JURNAL CAHAYA MANDALIKA

P-ISSN: 2828-495X
E-ISSN: 2721-4796

EVALUASI EFEKTIVITAS SISTEM KONTROL TI, PROSEDUR AUDIT, DAN DETEKSI KECURANGAN DI INSTITUSI KEUANGAN

I Nyoman Angga Prabawa, Ida Ayu Trisna Yudi Asri, I Gusti Ngurah Agung Pawana
Universitas Warmadewa
Email: prabawa_angga@yahoo.co.id, dayutrisnaa@gmail.com, rahgungpawana@gmail.com

Kata kunci:
Teknologi Informasi, Audit, Institusi Keuangan

ABSTRAK

Penelitian ini bertujuan untuk mengevaluasi efektivitas sistem kontrol teknologi informasi (TI), prosedur audit, dan deteksi kecurangan di institusi keuangan melalui pendekatan kualitatif dengan metode literature review. Sistem kontrol TI memainkan peran kunci dalam menjaga keamanan data dan integritas operasional, sementara prosedur audit berfungsi sebagai mekanisme pengawasan yang dapat mendeteksi dan mencegah terjadinya kecurangan. Dalam penelitian ini, kami mengumpulkan dan menganalisis berbagai literatur yang berkaitan dengan topik tersebut, termasuk studi empiris, artikel teori, dan laporan praktik terbaik. Hasil evaluasi menunjukkan bahwa institusi keuangan yang menerapkan sistem kontrol TI yang komprehensif dan terus diperbarui mampu mengurangi risiko kebocoran data dan penyalahgunaan informasi. Prosedur audit yang efektif dan berbasis risiko terbukti mampu mengidentifikasi kelemahan dalam sistem dan operasi yang berpotensi menjadi titik masuk bagi kecurangan. Namun, deteksi kecurangan tidak hanya bergantung pada kekuatan teknologi dan prosedur audit, tetapi juga pada kesadaran dan keterlibatan seluruh pemangku kepentingan dalam institusi keuangan tersebut.

Keywords:
Information Technology, Audit, Financial Institutions

ABSTRACT

This study aims to evaluate the effectiveness of information technology (IT) control systems, audit procedures, and fraud detection in financial institutions through a qualitative approach with the literature review method. IT control systems play a key role in maintaining data security and operational integrity, while audit procedures serve as oversight mechanisms that can detect and prevent fraud. In this study, we collected and analyzed a wide range of literature related to the topic, including empirical studies, theoretical articles, and best practice reports. The results of the evaluation show that financial institutions that implement a comprehensive and continuously updated IT control system are able to reduce the risk of data leakage and information misuse. Effective and risk-based audit procedures have proven to be able to identify weaknesses in systems and operations that have the potential to become entry points for fraud. However, fraud detection depends not only on the strength of technology and audit procedures, but also on the awareness and involvement of all stakeholders in the financial institution..

PENDAHULUAN

Dalam era globalisasi yang serba cepat dan kompetitif, institusi keuangan menghadapi tantangan yang semakin kompleks dalam mengelola risiko dan menjaga keandalan sistem kontrol TI serta prosedur audit. Perkembangan teknologi informasi (TI) yang pesat telah membawa

dampak signifikan terhadap efektivitas sistem kontrol, prosedur audit, dan deteksi kecurangan di institusi keuangan. Untuk menjawab tantangan ini, evaluasi terhadap efektivitas sistem kontrol TI, prosedur audit, dan deteksi kecurangan menjadi sangat penting untuk memastikan integritas dan keandalan operasional institusi keuangan.

Meskipun telah banyak penelitian sebelumnya yang mengkaji topik terkait evaluasi sistem kontrol TI, prosedur audit, dan deteksi kecurangan di institusi keuangan, masih terdapat kesenjangan penelitian yang perlu ditindaklanjuti. Penelitian sebelumnya cenderung terfokus pada aspek teknis dan keandalan sistem TI tanpa mempertimbangkan secara komprehensif aspek audit dan deteksi kecurangan.

Dalam konteks ini, penelitian ini bertujuan untuk mengisi celah pengetahuan (research gap) dengan menyelidiki secara holistik efektivitas sistem kontrol TI, prosedur audit, dan deteksi kecurangan di institusi keuangan. Penelitian sebelumnya yang relevan, seperti penelitian oleh (Nama Peneliti, Tahun), telah memberikan pemahaman awal terhadap konsep dan aplikasi sistem kontrol TI, prosedur audit, dan deteksi kecurangan. Namun, penelitian ini akan memberikan kontribusi baru dengan mengkaji integrasi dan interaksi antara ketiga aspek tersebut dalam konteks institusi keuangan.

Tujuan utama dari penelitian ini adalah untuk mengevaluasi efektivitas sistem kontrol TI, prosedur audit, dan deteksi kecurangan di institusi keuangan serta mengidentifikasi faktor-faktor yang mempengaruhi keberhasilan implementasi. Melalui analisis yang mendalam, penelitian ini bertujuan untuk memberikan wawasan baru yang dapat menjadi dasar bagi pengembangan kebijakan dan praktik terbaik dalam manajemen risiko dan keandalan operasional institusi keuangan. Diharapkan hasil dari penelitian ini dapat memberikan kontribusi signifikan bagi pemangku kepentingan dalam meningkatkan tata kelola dan pengelolaan risiko di institusi keuangan.

METODE

Jenis penelitian yang digunakan dalam studi ini adalah penelitian kualitatif. Pendekatan kualitatif dipilih karena memungkinkan peneliti untuk memahami secara mendalam fenomena yang kompleks dan multifaset, seperti evaluasi efektivitas sistem kontrol TI, prosedur audit, dan

deteksi kecurangan di institusi keuangan (Yin, 2018). Dalam penelitian kualitatif, data diperoleh melalui observasi, wawancara, dan analisis dokumen (Creswell & Creswell, 2017).

Sumber data utama dalam penelitian ini adalah institusi keuangan yang menjadi objek penelitian. Data akan dikumpulkan melalui wawancara mendalam dengan manajer senior, auditor internal, dan staf yang terlibat langsung dalam pengelolaan sistem kontrol TI, prosedur audit, dan deteksi kecurangan. Selain itu, data juga akan diperoleh dari dokumen-dokumen internal institusi keuangan, seperti kebijakan, prosedur operasional standar, laporan audit, dan laporan keuangan (Patton, 2015).

Teknik pengumpulan data yang digunakan meliputi wawancara mendalam dan analisis dokumen. Wawancara mendalam akan dilakukan dengan menggunakan pedoman wawancara yang telah disusun sebelumnya untuk memastikan konsistensi dan relevansi pertanyaan (Merriam, 2009). Analisis dokumen akan dilakukan dengan memeriksa dan menganalisis dokumen-dokumen yang relevan dengan tujuan penelitian (Creswell & Creswell, 2017).

Metode analisis data yang digunakan adalah analisis kualitatif. Data yang diperoleh dari wawancara dan analisis dokumen akan dianalisis secara tematik, di mana pola-pola tematik akan diidentifikasi dan dianalisis untuk menghasilkan temuan-temuan yang signifikan terkait dengan efektivitas sistem kontrol TI, prosedur audit, dan deteksi kecurangan di institusi keuangan (Braun & Clarke, 2006).

HASIL DAN PEMBAHASAN

1. Efektivitas Sistem Kontrol Teknologi Informasi (TI)

Sistem kontrol TI merupakan kerangka kerja yang memastikan keamanan, integritas, dan ketersediaan data serta informasi di institusi keuangan (Hunton et al., 2004). Hasil analisis menunjukkan bahwa efektivitas sistem kontrol TI di institusi keuangan masih memiliki beberapa kelemahan. Meskipun telah diimplementasikan, masih terdapat celah keamanan yang memungkinkan terjadinya pelanggaran dan penyalahgunaan data. Hal ini dapat disebabkan oleh kekurangan dalam pemantauan dan pembaruan sistem, kurangnya kesadaran akan risiko keamanan, serta kurangnya sumber daya yang diperuntukkan untuk pengelolaan keamanan TI secara efektif.

Sistem Kontrol Teknologi Informasi (TI) merupakan serangkaian kebijakan, prosedur, dan alat teknologi yang dirancang untuk melindungi aset informasi, menjaga integritas data, memastikan ketersediaan sistem, dan menjaga kerahasiaan informasi di dalam sebuah organisasi, termasuk institusi keuangan. Efektivitas sistem kontrol TI dapat dilihat dari kemampuannya untuk mendeteksi dan mencegah potensi risiko, melindungi data dari ancaman internal dan eksternal, serta memastikan kepatuhan terhadap regulasi dan kebijakan yang berlaku.

Sistem kontrol TI sering dibahas dalam konteks pengendalian internal yang lebih luas dalam organisasi. Menurut COSO (Committee of Sponsoring Organizations of the Treadway Commission), pengendalian internal termasuk di dalamnya adalah sistem kontrol TI yang bertujuan untuk memberikan jaminan bahwa tujuan-tujuan operasional, pelaporan, dan kepatuhan suatu organisasi dapat dicapai (COSO, 2013). Framework ini menggarisbawahi pentingnya kontrol TI dalam memastikan keandalan sistem informasi dan keamanan data.

Hunton et al. (2004) dalam penelitiannya menekankan bahwa sistem kontrol TI yang efektif harus mencakup kontrol umum TI (general IT controls) dan kontrol aplikasi (application controls). Kontrol umum TI meliputi kontrol terhadap infrastruktur TI seperti perangkat keras, perangkat lunak, jaringan, dan data, sedangkan kontrol aplikasi berfokus pada integritas dan keamanan aplikasi-aplikasi yang digunakan dalam pengolahan data. Penelitian lain oleh Rezaee (2002) mengindikasikan bahwa kontrol TI yang efektif juga harus mencakup pemantauan terus-menerus terhadap sistem untuk mendeteksi dan menanggulangi ancaman secara real-time. Ini melibatkan penggunaan alat pemantauan otomatis yang dapat memberikan peringatan dini terhadap potensi ancaman.

Penelitian terbaru menunjukkan bahwa meskipun banyak organisasi yang telah menerapkan sistem kontrol TI, efektivitasnya sering kali terganggu oleh berbagai faktor, seperti kurangnya pemahaman tentang risiko teknologi, kelemahan dalam pemantauan, dan keterbatasan dalam sumber daya untuk mengelola kontrol tersebut (Baskerville et al., 2014). Temuan baru yang menjadi poin penting dalam pembahasan ini adalah:

1) Keterbatasan Sumber Daya dan Pengetahuan: Banyak institusi keuangan yang mengalami keterbatasan dalam hal sumber daya manusia dan pengetahuan terkait teknologi informasi. Kekurangan ini membuat sulit untuk melakukan pemantauan dan pemeliharaan sistem kontrol TI secara efektif. Banyak organisasi masih menggunakan pendekatan reaktif

daripada proaktif dalam menangani masalah keamanan TI, yang seringkali terlambat dalam mendeteksi ancaman yang muncul (Wang & Li, 2017).

2) Pemanfaatan Teknologi yang Tidak Optimal: Meskipun teknologi canggih tersedia untuk pemantauan dan pengendalian, banyak institusi yang belum memanfaatkan sepenuhnya potensi teknologi tersebut. Misalnya, alat-alat seperti sistem deteksi intrusi (Intrusion Detection Systems) dan analitik prediktif (predictive analytics) yang dapat mendeteksi ancaman sebelum terjadi masih kurang dimanfaatkan secara optimal. Penggunaan teknologi ini dapat secara signifikan meningkatkan efektivitas kontrol TI dengan memberikan deteksi dini dan respons yang lebih cepat terhadap ancaman (Jouini et al., 2014).
3) Kepatuhan terhadap Regulasi: Regulasi seperti GDPR di Eropa dan berbagai regulasi perbankan internasional lainnya menuntut tingkat keamanan data yang tinggi dan kepatuhan terhadap standar keamanan informasi. Penelitian menunjukkan bahwa institusi yang berhasil dalam menjaga kepatuhan terhadap regulasi ini memiliki sistem kontrol TI yang lebih kuat dan lebih efektif dalam melindungi data dan informasi mereka (Ross & Anderson, 2016).
4) Kolaborasi Antardepartemen: Efektivitas kontrol TI tidak hanya bergantung pada departemen IT saja, tetapi juga memerlukan kerjasama yang erat dengan departemen lain seperti manajemen risiko, kepatuhan, dan audit internal. Kolaborasi yang baik dapat membantu dalam identifikasi dan mitigasi risiko yang lebih komprehensif dan efektif (Dhillon & Backhouse, 2013).

Dengan demikian, untuk meningkatkan efektivitas sistem kontrol TI, institusi keuangan perlu fokus pada peningkatan pengetahuan dan sumber daya, optimalisasi penggunaan teknologi canggih, kepatuhan terhadap regulasi yang ketat, serta memperkuat kolaborasi antardepartemen dalam organisasi.

2. Evaluasi Prosedur Audit

Prosedur audit merupakan langkah-langkah yang dilakukan untuk memeriksa keandalan, keakuratan, dan kepatuhan terhadap kebijakan dan prosedur yang telah ditetapkan (Rezaee, 2002). Dalam analisis ini, ditemukan bahwa prosedur audit yang diterapkan di institusi keuangan masih

belum optimal dalam mendeteksi potensi kecurangan dan pelanggaran. Beberapa prosedur audit mungkin kurang efisien atau kurang relevan dengan tantangan keuangan dan teknologi yang dihadapi oleh institusi keuangan saat ini. Oleh karena itu, perlu adanya evaluasi mendalam terhadap prosedur audit yang ada dan penyempurnaan untuk meningkatkan efektivitasnya.

Prosedur audit adalah serangkaian langkah atau tindakan yang dilakukan oleh auditor untuk memperoleh bukti yang cukup dan relevan guna memberikan opini atas kewajaran laporan keuangan atau kepatuhan terhadap standar dan regulasi yang berlaku (Arens, Elder, & Beasley, 2017). Prosedur ini mencakup berbagai aktivitas mulai dari pengumpulan, analisis, hingga evaluasi informasi dan data yang berhubungan dengan entitas yang diaudit.

Tujuan dari prosedur audit adalah untuk mengidentifikasi dan menilai risiko salah saji material dalam laporan keuangan atau pelanggaran terhadap peraturan yang dapat berdampak pada integritas informasi yang dilaporkan. Melalui prosedur ini, auditor dapat menentukan apakah laporan keuangan telah disusun sesuai dengan prinsip akuntansi yang berlaku umum (GAAP) atau standar lainnya yang relevan (Messier, Glover, & Prawitt, 2018).

Teori terkait prosedur audit mencakup berbagai pendekatan, seperti risiko audit, siklus pengendalian internal, dan standar audit internasional (ISA). Menurut teori risiko audit, auditor harus memahami dan mengevaluasi risiko yang terkait dengan entitas yang diaudit untuk merancang dan melaksanakan prosedur audit yang tepat guna (Hayes, Dassen, Schilder, & Wallage, 2004). Risiko audit sendiri terdiri dari risiko bawaan, risiko pengendalian, dan risiko deteksi yang harus dikelola secara komprehensif untuk mencapai hasil audit yang diinginkan (Whittington & Pany, 2019). Penelitian sebelumnya oleh Gramling, Maletta, Schneider, dan Church (2004) menekankan pentingnya pemahaman yang mendalam terhadap sistem pengendalian internal dalam pelaksanaan prosedur audit. Sistem pengendalian yang efektif dapat membantu auditor dalam mengidentifikasi area yang berisiko tinggi dan menentukan prosedur audit yang sesuai. Penelitian ini juga menyoroti bahwa penggunaan teknologi informasi dapat meningkatkan efisiensi dan efektivitas prosedur audit, namun juga menambah kompleksitas dalam pengendalian dan pengawasan.

Penelitian terbaru menunjukkan bahwa efektivitas prosedur audit sering kali dipengaruhi oleh berbagai faktor, seperti integritas data, pemahaman auditor terhadap risiko TI, dan perubahan

regulasi yang terus berkembang (Brown-Liburd, Cohen, & Zamora, 2018). Dalam konteks ini, beberapa temuan baru yang menjadi poin penting adalah:

1) Penggunaan Analitik Data dalam Proses Audit: Penggunaan analitik data telah menjadi fokus utama dalam prosedur audit modern. Teknologi ini memungkinkan auditor untuk menganalisis data dalam jumlah besar dengan cepat dan efisien, yang pada gilirannya dapat membantu dalam mendeteksi anomali atau pola yang mencurigakan. Penelitian oleh Appelbaum, Kogan, dan Vasarhelyi (2017) menunjukkan bahwa analitik data dapat meningkatkan kemampuan auditor dalam mengidentifikasi risiko dan mengurangi kesalahan manusia dalam proses audit.
2) Evaluasi Pengendalian Internal yang Lebih Mendalam: Auditor kini dihadapkan pada kebutuhan untuk melakukan evaluasi pengendalian internal yang lebih mendalam dan kompleks. Sistem pengendalian yang terintegrasi dengan teknologi informasi memerlukan pendekatan audit yang lebih canggih dan pengetahuan mendalam tentang risiko TI. Penelitian oleh Soh dan Martinov-Bennie (2018) mengindikasikan bahwa pemahaman terhadap pengendalian internal TI yang efektif sangat penting untuk mengurangi risiko salah saji material dalam laporan keuangan.
3) Kepatuhan terhadap Standar Internasional: Penelitian oleh Mock, Srivastava, dan Wright (2017) menunjukkan bahwa kepatuhan terhadap standar audit internasional (ISA) sangat penting untuk menjaga kualitas audit dan meningkatkan kepercayaan pemangku kepentingan. Penerapan standar yang konsisten memungkinkan auditor untuk melakukan evaluasi prosedur audit dengan lebih efektif dan efisien, serta memastikan bahwa temuan audit dapat diterima di berbagai yurisdiksi.
4) Peningkatan Peran Audit Berbasis Risiko: Prosedur audit berbasis risiko kini menjadi pendekatan yang dominan dalam praktik audit. Penelitian oleh Knechel (2016) menunjukkan bahwa audit berbasis risiko memungkinkan auditor untuk fokus pada area yang memiliki risiko lebih tinggi dan menyesuaikan prosedur audit sesuai dengan tingkat risiko yang diidentifikasi. Hal ini membantu dalam meningkatkan efektivitas dan efisiensi audit serta memastikan bahwa sumber daya audit digunakan dengan bijaksana.

5) Perubahan Dinamis dalam Regulasi: Perubahan regulasi yang terus berkembang mempengaruhi prosedur audit secara signifikan. Auditor harus selalu mengikuti perkembangan terbaru dalam regulasi untuk memastikan bahwa audit yang dilakukan sesuai dengan persyaratan hukum dan standar yang berlaku. Penelitian oleh PwC (2019) menunjukkan bahwa adaptasi cepat terhadap perubahan regulasi menjadi kunci dalam menjaga kualitas dan efektivitas prosedur audit.

Dari pembahasan ini, dapat disimpulkan bahwa efektivitas prosedur audit sangat bergantung pada pemahaman yang mendalam terhadap risiko, penggunaan teknologi yang tepat, dan kepatuhan terhadap standar serta regulasi yang berlaku. Dengan mengadopsi pendekatan berbasis risiko dan memanfaatkan teknologi analitik data, auditor dapat meningkatkan kualitas dan efisiensi audit serta memberikan nilai tambah bagi organisasi yang diaudit.

3. Deteksi Kecurangan dalam Institusi Keuangan

Deteksi kecurangan merupakan upaya untuk mengidentifikasi dan mencegah tindakan penipuan atau pelanggaran yang terjadi dalam institusi keuangan (Wells, 2005). Namun, hasil analisis menunjukkan bahwa deteksi kecurangan masih belum optimal di banyak institusi keuangan. Keterbatasan dalam teknologi pendeteksian kecurangan, kurangnya kesadaran akan pola kecurangan yang berkembang, dan kelemahan dalam prosedur pengawasan internal dapat menyebabkan banyak kecurangan yang tidak terdeteksi atau diatasi secara tepat waktu.

Kecurangan atau fraud dalam institusi keuangan merupakan tindakan tidak sah yang dilakukan dengan niat untuk memperoleh keuntungan pribadi dengan cara yang melanggar hukum atau melanggar prinsip kepercayaan (Albrecht, Albrecht, Albrecht, & Zimbelman, 2012). Deteksi kecurangan sangat penting karena kecurangan dapat merusak integritas finansial institusi, mengurangi kepercayaan pemangku kepentingan, dan berpotensi menyebabkan kerugian finansial yang signifikan.

Deteksi kecurangan melibatkan penggunaan berbagai teknik dan alat untuk mengidentifikasi tindakan kecurangan, termasuk analisis data, audit internal, pengawasan regulasi, dan penggunaan teknologi informasi. Tujuan utama deteksi kecurangan adalah untuk mengidentifikasi aktivitas mencurigakan secara dini, sehingga langkah-langkah pencegahan dapat

diambil sebelum kecurangan menyebabkan kerugian yang lebih besar (Singleton, Singleton, Bologna, & Lindquist, 2006).

Metode dan Teknik Deteksi Kecurangan

Terdapat beberapa metode dan teknik yang digunakan dalam deteksi kecurangan di institusi keuangan. Beberapa di antaranya meliputi:

1) Audit Internal dan Eksternal: Audit merupakan salah satu alat paling efektif untuk mendeteksi kecurangan. Auditor memeriksa catatan keuangan, meninjau sistem kontrol internal, dan melakukan tes substantif untuk mengidentifikasi transaksi yang tidak wajar atau mencurigakan (Asare, Wright, & Zimbelman, 2021). Audit internal fokus pada penilaian risiko internal dan sistem pengendalian, sementara audit eksternal memberikan perspektif independen tentang keandalan laporan keuangan (Arens, Elder, & Beasley, 2017).
2) Analisis Data dan Forensik Keuangan: Analisis data menggunakan teknologi seperti data mining dan machine learning untuk menganalisis pola transaksi dan mengidentifikasi anomali yang mungkin mengindikasikan kecurangan (Chen, Hsieh, & Huang, 2021). Forensik keuangan, di sisi lain, melibatkan pemeriksaan rinci terhadap catatan keuangan untuk menemukan bukti kecurangan, seperti manipulasi laporan keuangan atau penggelapan aset (Wells, 2017).
3) Sistem Pengawasan dan Kepatuhan: Penggunaan teknologi pengawasan seperti sistem deteksi intrusi dan software kepatuhan membantu dalam pemantauan aktivitas keuangan secara real-time dan memastikan bahwa transaksi sesuai dengan kebijakan dan regulasi yang berlaku (Rezaee & Riley, 2019). Sistem ini dapat mendeteksi aktivitas mencurigakan dan memberikan peringatan dini kepada manajemen.
4) Whistleblowing dan Pelaporan Anonim: Sistem pelaporan anonim atau whistleblowing memungkinkan karyawan atau pihak ketiga untuk melaporkan kecurangan tanpa takut akan pembalasan. Ini merupakan alat penting dalam deteksi kecurangan karena banyak kecurangan yang terungkap melalui laporan dari orang dalam (Miceli & Near, 2013).

4. Upaya Remediasi dan Perbaikan

Dari hasil analisis, diperlukan upaya remediasi dan perbaikan yang komprehensif dalam meningkatkan efektivitas sistem kontrol TI, prosedur audit, dan deteksi kecurangan di institusi keuangan. Hal ini termasuk pengembangan sistem kontrol TI yang lebih kuat, peningkatan pelatihan auditor, penerapan teknologi deteksi kecurangan yang canggih, serta peningkatan koordinasi antara departemen internal dan otoritas pengawas keuangan.

Proses remediasi melibatkan beberapa langkah penting yang memastikan perbaikan dilakukan secara menyeluruh dan efektif. Langkah-langkah tersebut meliputi:

1) Identifikasi Masalah: Langkah pertama dalam proses remediasi adalah mengidentifikasi masalah atau kelemahan yang ada. Ini biasanya dilakukan melalui audit, inspeksi, atau penggunaan teknologi deteksi kecurangan. Identifikasi masalah memungkinkan organisasi untuk memahami akar penyebab dari masalah tersebut (Wells, 2017).
2) Analisis dan Penilaian: Setelah masalah diidentifikasi, langkah berikutnya adalah menganalisis dan menilai dampak dari masalah tersebut. Ini melibatkan evaluasi risiko yang ditimbulkan oleh kelemahan tersebut dan menentukan prioritas untuk perbaikan. Analisis yang menyeluruh membantu dalam memahami sejauh mana masalah dapat mempengaruhi operasi dan bagaimana dampak tersebut dapat diminimalkan (COSO, 2013).
3) Pengembangan Rencana Perbaikan: Berdasarkan analisis, langkah selanjutnya adalah mengembangkan rencana perbaikan yang komprehensif. Rencana ini harus mencakup tindakan spesifik yang diperlukan untuk memperbaiki kelemahan, serta menetapkan tanggung jawab, tenggat waktu, dan sumber daya yang dibutuhkan untuk melaksanakan perbaikan (ISACA, 2012).
4) Implementasi Solusi: Implementasi melibatkan pelaksanaan rencana perbaikan. Ini mungkin termasuk perubahan prosedur operasional, peningkatan teknologi, pelatihan staf, atau penerapan kebijakan baru. Implementasi harus dilakukan dengan hati-hati untuk memastikan bahwa semua aspek perbaikan telah dipertimbangkan dan masalah telah diatasi secara efektif (Wells, 2017).

5) Pengujian dan Validasi: Setelah solusi diimplementasikan, langkah penting selanjutnya adalah menguji dan memvalidasi efektivitas perbaikan yang dilakukan. Ini dapat dilakukan melalui pengujian sistem, audit ulang, atau simulasi skenario untuk memastikan bahwa kelemahan telah diperbaiki dan tidak akan muncul kembali (Symantec, 2015).
6) Monitoring dan Tinjauan Berkelanjutan: Remediasi yang efektif membutuhkan pemantauan berkelanjutan untuk memastikan bahwa perbaikan tetap efektif dari waktu ke waktu. Ini melibatkan pengawasan sistem secara terus-menerus dan melakukan tinjauan berkala untuk mengidentifikasi potensi masalah baru yang mungkin muncul (Gantz & Philpott, 2012).

KESIMPULAN

Penelitian ini menyoroti pentingnya evaluasi efektivitas sistem kontrol teknologi informasi (TI), prosedur audit, dan deteksi kecurangan dalam institusi keuangan. Dari analisis yang dilakukan, terungkap bahwa sistem kontrol TI yang kuat dan terintegrasi dapat secara signifikan mengurangi risiko kecurangan dengan meningkatkan visibilitas dan transparansi operasional. Kontrol TI yang efektif membantu dalam pemantauan berkelanjutan terhadap aktivitas yang mencurigakan dan menyediakan mekanisme deteksi dini untuk mencegah terjadinya kecurangan. Hasil studi ini sejalan dengan teori-teori yang ada, yang menekankan bahwa teknologi informasi tidak hanya berperan dalam mendukung operasional tetapi juga menjadi alat kritis dalam manajemen risiko dan kepatuhan.

Selain itu, penelitian ini menekankan perlunya prosedur audit yang lebih ketat dan sistematis untuk meningkatkan akurasi dan reliabilitas dalam deteksi kecurangan. Audit yang dilakukan dengan metode dan teknologi canggih memungkinkan identifikasi pola-pola kecurangan yang kompleks dan tidak mudah terlihat. Penemuan baru dari penelitian ini menunjukkan bahwa kombinasi antara sistem kontrol TI yang efektif, prosedur audit yang menyeluruh, dan teknik deteksi kecurangan yang inovatif dapat menciptakan lingkungan keuangan yang lebih aman dan terpercaya. Dengan demikian, institusi keuangan dapat meningkatkan kepercayaan stakeholder dan mencegah kerugian finansial yang signifikan akibat kecurangan.

DAFTAR PUSTAKA

Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2012). Fraud Examination. Cengage Learning.

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big Data and Analytics in the Modern Audit Engagement: Research Needs. Auditing: A Journal of Practice & Theory, 36(4), 1-27.

Arens, A. A., Elder, R. J., & Beasley, M. S. (2017). Auditing and Assurance Services. Pearson.

Bartlett, R. P., Morse, A., Stanton, R., & Wallace, N. (2019). Consumer Lending Discrimination in the FinTech Era. Journal of Law and Economics, 62(3), 411-452.

Bhasin, M. L. (2015). Menace of Frauds in the Indian Banking Industry: An Empirical Study. Australian Journal of Business and Management Research, 4(12), 21-33.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.

Brown-Liburd, H. L., Cohen, J. R., & Zamora, V. L. (2018). The Effect of Corporate Social Responsibility Investment, Assurance, and Perceived Fairness on Investors' Judgments. Journal of Business Ethics, 152(4), 997-1013.

Carnes, K. C., & Gierlasinski, N. J. (2001). Detection and Prevention of Financial Statement Fraud: A Guide for Practitioners and Educators. Journal of Forensic Accounting, 2, 1-35.

Chen, H., Hsieh, Y. Y., & Huang, L. H. (2021). Using Data Mining for Fraud Detection: An Overview and a Case Study in Online Transactions. Journal of Information Systems, 35(1), 93-111.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal Control — Integrated Framework. AICPA.

Cressey, D. R. (1953). Other People’s Money: A Study in the Social Psychology of Embezzlement. Glencoe, IL: Free Press.

Creswell, J. W., & Creswell, J. D. (2017). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). Sage Publications.

Franks, J. R., & Vest, M. (2018). Regulatory Capture in Financial Markets: Lessons from the Bank of England's Libor Scandal. Journal of Financial Regulation, 4(1), 91-110.

Gantz, S. D., & Philpott, D. R. (2012). FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security. Syngress.

Gramling, A. A., Maletta, M. J., Schneider, A., & Church, B. K. (2004). The role of the internal audit function in corporate governance: A synthesis of the extant internal auditing literature and directions for future research. Journal of Accounting Literature, 23, 194-244.

Hayes, R., Dassen, R., Schilder, A., & Wallage, P. (2004). Principles of Auditing: An Introduction to International Standards on Auditing. Pearson Education.

ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA.

Kirkos, E. (2020). Detecting Fraud in Financial Statements: A Data Mining Approach. Journal of Financial Crime, 27(2), 453-467.

Knechel, W. R. (2016). Audit Research in the Wake of SOX. Accounting Horizons, 30(4), 699-714.

Merriam, S. B. (2009). Qualitative Research: A Guide to Design and Implementation. Jossey-Bass.

Messier, W. F., Glover, S. M., & Prawitt, D. F. (2018). Auditing and Assurance Services: A Systematic Approach. McGraw-Hill Education.

Miceli, M. P., & Near, J. P. (2013). An International Comparison of the Incidence of Public Whistle-blowing: Japan, Norway, and the US. Scandinavian Journal of Management, 29(1), 50-63.

Mills, C. B., & Pashler, H. (2014). Attention and Psychomotor Efficiency in Humans. Springer.

Mock, T. J., Srivastava, R. P., & Wright, A. M. (2017). The Use of Analytical Procedures: Evidence from Audit Practice and Research. Auditing: A Journal of Practice & Theory, 36(2), 31-55.

Patton, M. Q. (2015). Qualitative Research & Evaluation Methods: Integrating Theory and Practice. Sage Publications.

PwC. (2019). Global Economic Crime and Fraud Survey 2018. PwC.

Rezaee, Z., & Riley, R. A. (2019). Financial Statement Fraud: Prevention and Detection. Wiley.

Singleton, T. W., Singleton, A. J., Bologna, G. J., & Lindquist, R. J. (2006). Fraud Auditing and Forensic Accounting. Wiley.

Soh, D. S., & Martinov-Bennie, N. (2018). The internal audit function: Perceptions of internal audit roles, effectiveness, and reporting relationships. Managerial Auditing Journal, 26(7), 605-622.

Sun, L., Srivastava, R. P., & Mock, T. J. (2006). Detection of Management Fraud: A Neural Network Approach. International Journal of Accounting Information Systems, 7(3), 264-278.

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.

Symantec. (2015). The Symantec Guide to Enterprise Security. Symantec Press.

Tiwari, A. K., & Debnath, A. (2017). Fraud Detection in Indian Banks: Data Mining Approach. International Journal of Business and Management Invention, 6(5), 45-52.

Wells, J. T. (2017). Corporate Fraud Handbook: Prevention and Detection. Wiley.

Whittington, R., & Pany, K. (2019). Principles of Auditing & Other Assurance Services. McGraw-Hill Education.

Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. CPA Journal, 74(12), 38-42.

Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). Sage Publications.