Jurnal Publikasi Ekonomi dan Akuntansi
Volume 5 Nomor 2 Mei 2025
E-ISSN : 2808-9006; P-ISSN 2808-9391, Hal : 78-86
DOI: 10.55606/jupea.v5i2.3876
Available online at: https://journalcenter.org/index.php/jupea

Peran Sistem Informasi Akuntansi Dalam Mengidentifikasi Dan Mencegah Kecurangan Pada Penyalahgunaan Akses Internal Perusahaan

Muhammad Riyan Dani [1], Erik Martua Simatupang [2], Arif Anakampun[3], Yolanda Pratiwi [4], Dea Natalia[5], Rivana Perangin-angin[6], Jufri Darma [7]
[1,2,3,4,5,6,7]Universitas Negeri Medan
Email: [1]riyandani816@gmail.com,[2] eriksimatupang291104@gmail.com,[3] arifanakampin79@gmail.com,[4] yolandapratiwi584@gmail.com,[5] deanataliaw@gmail.com [6] rivanaperangin.angin5@gmail.com,[7] jufridarma@unimed.ac.id

Alamat: Kenangan Baru, Kec. Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara
Korespondensi Penulias: riyandani816@gmail.com

Abstract: *Internal access abuse is a form of fraud that can significantly harm a company, both financially and reputationally. Therefore, it is essential for companies to implement effective preventive measures to protect the integrity of their information systems and assets. This article discusses various strategies that can be applied to prevent fraud, including the implementation of strong internal controls, segregation of duties, and strict access controls. Additionally, features such as audit trails, clear security policies, and the use of advanced security technologies are key elements in detecting and preventing access abuse. Building a culture of ethics and transparency within the company, as well as providing ongoing education and training to employees, is also crucial for raising awareness of fraud risks. Conducting regular audits and risk assessments can help companies identify potential weaknesses in their internal control systems. By adopting a comprehensive and integrated approach, companies can protect their assets, maintain operational integrity, and build trust among employees and stakeholders, ultimately contributing to the long-term success of the organization.*
Keywords: *Fraud, Internal Control, Access Control*
Abstrak: Penyalahgunaan akses internal merupakan salah satu bentuk kecurangan yang dapat merugikan perusahaan secara signifikan, baik dari segi finansial maupun reputasi. Oleh karena itu, penting bagi perusahaan untuk menerapkan langkah-langkah pencegahan yang efektif untuk melindungi integritas sistem informasi dan aset yang dimiliki. Artikel ini membahas berbagai strategi yang dapat diterapkan untuk mencegah kecurangan, termasuk penerapan pengendalian internal yang kuat, pemisahan tugas, dan kontrol akses yang ketat. Selain itu, fitur audit trail, kebijakan keamanan yang jelas, dan penggunaan teknologi keamanan canggih juga menjadi elemen kunci dalam mendeteksi dan mencegah penyalahgunaan akses. Membangun budaya etika dan transparansi di dalam perusahaan, serta memberikan pendidikan dan pelatihan berkelanjutan kepada karyawan, juga sangat penting untuk meningkatkan kesadaran akan risiko kecurangan. Melakukan audit dan penilaian risiko secara berkala dapat membantu perusahaan mengidentifikasi potensi kelemahan dalam sistem pengendalian internal. Dengan menerapkan pendekatan yang komprehensif dan terintegrasi, perusahaan dapat melindungi asetnya, menjaga integritas operasional, dan membangun kepercayaan di antara karyawan dan pemangku kepentingan, yang pada akhirnya berkontribusi pada keberhasilan jangka panjang perusahaan.
Kata kunci: Kecurangan, Pengendalian Internal, Kontrol akses.

1. PENDAHULUAN

Sistem Informasi Akuntansi (SIA) memiliki peran yang sangat penting dalam mengidentifikasi dan mencegah kecurangan, terutama dalam konteks penyalahgunaan akses internal perusahaan. Dalam era digital saat ini, di mana informasi dapat diakses dengan mudah dan cepat, risiko kecurangan semakin meningkat. Penyalahgunaan akses internal sering kali

Received: Maret 03, 2025; Revised: Maret 12, 2025; Accepted: April 22, 2025; Published: Mei 05, 2025;
**riyandani816@gmail.com*

terjadi ketika individu yang memiliki otoritas dalam sistem menggunakan akses tersebut untuk kepentingan pribadi, seperti manipulasi data keuangan atau penggelapan aset (Internal, Sukadwilinda, and Ratnawati 2013). Oleh karena itu, SIA yang dirancang dengan baik dapat menjadi alat yang efektif untuk mendeteksi dan mencegah tindakan kecurangan ini (Supriyanto et al. 2022). SIA berfungsi sebagai pengendali yang dapat memantau dan mencatat setiap transaksi yang terjadi dalam perusahaan. Dengan adanya sistem yang terintegrasi, setiap aktivitas yang dilakukan oleh karyawan dapat direkam secara otomatis, sehingga memudahkan dalam melakukan audit dan penelusuran jika terjadi kecurangan (Udayani and Sari 2017). Selain itu, SIA juga dilengkapi dengan fitur keamanan yang dapat membatasi akses pengguna berdasarkan peran dan tanggung jawab mereka. Hal ini penting untuk memastikan bahwa hanya individu yang berwenang yang dapat mengakses informasi sensitif, sehingga mengurangi kemungkinan penyalahgunaan. Penerapan pengendalian internal yang kuat dalam SIA juga berkontribusi pada pencegahan kecurangan. Misalnya, dengan adanya pemisahan tugas, di mana satu orang tidak dapat melakukan seluruh proses transaksi tanpa melibatkan pihak lain, dapat mengurangi risiko kecurangan. Selain itu, sistem ini juga dapat memberikan laporan yang transparan dan akurat, sehingga manajemen dapat dengan mudah memantau kinerja keuangan dan mendeteksi anomali yang mungkin menunjukkan adanya kecurangan.

Pelatihan dan kesadaran karyawan juga menjadi faktor penting. Karyawan yang memahami pentingnya integritas dan etika dalam penggunaan SIA akan lebih cenderung untuk tidak melakukan tindakan yang merugikan perusahaan. Oleh karena itu, perusahaan perlu menginvestasikan waktu dan sumber daya untuk memberikan pelatihan yang memadai mengenai penggunaan SIA dan implikasi dari kecurangan (Putri, Juliharta, and Darmawan 2025) . SIA berfungsi sebagai pengendali yang dapat memantau dan mencatat setiap transaksi yang terjadi dalam perusahaan. Dengan adanya sistem yang terintegrasi, setiap aktivitas yang dilakukan oleh karyawan dapat direkam secara otomatis, sehingga memudahkan dalam melakukan audit dan penelusuran jika terjadi kecurangan. Selain itu, SIA juga dilengkapi dengan fitur keamanan yang dapat membatasi akses pengguna berdasarkan peran dan tanggung jawab mereka (Alou, Ilat, and Gamaliel 2017). Hal ini penting untuk memastikan bahwa hanya individu yang berwenang yang dapat mengakses informasi sensitif, sehingga mengurangi kemungkinan penyalahgunaan. Penerapan pengendalian internal yang kuat dalam SIA juga berkontribusi pada pencegahan kecurangan. Misalnya, dengan adanya pemisahan tugas, di mana satu orang tidak dapat melakukan seluruh proses transaksi tanpa melibatkan pihak lain, dapat mengurangi risiko kecurangan. Selain itu, sistem ini juga dapat memberikan laporan yang transparan dan akurat, sehingga manajemen dapat dengan mudah memantau kinerja keuangan dan mendeteksi anomali yang mungkin menunjukkan adanya kecurangan Pelatihan dan kesadaran karyawan juga menjadi faktor penting (Aprilia 2017). Karyawan yang memahami pentingnya integritas dan etika dalam penggunaan SIA akan lebih cenderung untuk tidak melakukan tindakan yang merugikan perusahaan. Oleh karena itu, perusahaan perlu menginvestasikan waktu dan sumber daya untuk memberikan pelatihan yang memadai mengenai penggunaan SIA dan implikasi dari kecurangan.

Peran SIA dalam mengidentifikasi dan mencegah kecurangan pada penyalahgunaan akses internal perusahaan sangatlah krusial. Dengan sistem yang tepat, pengendalian internal yang kuat, dan kesadaran karyawan, perusahaan dapat meminimalkan risiko kecurangan dan menjaga integritas laporan keuangan (Novida 2025). Hal ini tidak hanya melindungi aset perusahaan, tetapi juga membangun kepercayaan dari pemangku kepentingan dan meningkatkan reputasi perusahaan di pasar. Dengan demikian, SIA bukan hanya sekadar alat akuntansi, tetapi juga merupakan benteng pertahanan yang vital dalam menjaga kejujuran dan transparansi dalam operasional perusahaan.

2. METODE

Metode yang digunakan dalam penelitian ini adalah metode kualitatif dengan pendekatan studi literatur. Metode kualitatif memungkinkan peneliti untuk mengeksplorasi fenomena secara mendalam, memahami konteks, dan menggali makna dari berbagai sumber informasi yang relevan (Rodiah, Ardianni, and Herlina 2019). Dalam konteks peran Sistem Informasi Akuntansi (SIA) dalam mengidentifikasi dan mencegah kecurangan, pendekatan studi literatur menjadi sangat penting karena memberikan landasan teoritis yang kuat serta wawasan dari penelitian sebelumnya. Melalui studi literatur, peneliti dapat mengumpulkan data dari berbagai sumber, seperti artikel jurnal, buku, laporan penelitian, dan dokumen lainnya yang berkaitan dengan SIA dan kecurangan (Fitriani 2023). Proses ini melibatkan identifikasi, analisis, dan sintesis informasi yang ada untuk mendapatkan pemahaman yang komprehensif mengenai topik yang diteliti. Dengan cara ini, peneliti dapat mengidentifikasi pola, tema, dan hubungan antara konsep-konsep yang ada dalam literatur, serta mengaitkannya dengan konteks yang lebih luas. Salah satu keuntungan dari metode ini adalah kemampuannya untuk memberikan perspektif yang beragam mengenai peran SIA. Misalnya, peneliti dapat menemukan berbagai pandangan tentang bagaimana SIA dapat berfungsi sebagai alat pengendalian yang efektif dalam mendeteksi dan mencegah kecurangan. Selain itu, studi literatur juga memungkinkan peneliti untuk mengeksplorasi berbagai praktik terbaik yang telah diterapkan oleh perusahaan lain dalam menggunakan SIA untuk mengurangi risiko kecurangan.

Peneliti juga dapat mengevaluasi efektivitas pengendalian internal yang diterapkan dalam SIA. Misalnya, banyak penelitian menunjukkan bahwa penerapan prinsip pemisahan tugas dan otorisasi transaksi dapat mengurangi kemungkinan terjadinya kecurangan. Dengan memahami bagaimana pengendalian internal berfungsi dalam konteks SIA, peneliti dapat memberikan rekomendasi yang lebih baik bagi perusahaan dalam merancang sistem yang lebih aman dan efektif. Pentingnya pelatihan dan kesadaran karyawan juga menjadi fokus dalam studi literatur ini. Penelitian menunjukkan bahwa karyawan yang dilatih dengan baik mengenai etika dan penggunaan SIA cenderung lebih bertanggung jawab dan tidak terlibat dalam tindakan kecurangan. Oleh karena itu, perusahaan perlu menginvestasikan waktu dan sumber daya untuk program pelatihan yang berkelanjutan. Metode kualitatif dengan pendekatan studi literatur memberikan wawasan yang mendalam mengenai peran SIA dalam mengidentifikasi dan mencegah kecurangan. Dengan mengumpulkan dan menganalisis informasi dari berbagai sumber, peneliti dapat menyusun gambaran yang lebih jelas tentang bagaimana SIA dapat berfungsi sebagai alat pengendalian yang efektif dalam menjaga integritas dan transparansi dalam operasional perusahaan

3. HASIL DAN PEMBAHASAN

Dalam era digital yang semakin maju, peran Sistem Informasi Akuntansi (SIA) dalam mengidentifikasi dan mencegah kecurangan, khususnya terkait penyalahgunaan akses internal perusahaan, menjadi semakin krusial. Hasil dari studi literatur menunjukkan bahwa SIA tidak hanya berfungsi sebagai alat pencatatan transaksi, tetapi juga sebagai sistem pengendalian yang dapat mendeteksi dan mencegah tindakan kecurangan yang mungkin dilakukan oleh individu dengan akses internal (Marselina Rachma, Sapitri, and Novelina 2024). Pembahasan ini akan menguraikan beberapa aspek penting dari peran SIA dalam konteks tersebut, termasuk fitur pengendalian internal, keamanan sistem, dan kesadaran karyawan.

A. Fitur Pengendalian Internal

Fitur pengendalian internal dalam Sistem Informasi Akuntansi (SIA) merupakan elemen krusial yang berfungsi untuk mencegah kecurangan dan penyalahgunaan akses internal. Berikut adalah beberapa poin penting yang menjelaskan lebih rinci mengenai fitur ini:

1) Pemisahan Tugas (Segregation of Duties):

Prinsip ini mengharuskan bahwa tidak ada satu individu pun yang memiliki kontrol penuh atas seluruh proses transaksi. Misalnya, satu orang tidak boleh bertanggung jawab untuk membuat, memverifikasi, dan menyetujui transaksi yang sama. Dengan cara ini, jika satu individu berusaha melakukan kecurangan, tindakan tersebut akan lebih mudah terdeteksi karena melibatkan lebih dari satu orang.

2) Audit Trail:

Fitur audit trail mencatat semua aktivitas yang dilakukan dalam sistem, termasuk siapa yang melakukan perubahan, kapan perubahan tersebut dilakukan, dan jenis perubahan yang dilakukan. Ini memberikan jejak yang jelas dan dapat ditelusuri, sehingga memudahkan perusahaan dalam melakukan investigasi jika terjadi kecurangan.

3) Kontrol Akses:

SIA harus dilengkapi dengan kontrol akses yang ketat, di mana pengguna hanya dapat mengakses informasi dan fungsi yang sesuai dengan peran dan tanggung jawab mereka. Hal ini mengurangi risiko penyalahgunaan akses oleh individu yang tidak berwenang.

4) Pemberitahuan dan Laporan:

Sistem dapat diatur untuk memberikan pemberitahuan otomatis kepada manajemen jika terjadi aktivitas yang mencurigakan atau tidak biasa. Laporan berkala mengenai aktivitas pengguna juga dapat membantu dalam memantau dan mengevaluasi kepatuhan terhadap kebijakan pengendalian internal.

5) Evaluasi dan Peninjauan Berkala:

Pengendalian internal harus dievaluasi dan ditinjau secara berkala untuk memastikan efektivitasnya. Perusahaan perlu melakukan audit internal untuk mengidentifikasi potensi kelemahan dalam sistem dan melakukan perbaikan yang diperlukan.

Fitur pengendalian internal dalam Sistem Informasi Akuntansi memainkan peran yang sangat penting dalam mencegah kecurangan dan menjaga integritas data. Dengan menerapkan prinsip pemisahan tugas, otorisasi, audit trail, kontrol akses, dan langkah- langkah lainnya, perusahaan dapat menciptakan lingkungan yang aman dan transparan. Selain itu, pelatihan dan kesadaran karyawan juga merupakan faktor kunci dalam memastikan bahwa pengendalian internal berfungsi dengan baik (Prasetyo 2014). Dengan demikian, SIA tidak hanya berfungsi sebagai alat akuntansi, tetapi juga sebagai sistem pengendalian yang efektif untuk melindungi aset dan reputasi perusahaan.

B. Keamanan Sistem dalam Sistem Informasi Akuntansi

Keamanan sistem merupakan aspek yang sangat penting dalam Sistem Informasi Akuntansi (SIA) untuk melindungi data sensitif dan mencegah penyalahgunaan akses internal (Supriyanto et al. 2022). Berikut adalah beberapa poin yang menjelaskan lebih lanjut mengenai keamanan sistem dalam konteks SIA:

1) Otentikasi Pengguna:

Proses otentikasi pengguna adalah langkah pertama dalam menjaga keamanan sistem. Pengguna harus memasukkan kredensial yang valid, seperti nama pengguna dan kata sandi, untuk mengakses SIA. Penggunaan kata sandi yang kuat dan kompleks sangat dianjurkan untuk mengurangi risiko akses tidak sah. Selain itu, penerapan autentikasi dua faktor (2FA) dapat memberikan lapisan keamanan tambahan dengan meminta pengguna untuk memasukkan kode yang dikirimkan ke perangkat mereka.

2) Enkripsi Data:

Enkripsi adalah proses mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang tepat. Dengan mengenkripsi data sensitif, seperti informasi keuangan dan data pribadi karyawan, perusahaan dapat melindungi informasi tersebut dari akses yang tidak sah, baik saat data disimpan maupun saat data ditransmisikan melalui jaringan.

3) Kontrol Akses Berbasis Peran (Role-Based Access Control - RBAC):

RBAC adalah metode yang membatasi akses pengguna berdasarkan peran mereka dalam organisasi. Dengan cara ini, setiap pengguna hanya dapat mengakses informasi dan fungsi yang relevan dengan tugas mereka. Misalnya, seorang akuntan mungkin memiliki akses untuk memasukkan data transaksi, tetapi tidak untuk mengubah pengaturan sistem. Ini membantu mencegah penyalahgunaan akses oleh individu yang tidak berwenang.

4) Pemantauan dan Deteksi Ancaman:

Sistem SIA harus dilengkapi dengan alat pemantauan yang dapat mendeteksi aktivitas mencurigakan atau tidak biasa. Misalnya, jika ada upaya login yang gagal berulang kali dari alamat IP yang tidak dikenal, sistem dapat mengirimkan peringatan kepada administrator. Pemantauan yang proaktif memungkinkan perusahaan untuk merespons ancaman dengan cepat sebelum kerusakan terjadi.

5) Pembaruan dan Pemeliharaan Sistem:

Keamanan sistem juga bergantung pada pemeliharaan dan pembaruan perangkat lunak secara berkala. Perusahaan harus memastikan bahwa semua perangkat lunak, termasuk SIA, diperbarui dengan patch keamanan terbaru untuk melindungi dari kerentanan yang diketahui. Selain itu, audit keamanan rutin harus dilakukan untuk mengidentifikasi dan mengatasi potensi kelemahan dalam sistem.

6) Pelatihan Kesadaran Keamanan:

Karyawan merupakan garis pertahanan pertama dalam menjaga keamanan sistem. Oleh karena itu, perusahaan perlu memberikan pelatihan yang memadai mengenai praktik keamanan yang baik, seperti cara mengenali phishing, pentingnya menjaga kerahasiaan kata sandi, dan langkah-langkah yang harus diambil jika mereka mencurigai adanya pelanggaran keamanan.

Dengan menerapkan langkah-langkah keamanan yang komprehensif ini, perusahaan dapat melindungi SIA mereka dari ancaman internal dan eksternal, serta menjaga integritas dan kerahasiaan data yang dikelola. Keamanan sistem yang kuat tidak hanya melindungi aset perusahaan, tetapi juga membangun kepercayaan di antara karyawan dan pemangku kepentingan, yang pada gilirannya dapat meningkatkan reputasi perusahaan di pasar.

C. Pencegahan Kecurangan pada Penyalahgunaan Akses Internal Perusahaan

Penyalahgunaan akses internal adalah salah satu tantangan serius yang dihadapi oleh banyak perusahaan. Karyawan yang memiliki akses ke sistem informasi dan data sensitif dapat dengan mudah melakukan tindakan yang merugikan perusahaan, seperti manipulasi data, pencurian aset, atau penggelapan (Ii 2015). Oleh karena itu, penting bagi perusahaan untuk mengimplementasikan strategi yang efektif untuk mencegah kecurangan ini. Berikut adalah beberapa pendekatan dan strategi yang dapat diterapkan:

1) Implementasi Kebijakan Keamanan yang Jelas

Perusahaan harus memiliki kebijakan keamanan yang jelas dan terperinci mengenai penggunaan sistem informasi. Kebijakan ini harus mencakup aturan tentang siapa yang memiliki akses ke data tertentu, bagaimana data harus dikelola, dan konsekuensi dari

pelanggaran kebijakan. Dengan adanya kebijakan yang jelas, karyawan akan lebih memahami batasan dan tanggung jawab mereka, serta risiko yang terkait dengan penyalahgunaan akses.

2) Penggunaan Teknologi Keamanan yang Canggih

Teknologi keamanan yang canggih, seperti sistem deteksi intrusi (IDS) dan perangkat lunak pemantauan aktivitas pengguna, dapat membantu perusahaan dalam mendeteksi dan mencegah penyalahgunaan akses. Sistem ini dapat memberikan peringatan kepada manajemen jika ada aktivitas yang mencurigakan, seperti upaya login yang tidak sah atau perubahan data yang tidak biasa. Dengan pemantauan yang proaktif, perusahaan dapat mengambil tindakan cepat sebelum kerugian terjadi.

3) Penerapan Otentikasi Multi-Faktor (MFA)

Otentikasi multi-faktor adalah metode yang menambahkan lapisan keamanan tambahan dengan meminta pengguna untuk memberikan lebih dari satu bentuk identifikasi sebelum mengakses sistem (Senapan et al. 2022). Misalnya, selain memasukkan kata sandi, pengguna juga harus memasukkan kode yang dikirimkan ke ponsel mereka . Dengan menerapkan MFA, perusahaan dapat mengurangi risiko akses tidak sah, bahkan jika kata sandi pengguna telah dicuri.

4) Audit dan Penilaian Risiko Secara Berkala

Melakukan audit dan penilaian risiko secara berkala adalah langkah penting dalam mengidentifikasi potensi kelemahan dalam sistem pengendalian internal. Audit ini harus mencakup evaluasi terhadap kebijakan keamanan, kontrol akses, dan kepatuhan terhadap prosedur yang telah ditetapkan. Dengan melakukan audit secara rutin, perusahaan dapat menemukan dan memperbaiki celah yang dapat dimanfaatkan oleh individu yang berniat jahat.

5) Membangun Budaya Etika dan Transparansi

Membangun budaya perusahaan yang menekankan etika dan transparansi sangat penting dalam mencegah kecurangan. Perusahaan harus mendorong karyawan untuk berbicara tentang masalah etika dan memberikan saluran yang aman untuk melaporkan aktivitas mencurigakan (Alifiananda et al. 2021). Ketika karyawan merasa bahwa mereka dapat melaporkan masalah tanpa takut akan pembalasan, mereka akan lebih cenderung untuk melaporkan potensi penyalahgunaan akses.

6) Pendidikan dan Pelatihan Berkelanjutan

Pendidikan dan pelatihan berkelanjutan mengenai keamanan informasi dan etika bisnis harus menjadi bagian integral dari program pengembangan karyawan (Karlina Ghazalah Rahman, Siti Nur Reskiyawati Said 2022). Pelatihan ini harus mencakup cara mengenali tanda-tanda penyalahgunaan akses, pentingnya menjaga kerahasiaan informasi, dan prosedur pelaporan yang tepat. Dengan meningkatkan kesadaran karyawan, perusahaan dapat menciptakan lingkungan yang lebih aman dan mengurangi risiko kecurangan.

7) Penerapan Teknologi Blockchain

Meskipun masih dalam tahap pengembangan di banyak sektor, teknologi blockchain menawarkan potensi untuk meningkatkan keamanan dan transparansi dalam pengelolaan data. Dengan menggunakan blockchain, setiap transaksi dicatat dalam buku besar yang tidak dapat diubah, sehingga meminimalkan risiko manipulasi data. Meskipun penerapannya mungkin memerlukan investasi awal yang signifikan, manfaat jangka panjang dalam hal keamanan dan kepercayaan dapat sangat berharga.

Mencegah kecurangan pada penyalahgunaan akses internal perusahaan memerlukan pendekatan yang holistik dan terintegrasi (Febrianti, Mulyadi, and Setiawan 2021). Dengan

mengimplementasikan kebijakan keamanan yang jelas, menggunakan teknologi canggih, menerapkan otentikasi multi-faktor, melakukan audit berkala, membangun budaya etika, dan memberikan pelatihan yang berkelanjutan, perusahaan dapat secara signifikan mengurangi risiko kecurangan. Langkah-langkah ini tidak hanya melindungi aset perusahaan, tetapi juga membangun kepercayaan di antara karyawan dan pemangku kepentingan, yang pada akhirnya berkontribusi pada keberhasilan jangka panjang perusahaan.

4. KESIMPULAN

Penyalahgunaan akses internal perusahaan menunjukkan bahwa perlunya pendekatan yang komprehensif dan terintegrasi untuk melindungi integritas sistem informasi dan aset perusahaan. Penyalahgunaan akses internal dapat menimbulkan kerugian yang signifikan, baik dari segi finansial maupun reputasi, sehingga perusahaan harus proaktif dalam menerapkan langkah-langkah pencegahan yang efektif. Salah satu langkah utama yang harus diambil adalah penerapan pengendalian internal yang kuat, yang mencakup prinsip pemisahan tugas. Dengan memisahkan tanggung jawab di antara beberapa individu, perusahaan dapat mengurangi risiko kecurangan, karena tidak ada satu orang pun yang memiliki kontrol penuh atas seluruh proses transaksi. Selain itu, kontrol akses yang ketat juga sangat penting untuk membatasi siapa saja yang dapat mengakses informasi sensitif dan melakukan tindakan tertentu dalam sistem. Dengan memberikan akses hanya kepada individu yang berwenang, perusahaan dapat mencegah penyalahgunaan oleh karyawan yang tidak memiliki hak. Fitur audit trail juga menjadi elemen kunci dalam mencegah kecurangan. Dengan mencatat semua aktivitas yang dilakukan dalam sistem, audit trail memungkinkan perusahaan untuk melacak tindakan yang mencurigakan dan melakukan investigasi jika diperlukan. Ini memberikan transparansi dan akuntabilitas dalam penggunaan sistem, sehingga memudahkan deteksi dini terhadap potensi penyalahgunaan. Selain itu, perusahaan harus memiliki kebijakan keamanan yang jelas dan terperinci mengenai penggunaan sistem informasi. Kebijakan ini harus mencakup aturan tentang siapa yang memiliki akses ke data tertentu, bagaimana data harus dikelola, dan konsekuensi dari pelanggaran kebijakan. Dengan adanya kebijakan yang jelas, karyawan akan lebih memahami batasan dan tanggung jawab mereka.

Penggunaan teknologi keamanan yang canggih, seperti sistem deteksi intrusi dan perangkat lunak pemantauan aktivitas pengguna, juga sangat dianjurkan. Teknologi ini dapat memberikan peringatan kepada manajemen jika ada aktivitas yang mencurigakan, sehingga memungkinkan perusahaan untuk mengambil tindakan cepat sebelum kerugian terjadi. Selain itu, penerapan otentikasi multi-faktor (MFA) dapat menambah lapisan keamanan tambahan dengan meminta pengguna untuk memberikan lebih dari satu bentuk identifikasi sebelum mengakses sistem. Ini sangat penting untuk mengurangi risiko akses tidak sah, bahkan jika kata sandi pengguna telah dicuri. Membangun budaya etika dan transparansi di dalam perusahaan juga merupakan langkah penting dalam mencegah kecurangan. Perusahaan harus mendorong karyawan untuk berbicara tentang masalah etika dan memberikan saluran yang aman untuk melaporkan aktivitas mencurigakan. Ketika karyawan merasa bahwa mereka dapat melaporkan masalah tanpa takut akan pembalasan, mereka akan lebih cenderung untuk melaporkan potensi penyalahgunaan akses. Selain itu, pendidikan dan pelatihan berkelanjutan mengenai keamanan informasi dan etika bisnis harus menjadi bagian integral dari program pengembangan karyawan. Pelatihan ini harus mencakup cara mengenali tanda-tanda penyalahgunaan akses, pentingnya menjaga kerahasiaan informasi, dan prosedur pelaporan yang tepat. Melakukan audit dan penilaian risiko secara berkala adalah langkah penting dalam mengidentifikasi potensi kelemahan dalam sistem pengendalian internal. Audit ini harus mencakup evaluasi terhadap kebijakan keamanan, kontrol akses, dan kepatuhan terhadap prosedur yang telah ditetapkan. Dengan melakukan audit secara rutin, perusahaan dapat menemukan dan memperbaiki celah yang dapat dimanfaatkan oleh individu yang berniat jahat. Secara keseluruhan, mencegah

kecurangan pada penyalahgunaan akses internal perusahaan memerlukan pendekatan yang holistik dan terintegrasi. Dengan menerapkan langkah-langkah yang telah dibahas, perusahaan tidak hanya dapat melindungi asetnya, tetapi juga membangun kepercayaan di antara karyawan dan pemangku kepentingan, yang pada akhirnya berkontribusi pada keberhasilan jangka panjang perusahaan.

REFERENSI

Alifiananda, Nisrina, Nurul Safura, Putri Sekar Arum, Putri Vira Salsabila, Raffli Dika Pratama, and Arwan Gunawan. 2021. "Tinjauan Sistem Informasi Akuntansi Dan Deteksi-Pencegahan Kecurangan Akuntansi." Prosiding The 12thIndustrial Research Workshop and National Seminar 4–5.

Alou, Shelby Defiany, Ventje Ilat, and Hendrik Gamaliel. 2017. "Pengaruh Kesesuaian Kompensasi, Moralitas Manajemen, Dan Keefektifan Pengendalian Internal Terhadap Kecenderungan Kecurangan Akuntansi Pada Perusahaan Konstruksi Di Manado." Going Concern : Jurnal Riset Akuntansi 12(01):139–48. doi: 10.32400/gc.12.01.17146.2017.

Aprilia, Aprilia. 2017. "Analisis Pengaruh Fraud Pentagon Terhadap Kecurangan Laporan Keuangan Menggunakan Beneish Model Pada Perusahaan Yang Menerapkan Asean Corporate Governance Scorecard." Jurnal ASET (Akuntansi Riset) 9(1):101. doi: 10.17509/jaset.v9i1.5259.

Febrianti, Fitri, Ajang Mulyadi, and Yana Setiawan. 2021. "Analisis Pengendalian Interna Dan Kecenderungan Kecurangan (Fraud) Usaha Mikro Kecil Menengah Di Kota Tasikmalaya." Jurnal Ilmu Manajemen Dan Bisnis 12(1):73–78.

Fitriani, Dita. 2023. "PENGARUH SISTEM INFORMASI AKUNTANSI DALAM PENERAPAN SIKLUS PRODUKSI DAN PENGENDALIAN INTERNAL UNTUK MENINGKATKAN EFEKTIVITAS KINERJA UMKM." Jkpim : Jurnal Kajian Dan

Ii, B. A. B. 2015. "BAB II TINJAUAN PUSTAKA 2.1 Review Penelitian Sebelumnya." (2014).

Internal, Pengendalian, Terhadap Kecurangan Sukadwilinda, and R. Aryanti Ratnawati. 2013. "Jurnal Aset (Akuntansi Riset)." Jurnal Aset (Akuntansi Riset) 5(1):11–21.

Karlina Ghazalah Rahman, Siti Nur Reskiyawati Said, Adelia Nindya Putri. 2022. "Peran Audit Internal Dalam Pencegahan Kecurangan Pada Pemerintah Daerah." IMPREST: Jurnal Ilmiah Akuntans 1(2):73–79.

Marselina Rachma, Ade, Sarah Sapitri, and Fransisca Novelina. 2024. "ANALISA PERAN AUDIT INTERNAL DALAM MENGATASI KECURANGAN TERHADAP LAPORAN KEUANGAN." JIAP 4(2).

Novida, Diah Rachmawatie. 2025. "Evolusi Sistem Informasi Akuntansi Dalam Era Digital: Tinjauan Literatur Tentang Tren, Tantangan, Dan Peluang." Jurnal Minfo Polgan 14(1):77–85. doi: 10.33395/jmp.v14i1.14628.

Penalaran Ilmu Manajemen 1(1).

PERBANKAN DI INDONESIA." SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan 2(1):223–32. doi: 10.54443/sibatik.v2i1.535.Alifiananda, Nisrina, Nurul Safura, Putri Sekar Arum, Putri Vira Salsabila, Raffli Dika Pratama, and Arwan Gunawan. 2021. "Tinjauan Sistem Informasi Akuntansi Dan Deteksi-Pencegahan Kecurangan Akuntansi." Prosiding The 12thIndustrial Research Workshop and National Seminar 4–5.

Prasetyo, Andrian Budi. 2014. "Pengaruh Karakteristik Komite Audit Dan Perusahaan

Putri, Siluh Made Ayu Anisa, I. Gede Putu Krisna Juliharta, and I. Made Dwi Hita Darmawan. 2025. "Peran Pengendalian Internal Dalam Mengurangi Risiko Fraud Reservasi Kamar Pada Adi Rama Beach Hotel." Remik 9(1):382–88. doi: 10.33395/remik.v9i1.14513.

Rodiah, Siti, Ika Ardianni, and Aftania Herlina. 2019. "Pengaruh Pengendalian Internal , Ketaatan Aturan Akuntansi , Moralitas Manajemen Dan Budaya Organisasi Terhadap Kecurangan Akuntansi The Effect of Internal Control , Compliance with Accounting Rules , Management Morality and Organization Culture to Accoun." Jurnal Akuntansi & Ekonomika 9(1):1–11.
Rodiah, Siti, Ika Ardianni, and Aftania Herlina. 2019. "Pengaruh Pengendalian Internal , Ketaatan Aturan Akuntansi , Moralitas Manajemen Dan Budaya Organisasi Terhadap Kecurangan Akuntansi The Effect of Internal Control , Compliance with Accounting Rules , Management Morality and Organization Culture to Accoun." Jurnal Akuntansi & Ekonomika 9(1):1–11.
Senapan, Uli Hidayati, Taris Anggie Fahriza Senapan, Early Agista Mahardhika Senapan, and Rizdina Azmiyanti Senapan. 2022. "Literature Review: Peran Sistem Pengendalian Internal Dalam Pencegahan Kecurangan Akuntansi." Seminar Nasional Akuntansi Dan Call for Paper (SENAPAN) 2(1):86–95. doi: 10.33005/senapan.v2i1.174.

Supriyanto, Supriyanto, Michael Learns Tay, Saltycia Chairika, and Stella Maria Theresia Barahama. 2022. "MANAJEMEN RISIKO KECURANGAN PADA PERUSAHAAN
Terhadap Kecurangan Pelaporan Keuangan." Jurnal Akuntansi & Auditing 11(1):1–24.

Udayani, Anak Agung K. Finty, and Maria M. Ratna Sari. 2017. "Penelitian Ini Bertujuan Untuk Mengetahui Pengaruh Pengendalian Internal Dan Moralitas Individu Pada Kecenderungan Kecurangan Akuntansi. Teori Yang Digunakan Dalam Penelitian Ini Adalah." Akuntansi Universitas Udayana 18:1774–99.