data yang valid dan kaya, penelitian ini menggabungkan teknik triangulasi, yang mencakup triangulasi sumber, triangulasi metode, dan triangulasi analisis. Triangulasi sumber dilakukan dengan mengumpulkan data dari berbagai informan yang memiliki perspektif yang berbeda-beda, seperti CIO, manajer TI, dan auditor internal bank. Hal ini bertujuan untuk memastikan bahwa data yang diperoleh memiliki variasi pandangan dan mencerminkan realitas yang lebih holistik.

Triangulasi metode dilakukan dengan menggunakan beberapa teknik pengumpulan data yang saling melengkapi, yaitu wawancara, analisis dokumen, dan observasi langsung. Penggunaan berbagai metode ini memungkinkan peneliti untuk mengonfirmasi temuan-temuan yang diperoleh dari satu metode dengan temuan dari metode lainnya, sehingga meningkatkan keandalan dan validitas data.

Triangulasi analisis dilakukan dengan membandingkan hasil analisis data dari berbagai metode yang digunakan, untuk memastikan bahwa kesimpulan yang ditarik didasarkan pada bukti yang konsisten. Dengan melakukan triangulasi ini, peneliti dapat mengurangi potensi bias dalam pengumpulan dan analisis data, serta meningkatkan kredibilitas hasil penelitian.

Menilai efektivitas dan efisiensi tata kelola TI yang diterapkan, penelitian ini menggunakan kerangka audit TI yang diakui secara internasional, seperti COBIT (Control Objectives for Information and Related Technologies). COBIT adalah framework yang menyediakan pedoman untuk mengelola dan mengawasi TI dalam organisasi, dengan fokus pada mencapai tujuan bisnis dan memitigasi risiko TI. Framework ini terdiri dari berbagai domain yang mencakup pengelolaan dan pengawasan TI, manajemen risiko, serta kontrol dan audit terhadap sistem informasi.

Selain COBIT, penelitian ini juga mengacu pada standar ISO 27001, yang berfokus pada manajemen keamanan informasi. ISO 27001 menyediakan pedoman untuk memastikan bahwa data dan informasi yang dikelola oleh bank tetap aman, terjaga kerahasiaannya, serta dapat diakses dan digunakan sesuai dengan kebutuhan bisnis. Standar ini menjadi penting karena industri perbankan sangat bergantung pada integritas dan keamanan data dalam menjalankan operasionalnya.

Kerangka audit TI ini digunakan untuk mengevaluasi kesesuaian antara kebijakan dan prosedur yang ada dengan prinsip-prinsip tata kelola TI yang baik, serta untuk mengidentifikasi potensi kelemahan dan peluang perbaikan dalam pengelolaan TI di bank-bank yang diteliti. Dalam proses audit, peneliti mengevaluasi aspek-aspek seperti pengelolaan risiko TI, kepatuhan terhadap standar dan regulasi yang berlaku, kontrol internal, serta efektivitas pengawasan terhadap sistem dan aplikasi yang digunakan dalam operasional perbankan.

Proses audit TI dilakukan dalam beberapa tahapan yang sistematis, yaitu perencanaan, pengumpulan data, analisis data, dan penyusunan laporan audit. Pada tahap perencanaan, peneliti merancang dan menentukan ruang lingkup audit, termasuk bank-bank yang akan diteliti, kebijakan dan prosedur TI yang akan dievaluasi, serta indikator-indikator yang akan digunakan untuk mengukur efektivitas tata kelola TI.

Setelah perencanaan, data dikumpulkan melalui wawancara, analisis dokumen, dan observasi langsung. Proses ini berlangsung dalam beberapa sesi yang direncanakan untuk memperoleh gambaran yang menyeluruh mengenai penerapan tata kelola TI di bank. Pada tahap analisis, data yang terkumpul dianalisis dengan mengacu pada prinsip-prinsip tata kelola TI yang baik serta standar internasional yang relevan.

Tahap terakhir adalah penyusunan laporan audit, yang berisi temuan-temuan hasil analisis, kesimpulan, dan rekomendasi untuk perbaikan. Laporan ini disusun dengan tujuan untuk memberikan panduan kepada bank dalam meningkatkan pengelolaan TI mereka, serta memperbaiki kelemahan-kelemahan yang ditemukan selama proses audit.

Memastikan validitas dan keandalan data, penelitian ini menggunakan beberapa teknik verifikasi, seperti member checking, di mana hasil wawancara dikembalikan kepada informan untuk memastikan akurasi informasi yang diberikan. Selain itu, peneliti juga melakukan cross-checking antara data yang diperoleh melalui wawancara dengan data dari dokumen dan observasi lapangan, guna memastikan konsistensi dan kredibilitas data yang dikumpulkan. Dengan pendekatan ini, diharapkan penelitian ini dapat memberikan pemahaman yang lebih

komprehensif mengenai penerapan tata kelola TI di sektor perbankan Indonesia dan bagaimana audit sistem informasi dapat membantu meningkatkan efektivitas dan efisiensi pengelolaan TI yang ada.

HASIL DAN PEMBAHASAN

Dalam penelitian ini, beberapa temuan penting mengenai penerapan tata kelola teknologi informasi (TI) di sektor perbankan Indonesia telah teridentifikasi. Temuan-temuan ini berfokus pada kebijakan, prosedur, serta pelaksanaan audit sistem informasi di bank-bank yang diteliti. Berdasarkan hasil analisis, meskipun bank-bank tersebut telah memiliki kebijakan dan prosedur yang cukup lengkap terkait pengelolaan TI, masih terdapat sejumlah tantangan dalam penerapannya yang memerlukan perhatian lebih lanjut. Berikut ini adalah pembahasan lebih mendalam mengenai beberapa aspek penting yang ditemukan dalam penelitian ini.

Manajemen risiko TI merupakan salah satu aspek yang sangat penting dalam tata kelola TI, terutama di sektor perbankan yang sangat bergantung pada teknologi untuk menjalankan operasional sehari-hari (Purnawa et al., 2023). Berdasarkan temuan penelitian, sebagian besar bank yang diteliti sudah memiliki kebijakan risiko TI yang cukup baik dan mengikuti prosedur identifikasi serta mitigasi risiko. Namun, meskipun kebijakan sudah ada, penerapannya di lapangan masih cenderung bersifat reaktif daripada proaktif.

Pada sebagian besar bank, prosedur identifikasi risiko TI dilakukan secara periodik dan terstruktur. Namun, identifikasi ini seringkali dilakukan setelah terjadinya masalah atau insiden, seperti gangguan layanan atau kebocoran data. Proses ini tidak sepenuhnya mencakup potensi risiko yang muncul seiring dengan perkembangan teknologi, seperti risiko terkait dengan penggunaan teknologi baru atau ancaman siber yang terus berkembang. Banyak bank yang masih mengandalkan metode tradisional dalam mengidentifikasi risiko, yang mengarah pada pemahaman yang lebih terbatas tentang ancaman yang mungkin dihadapi (Trisyanto Surya et al., 2022).

Sebagian besar bank yang diteliti telah menetapkan prosedur mitigasi risiko yang mencakup langkah-langkah untuk mengurangi dampak dari ancaman yang telah diidentifikasi. Namun, penerapan mitigasi risiko masih sering kali dilakukan secara ad-hoc, tergantung pada situasi yang muncul. Hal ini mengakibatkan bank kurang siap menghadapi risiko yang muncul secara tiba-tiba atau yang lebih kompleks. Bank seharusnya mengembangkan strategi mitigasi risiko yang lebih terencana dan berbasis pada analisis risiko jangka panjang. Agar manajemen risiko TI dapat diterapkan lebih proaktif, bank-bank perlu meningkatkan sistem pemantauan dan deteksi dini untuk mengidentifikasi potensi ancaman sebelum

menjadi masalah besar. Selain itu, pelatihan dan pembekalan untuk staf terkait mitigasi risiko juga perlu diperkuat agar mereka dapat merespon lebih cepat dan tepat terhadap potensi ancaman yang ada.

Kepatuhan terhadap standar internasional, seperti ISO 27001 (standar sistem manajemen keamanan informasi) dan COBIT (Control Objectives for Information and Related Technologies), menjadi salah satu acuan penting dalam penerapan tata kelola TI di sektor perbankan. Penelitian ini menemukan bahwa sebagian besar bank yang diteliti sudah mengikuti standar-standar ini, tetapi implementasinya tidak selalu konsisten di seluruh bagian organisasi.

ISO 27001 dan COBIT adalah dua standar yang sangat relevan dalam industri perbankan karena keduanya membantu bank untuk mengelola keamanan informasi dan pengendalian TI secara efektif. Namun, temuan penelitian menunjukkan bahwa meskipun kebijakan dan prosedur terkait dengan standar ini telah diterapkan di sebagian besar bank, penerapannya masih terbatas pada bagian tertentu saja, seperti divisi TI atau unit yang bertanggung jawab langsung terhadap keamanan informasi.

Implementasi standar ini sering kali tidak merata di seluruh organisasi. Beberapa bagian dari bank, seperti unit pengembangan teknologi atau unit operasional, belum sepenuhnya mengadopsi prinsip-prinsip yang tercantum dalam ISO 27001 atau COBIT. Hal ini mengakibatkan inkonsistensi dalam pengelolaan risiko dan kontrol terhadap TI yang ada. Selain itu, penerapan standar ini cenderung lebih fokus pada aspek-aspek tertentu, seperti kebijakan keamanan data, sementara aspek lain, seperti manajemen sumber daya manusia atau pengelolaan perubahan, kurang mendapatkan perhatian yang memadai. Untuk meningkatkan kepatuhan terhadap standar internasional, bank-bank perlu memastikan bahwa implementasi standar seperti ISO 27001 dan COBIT dilakukan secara menyeluruh di seluruh bagian organisasi, bukan hanya di unit TI. Selain itu, perlu adanya pelatihan berkelanjutan untuk memastikan bahwa setiap pegawai memahami dan mematuhi standar yang ditetapkan. Bank juga dapat melakukan audit internal secara rutin untuk menilai sejauh mana kepatuhan terhadap standar ini diterapkan di seluruh area operasional.

Sumber daya manusia (SDM) yang terampil dan terlatih dalam pengelolaan TI sangat penting untuk kesuksesan penerapan tata kelola TI di bank-bank. Hasil penelitian menunjukkan bahwa banyak bank yang menghadapi tantangan dalam hal keterampilan dan pelatihan staf yang mengelola sistem TI.

Banyak bank yang belum memiliki staf TI dengan keterampilan yang memadai untuk menangani teknologi yang terus berkembang. Misalnya, dengan semakin berkembangnya sistem perbankan digital, mobile banking, dan aplikasi berbasis cloud, dibutuhkan SDM dengan keahlian khusus dalam mengelola dan mengamankan sistem-sistem tersebut. Sayangnya, pelatihan untuk staf TI di banyak bank masih terbatas pada aspek teknis dasar dan tidak selalu diperbarui sesuai dengan tren teknologi terbaru.

Keamanan TI adalah area yang sangat penting, mengingat ancaman siber yang semakin canggih. Namun, banyak staf yang tidak memiliki pemahaman mendalam tentang prinsip-prinsip keamanan informasi atau cara-cara mengelola risiko yang terkait dengan ancaman siber. Pelatihan yang diberikan sering kali kurang mencakup topik-topik penting, seperti pengelolaan data sensitif, kebijakan keamanan jaringan, atau respons terhadap insiden keamanan.

Bank-bank perlu berinvestasi lebih banyak dalam pelatihan dan pengembangan SDM TI mereka. Selain pelatihan teknis, bank juga harus menyediakan pelatihan berkelanjutan tentang keamanan TI, pengelolaan risiko, serta keterampilan manajerial dalam menghadapi perubahan teknologi yang pesat. Program pelatihan dan sertifikasi internasional, seperti CISSP (Certified Information Systems Security Professional) dan CISM (Certified Information Security Manager), bisa menjadi pilihan untuk meningkatkan kompetensi staf TI (Normah et al., 2022).

Audit internal memainkan peran penting dalam memastikan bahwa sistem TI yang diterapkan berfungsi dengan baik dan mematuhi kebijakan yang telah ditetapkan. Hasil penelitian menunjukkan bahwa meskipun audit internal dilakukan secara teratur, beberapa kelemahan masih ditemukan dalam pengawasan terhadap sistem TI yang lebih canggih dan berisiko tinggi, seperti sistem perbankan online dan aplikasi mobile banking (Angelo et al., 2024).

Audit internal di sebagian besar bank umumnya fokus pada aspek-aspek dasar, seperti pengendalian akses dan pemantauan kinerja sistem TI. Namun, audit ini belum mencakup secara mendalam sistem-sistem TI yang lebih kompleks dan rentan terhadap ancaman, seperti aplikasi mobile banking, sistem perbankan online, dan infrastruktur cloud. Dengan semakin berkembangnya teknologi, bank-bank perlu memastikan bahwa audit internal mencakup semua aspek sistem TI yang ada (Purnawa et al., 2023).

Beberapa bank tidak sepenuhnya melakukan audit terhadap sistem-sistem yang memiliki risiko tinggi. Sebagai contoh, aplikasi mobile banking dan sistem

perbankan online, yang sering menjadi target serangan siber, tidak selalu mendapatkan perhatian yang cukup dalam audit internal. Hal ini dapat mengarah pada potensi celah keamanan yang tidak terdeteksi (Waruwu & Sundari, 2024). Untuk meningkatkan efektivitas audit internal, bank-bank perlu memperluas ruang lingkup audit untuk mencakup semua sistem TI, terutama yang memiliki risiko tinggi. Bank juga perlu mengembangkan prosedur audit yang lebih rinci dan memastikan bahwa auditor internal memiliki pengetahuan yang cukup untuk mengidentifikasi risiko-risiko baru yang muncul seiring dengan perkembangan teknologi (Sahara et al., 2023).

Penelitian ini menunjukkan bahwa meskipun sebagian besar bank di Indonesia telah memiliki kebijakan dan prosedur yang memadai terkait dengan tata kelola TI, masih ada banyak ruang untuk perbaikan dalam penerapannya. Aspek-aspek seperti manajemen risiko TI, kepatuhan terhadap standar internasional, pengelolaan sumber daya manusia, dan kontrol serta audit internal memerlukan perhatian lebih lanjut agar tata kelola TI di sektor perbankan dapat berjalan lebih efektif. Dengan meningkatkan penerapan audit sistem informasi dan pengelolaan risiko yang lebih baik, bank-bank di Indonesia dapat memastikan bahwa mereka tidak hanya memenuhi regulasi yang ada, tetapi juga dapat mengelola teknologi dengan lebih aman dan efisien, serta siap menghadapi tantangan di masa depan.

SIMPULAN

Penelitian ini menyimpulkan bahwa tata kelola teknologi informasi (TI) di sektor perbankan Indonesia telah menunjukkan perkembangan yang signifikan, dengan sebagian besar bank telah memiliki kebijakan, prosedur, dan infrastruktur dasar yang mendukung pengelolaan TI. Namun, efektivitas penerapan kebijakan tersebut masih memerlukan peningkatan di berbagai aspek. Bank-bank di Indonesia telah menyadari pentingnya manajemen risiko TI dan telah mengembangkan kebijakan serta prosedur yang memadai. Namun, implementasi di lapangan cenderung bersifat reaktif daripada proaktif. Identifikasi dan mitigasi risiko yang lebih sistematis dan berbasis prediksi menjadi kebutuhan mendesak agar bank dapat menghadapi risiko TI yang semakin kompleks.

Sebagian besar bank telah mengadopsi standar internasional, seperti ISO 27001 dan COBIT, sebagai acuan tata kelola TI. Meskipun demikian, penerapan standar ini belum konsisten di seluruh bagian organisasi, terutama dalam divisi-divisi non-TI. Ketidakmerataan ini dapat mengurangi efektivitas tata kelola TI secara keseluruhan.

Keterampilan dan kapasitas sumber daya manusia yang terlibat dalam pengelolaan TI masih menjadi tantangan besar. Banyak bank menghadapi keterbatasan dalam hal pelatihan dan pengembangan staf, terutama dalam menghadapi teknologi baru dan ancaman siber yang semakin canggih. Upaya peningkatan kompetensi melalui program pelatihan berkelanjutan dan sertifikasi internasional menjadi hal yang sangat penting. Audit internal secara rutin telah dilakukan oleh sebagian besar bank, tetapi belum mencakup secara menyeluruh sistem TI yang memiliki risiko tinggi, seperti mobile banking dan aplikasi berbasis cloud. Kelemahan dalam pengawasan ini dapat membuka celah bagi potensi ancaman yang tidak terdeteksi, sehingga diperlukan audit yang lebih mendalam dan menyeluruh.

Mengembangkan sistem pemantauan risiko berbasis teknologi yang memungkinkan deteksi dini terhadap potensi ancaman. Melakukan evaluasi secara rutin terhadap penerapan standar internasional di seluruh bagian organisasi, termasuk divisi non-TI. Bank harus berinvestasi dalam pelatihan dan pengembangan kompetensi TI, khususnya dalam hal keamanan informasi dan teknologi mutakhir. Melibatkan sistem TI canggih dalam ruang lingkup audit serta memastikan auditor memiliki kompetensi untuk mengidentifikasi risiko baru. Bank-bank di Indonesia dapat memperkuat tata industri TI mereka, mengelola risiko dengan lebih efektif, meningkatkan keamanan industri informasi, dan memanfaatkan teknologi secara optimal untuk mendukung operasional serta pelayanan kepada nasabah. Pada akhirnya, ini akan memberikan dampak positif terhadap kepercayaan industri dan daya saing industri perbankan di era digital.

DAFTAR PUSTAKA

- [1] Angelo, J., Tania, S., Loren, F., & Angeline. (2024). Kajian Literatur terhadap Audit Sistem Informasi pada Perusahaan Perbankan. *JDMIS: Journal of Data Mining and Information Systems*, 2(2), 82–89. <https://doi.org/10.54259/jdmis.v2i2.2216>
- [2] Farah Ashma Nadiyah, Balqis Maharani, & Dien Noviany Rahmatika. (2024). Pengaruh Audit Teknologi Informasi Terhadap Kualitas Audit. *Ekonomi Keuangan Syariah Dan Akuntansi Pajak*, 1(3), 236–253. <https://doi.org/10.61132/eksap.v1i3.278>
- [3] Irawan Kelvin, Hanggara Buce Trias, & Suprpto. (2023). *Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi menggunakan Framework COBIT 2019*. 7(5), 2642–2651.
- [4] Nicholas, P., Tambunan, P., & Legowo, N. (2024). *Evaluasi Tata Kelola TI Bank Indonesia Provinsi Bengkulu Dengan COBIT 2019*. 11(1).

<http://jurnal.mdp.ac.id>

- [5] Normah, Rifai, B., & Afitta. (2022). Audit Tata Kelola Teknologi Informasi Menggunakan Cobit 4.1 PT. Daya Cipta Kemasindo Tangerang. *Indonesian Journal on Software Engineering (IJSE)*, 8(2), 163–172. <https://doi.org/10.31294/ijse.v8i2.14480>
- [6] Purnawa, I. G. N. G., Swastika, I. P. A., & Putra, I. G. J. E. (2023). Audit Tata Kelola Sistem Informasi Menggunakan Framework COBIT 5 (Studi Kasus Pada Bank BPR XYZ). *JATI (Jurnal Mahasiswa Teknik Informatika)*, 7(4), 2570–2577.
- [7] Putu, S., Krisnanda Wiguna, B., Pramesti, G. A., Putri, D., & Estiyanti, N. M. (2024). Audit Dan Tata Kelola Sistem Informasi Menggunakan Framework Cobit 2019 Pada Ksp Sri Satyam Sedana. *Jurnal TEKINKOM*, 7(1), 102–112. <https://doi.org/10.37600/tekinkom.v7i1.1190>
- [8] Sahara, E., Studi, P., Informasi, S., Teknik, J., & Dan, E. (2023). *Audit Tata Kelola Teknologi Informasi Pada Sistem Informasi E-Learning Universitas Jambi Menggunakan Kerangka*. <https://repository.unja.ac.id/id/eprint/59301>
- [9] Sinaga, R., & Permana, I. (2023). Audit Sistem Informasi Terhadap Pt Enseval Menggunakan Cobit 4.1 Domain Acquire Implementation. *Semnas Ristek (Seminar Nasional Riset Dan Inovasi Teknologi)*, 7(1), 1–6. <https://doi.org/10.30998/semnasristek.v7i1.623>
- [10] Trisyanto Surya, R., Suwondo, S., Hadiani, F., & Susilawaty Hutapea, R. (2022). Audit Tata Kelola Teknologi Informasi Perusahaan Perbankan Skala Kecil Menggunakan Framework Cobit. *Jurnal Sosial Dan Sains*, 2(7), 818–822. <https://doi.org/10.59188/jurnalsosains.v2i7.44>
- [11] Waruwu, G., & Sundari, J. (2024). Audit Teknologi Informasi Menggunakan Cobit 5 Studi Kasus PT. Global Network Dharma Jaya. *Infomatek*, 26(1), 69–74. <https://doi.org/10.23969/infomatek.v26i1.13333>