BAB II
TINJAUAN PUSTAKA

2.1 *Accounting Information System* (AIS)

Accounting Information System (AIS) merupakan elemen penting dalam manajemen keuangan setiap perusahaan. AIS adalah suatu sistem yang berfungsi mengumpulkan, menyimpan, mengelola, memproses, mengambil, dan melaporkan data keuangan guna menyediakan informasi yang akurat dan tepat waktu untuk mendukung proses pengambilan keputusan (Fontinelle & Kindness, 2023). Menurut Romney dan Steinbart (2018), terdapat enam komponen penting dalam AIS. Komponen-komponen tersebut antara lain:

1. Orang, yaitu meliputi pengguna yang menggunakan sistem.
2. Prosedur dan instruksi, yang digunakan untuk mengumpulkan, memproses, dan menyimpan data.
3. Data, yaitu informasi yang dikumpulkan, dicatat, dan disimpan oleh sistem.
4. Perangkat lunak, yakni termasuk aplikasi yang digunakan untuk memproses data.
5. Infrastruktur teknologi informasi, meliputi perangkat keras dan jaringan yang mendukung sistem.
6. Pengendalian internal dan prosedur keamanan, untuk melindungi sistem informasi akuntansi.

Menurut Endaryati (2021), AIS adalah suatu struktur pengelolaan sumber daya yang dirancang untuk mentransformasi data ekonomi menjadi informasi keuangan yang berguna dalam operasional suatu entitas, serta memberikan informasi akuntansi kepada pihak-pihak yang memiliki kepentingan terkait. AIS melibatkan sejumlah langkah, mulai dari pengumpulan data hingga proses pencatatan akuntansi. Pendekatan terbaik untuk menerapkannya adalah dengan mengikuti pendekatan siklus, seperti siklus pendapatan, pengeluaran kas, produksi, sumber daya manusia/penggajian, dan pembiayaan. Siklus-siklus tersebut dapat

diuraikan dan dipahami dengan mudah melalui penggunaan bagan alur, yang umumnya dikenal sebagai *flowchart*.

Flowchart atau diagram arus adalah representasi visual yang menunjukkan simbol-simbol standar yang digunakan oleh analis sistem untuk mengilustrasikan suatu sistem tertentu (Setiawan, 2021). Menurut Indrajani (2011), *flowchart* merupakan representasi grafis dari langkah-langkah dan urutan prosedur suatu program. Pembuatan *flowchart* ini diharapkan dapat mempermudah pemahaman para pihak yang berkepentingan terhadap keseluruhan sistem perusahaan. *Flowchart* digunakan untuk menampilkan kegiatan manual, kegiatan pemrosesan, atau keduanya, dan membantu dalam membangun sistem perusahaan. Beberapa jenis *flowchart* mencakup:

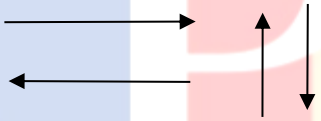
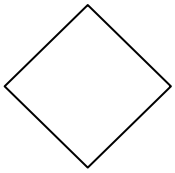
1. *System Flowchart*: Menyajikan alur kerja secara keseluruhan dari sistem, menjelaskan urutan prosedur yang ada di dalamnya.
2. *Document Flowchart*: Menggambarkan instruksi program komputer secara rinci, digunakan oleh pemrogram untuk mengilustrasikan alur prosedur.
3. *Schematic Flowchart*: Representasi grafis yang menggambarkan suatu skema atau prosedur dalam suatu sistem. Diagram alir ini mirip dengan diagram alir sistem. Namun, diagram alir skematis ini menampilkan detail lebih lanjut serta prosedur yang diilustrasikan melalui gambar-gambar komputer dan peralatan lain yang digunakan.
4. *Program Flowchart*: Representasi visual terperinci yang menggambarkan langkah-langkah atau urutan dari suatu proses pemrograman. *Program flowchart* adalah representasi visual yang secara terperinci menggambarkan langkah-langkah atau urutan dari suatu proses pemrograman. *Program flowchart* ini sering digunakan sebagai panduan dalam menyusun daftar program menggunakan bahasa komputer. Terdapat dua jenis *Program flowchart*, yaitu *Program Logic Flowchart* dan juga *Detailed Computer Program Flowchart*. *Program Logic Flowchart* bertujuan untuk mengilustrasikan setiap tahap dalam program komputer secara logis, yang dibuat oleh seorang analis sistem. Sementara itu, *Detailed Computer Program Flowchart* digunakan untuk menggambarkan instruksi dari suatu

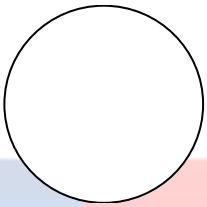
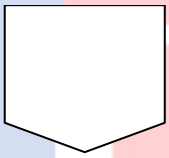
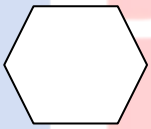
program komputer secara terperinci yang disusun oleh seorang *programmer*.

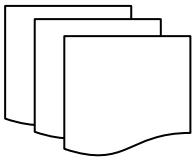
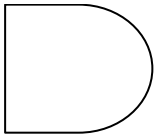
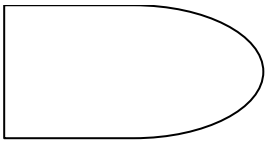
5. *Process Flowchart*: Sering digunakan dalam industri teknik dan analisis sistem untuk menggambarkan proses dalam suatu prosedur.

Flowchart dapat membantu mengidentifikasi masalah khusus yang perlu dipelajari dan dievaluasi lebih lanjut. Selain itu, *flowchart* juga dapat digunakan untuk menggambarkan langkah-langkah dalam pengembangan perangkat lunak dan sistem informasi. *Flowchart* memiliki beberapa simbol sebagai berikut:

Tabel 2.1 Simbol-Simbol Utama *Flowchart* Beserta Fungsinya

No.	Nama	Simbol	Fungsi
1	*Terminal Point Symbol* (Simbol Titik Terminal)		Menunjukkan permulaan (*start*) atau akhir (*stop*) dari suatu proses.
2	Flow Direction Symbol (Simbol Arus)		Menghubungkan antara simbol yang satu dengan simbol yang lain (*connecting line*). Simbol ini juga berfungsi untuk menunjukkan garis alir dari proses.
3	*Processing Symbol* (Simbol Proses)		Menunjukkan kegiatan yang dilakukan oleh komputer. Pada bidang industri (proses produksi barang), simbol ini menggambarkan kegiatan inspeksi atau yang biasa dikenal dengan simbol inspeksi
4	*Decision Symbol* (Simbol Keputusan)		Memilih proses atau keputusan berdasarkan kondisi yang ada. Simbol ini biasanya ditemui pada flowchart program.

5	*Input-Output* (Simbol Keluar-Masuk)		Menunjukkan proses input-output yang terjadi tanpa bergantung dari jenis peralatannya.
6	*Predefined Process* (Simbol Proses Terdefinisi)		Menunjukkan pelaksanaan suatu bagian prosedur (*sub-proses*). Dengan kata lain, prosedur yang terinformasi di sini belum detail dan akan dirinci di tempat lain.
7	*Connector (On-page)*		Menyederhanakan hubungan antar simbol yang letaknya berjauhan atau rumit bila dihubungkan dengan garis dalam satu halaman.
8	*Connector (Off-page)*		Menghubungkan simbol dalam halaman berbeda. label dari simbol ini dapat menggunakan huruf atau angka.
9	*Preparation Symbol* (Simbol Persiapan)		Mempersiapkan penyimpanan di dalam storage.
10	*Manual Input Symbol*		Menunjukkan input data secara manual menggunakan online keyboard.
11	*Manual Operation Symbol* (Simbol Kegiatan Manual)		Menunjukkan kegiatan/proses yang tidak dilakukan oleh komputer.
12	*Document Symbol*		Artinya input berasal dari dokumen dalam bentuk kertas, atau output yang perlu dicetak di atas kertas.

13	*Multiple Documents*		Sama seperti *document symbol* hanya saja dokumen yg digunakan lebih dari satu dalam simbol ini.
14	*Display Symbol*		Menyatakan penggunaan peralatan output, seperti layar monitor, printer, plotter dan lain sebagainya.
15	*Delay Symbol*		Menunjukkan proses delay (menunggu) yang perlu dilakukan. Seperti menunggu surat untuk diarsipkan, dan lain-lain.

Sumber: Ridho, 2024

Prosedur Operasi Standar (SOP) adalah dokumen yang merinci langkah-langkah yang harus diikuti oleh pekerja dalam melaksanakan tugas tertentu dan bersifat wajib untuk memastikan konsistensi dalam pelaksanaan suatu proses. Selain SOP, dokumen pendukung seperti flowchart dan spesifikasi material juga dapat digunakan. Jika ada penyimpangan yang diperbolehkan dari instruksi dalam SOP, maka ketentuan tersebut harus dijelaskan secara tertulis, termasuk pihak yang berwenang memberikan izin serta langkah-langkah yang harus dilakukan (Kathrin et al., 2020).

SOP memegang peranan penting dalam manajemen perusahaan, dirancang untuk menjamin konsistensi, efisiensi, dan kepatuhan dalam pelaksanaan operasional sehari-hari. Sebagai elemen strategis, SOP berfungsi untuk mengatur dan mengendalikan berbagai aspek kegiatan operasional, termasuk prosedur yang berkaitan dengan pengelolaan informasi keuangan melalui penerapan Sistem Informasi Akuntansi (AIS). Dalam konteks AIS, SOP menjadi sangat penting karena AIS bertanggung jawab atas pengumpulan, pengolahan, dan pelaporan informasi keuangan perusahaan. Integrasi antara SOP dan AIS menjadi langkah esensial untuk memastikan proses akuntansi berjalan sesuai standar yang telah ditetapkan, sehingga menghasilkan informasi keuangan yang akurat, andal, dan relevan.

Salah satu aspek penting dalam SOP perusahaan adalah pengelolaan data keuangan, yang mencakup langkah-langkah terperinci mengenai proses pengumpulan, pencatatan, dan pengolahan data keuangan melalui AIS. SOP dapat mengatur prosedur yang harus diikuti oleh karyawan dalam memasukkan transaksi keuangan, menetapkan batasan akses terhadap data sensitif, serta memastikan pencatatan dilakukan secara akurat dan tepat waktu. Selain itu, SOP juga berperan dalam pengelolaan keamanan informasi, dengan mencakup kebijakan pengelolaan kata sandi, pembatasan akses, dan penerapan langkah-langkah keamanan teknis untuk melindungi data keuangan dari ancaman keamanan *cyber*. Lebih jauh lagi, SOP perlu mencakup panduan bagi pihak terkait dalam penggunaan AIS, seperti pelatihan karyawan, penyediaan dokumentasi yang jelas, serta mekanisme pelaporan jika terjadi masalah atau gangguan sistem. Dengan SOP yang terstruktur dan terintegrasi, perusahaan dapat menciptakan pemahaman yang seragam di antara semua pihak terkait, sehingga mendukung optimalisasi proses akuntansi dan pengelolaan informasi keuangan secara keseluruhan.

2.2 *Internal Control*

2.2.1 Pengertian dan Tujuan *Internal Control*

Internal control merupakan suatu sistem yang dirancang untuk membantu perusahaan mencapai tujuan-tujuannya dengan efektif dan efisien, serta membantu dalam memastikan keandalan laporan keuangan. Menurut Committee of Sponsoring Organization of Treadway Commision (COSO) (2013), *internal control* merupakan suatu proses yang dilakukan oleh dewan entitas direksi, manajemen dan personil lainnya, dirancang untuk memberikan keyakinan memadai tentang pencapaian tujuan yang berkaitan dengan operasi, pelaporan dan kepatuhan. *Internal control* adalah suatu cara untuk mengarahkan, mengawasi dan mengukur sumber daya suatu organisasi.

Internal control berperan penting untuk mencegah dan mendeteksi penggelapan (*fraud*) dan melindungi sumber daya organisasi baik yang berwujud maupun tidak, seperti reputasi atau hak kekayaan intelektual (Kumaat & Saat, 2010). *Internal control* merujuk pada proses, kebijakan, dan langkah-langkah yang diterapkan oleh sebuah organisasi untuk memastikan pencapaian tujuan, menjaga

aset, dan mengurangi risiko penipuan serta kesalahan (Kenton et al., 2023). Peranan internal control sangat penting bagi perusahaan, dan berikut adalah beberapa manfaat penerapannya, menurut COSO (2013):

1. Mencegah kecurangan dan penyelewengan. *Internal control* membantu mencegah terjadinya kecurangan dan penyelewengan di dalam perusahaan. Dengan adanya kontrol yang ketat, perusahaan dapat mengurangi risiko terjadinya tindakan yang tidak etis atau ilegal.

2. Peningkatan keandalan informasi keuangan. *Internal control* membantu memastikan keandalan informasi keuangan. Dengan adanya kontrol yang baik, perusahaan dapat mengidentifikasi dan mengatasi kesalahan-kesalahan yang mungkin terjadi dalam proses pelaporan keuangan, sehingga laporan keuangan yang dihasilkan lebih akurat dan dapat dipercaya.

3. Optimasi penggunaan sumber daya. *Internal control* membantu perusahaan mengoptimalkan penggunaan sumber daya dengan memastikan bahwa aset perusahaan digunakan secara efisien dan efektif. Hal ini mencakup pengendalian terhadap pemakaian dana, manajemen inventaris, dan pengelolaan aset lainnya.

4. Peningkatan efisiensi operasional. Dengan adanya *internal control*, perusahaan dapat meningkatkan efisiensi operasionalnya. Pengendalian yang baik membantu mengidentifikasi proses-proses yang tidak efisien dan memberikan rekomendasi untuk perbaikan.

5. Kepatuhan terhadap regulasi dan kebijakan perusahaan. *Internal control* membantu memastikan bahwa perusahaan mematuhi peraturan dan kebijakan yang berlaku. Hal ini dapat melibatkan implementasi kontrol untuk memastikan kepatuhan terhadap hukum dan peraturan pemerintah serta kebijakan internal perusahaan.

Keefektifan *internal control* terletak pada kemampuannya untuk memberikan keyakinan yang wajar bahwa tujuan organisasi tercapai. *Internal*

control yang efektif membantu mengurangi risiko penipuan dan kesalahan saji material dengan menetapkan sistem pemeriksaan dan keseimbangan, memisahkan tugas-tugas, menerapkan proses otorisasi dan persetujuan yang tepat, serta memastikan pelaporan keuangan yang akurat serta dapat dipercaya. Menurut Petrozzello (2023), salah satu peran penting dari *internal control* adalah untuk mengurangi kecurangan dan kesalahan dalam proses bisnis. Hal ini dilakukan melalui langkah-langkah berikut:

1. Mencegah kecurangan. *Internal control* akan memastikan adanya mekanisme yang mencegah dan menghalangi aktivitas kecurangan. Salah satunya adalah dengan menerapkan pemisahan tugas, di mana berbagai karyawan bertanggung jawab atas langkah-langkah transaksi yang berbeda untuk memastikan tanggung jawab dan mengurangi peluang terjadinya kecurangan.

2. Mendeteksi kecurangan, *internal control* juga melibatkan kegiatan pemantauan dan penerapan audit internal dan eksternal untuk mendeteksi potensi kecurangan. Melakukan pemantauan secara rutin membantu dalam mengidentifikasi transaksi yang mencurigakan atau pola yang tidak biasa, sehingga memungkinkan dilakukannya penyelidikan tepat waktu dan tindakan perbaikan yang diperlukan.

3. Menjaga aset, *internal control* dirancang untuk melindungi aset organisasi dari pencurian, kehilangan, atau penyelewengan. Hal ini mencakup pengamanan fisik, seperti penyimpanan yang aman dan pengendalian akses, serta pengendalian keuangan, seperti rekonsiliasi rekening secara berkala dan proses persetujuan pengeluaran.

4. Memastikan akurasi dan keandalan, *internal control* memainkan peran penting dalam memastikan keakuratan dan keandalan informasi keuangan. Hal ini mencakup penerapan praktik akuntansi yang tepat, pemeliharaan catatan yang lengkap dan akurat, serta pelaksanaan rekonsiliasi dan peninjauan berkala untuk mendeteksi dan memperbaiki kesalahan apa pun.

Dapat disimpulkan bahwa *internal control* adalah serangkaian langkah, kebijakan, dan prosedur yang diterapkan oleh suatu organisasi untuk mencapai tujuan dan menjaga asetnya. Keberhasilannya tergantung pada kemampuannya dalam mencegah dan mendeteksi penipuan serta kesalahan, dengan demikian mengurangi risiko kerugian finansial. Dengan menerapkan mekanisme pemeriksaan dan keseimbangan, memisahkan tugas-tugas, serta menjamin laporan keuangan yang akurat, *internal control* memiliki peran penting dalam mempertahankan integritas proses bisnis.

2.2.2 Elemen *Internal Control*

Menurut COSO (2013), terdapat lima elemen yang terdapat dalam *internal control*, diantaranya adalah:

1. *Control Environment*. *Control environment* merupakan kumpulan standar, proses, dan struktur yang menjadi dasar pelaksanaan pengendalian internal di seluruh organisasi. Dewan direksi dan manajemen senior menetapkan landasan mengenai urgensi *internal control* dan standar perilaku yang diharapkan.

2. *Risk Assessment*. *Risk assessment* melibatkan serangkaian proses dinamis dan berulang guna mengidentifikasi serta menganalisis risiko dengan tujuan mencapai tujuan entitas. Ini membentuk dasar bagi manajemen untuk menentukan strategi pengelolaan risiko, dengan mempertimbangkan potensi perubahan dalam lingkungan eksternal dan model bisnis yang dapat menghambat pencapaian tujuan tersebut.

3. *Control Activities*. *Control activities* merupakan langkah-langkah yang telah ditentukan oleh kebijakan dan prosedur guna membantu memastikan bahwa instruksi dari manajemen untuk mengurangi risiko terhadap pencapaian tujuan telah diimplementasikan. *Control activities* dilakukan di semua tingkatan entitas, pada berbagai tahapan dalam proses bisnis, dan dalam konteks lingkungan teknologi. Hal ini dapat bersifat pencegahan maupun pendeteksian yang melibatkan serangkaian aktivitas baik manual maupun otomatis, seperti otorisasi dan persetujuan, verifikasi, rekonsiliasi,

dan evaluasi kinerja bisnis. Pemisahan tugas biasanya diintegrasikan dalam pemilihan dan pengembangan kegiatan pengendalian. Jika pemisahan tugas tidak memungkinkan, manajemen akan memilih dan mengembangkan kegiatan pengendalian alternatif.

4. *Information and Communication*. Informasi menjadi suatu keharusan bagi entitas guna menjalankan tanggung jawab *internal control* dengan maksud mendukung pencapaian tujuan. Komunikasi terjalin dengan baik, baik itu di internal maupun eksternal, dan memberikan organisasi akses terhadap informasi yang diperlukan untuk melaksanakan kegiatan pengendalian internal sehari-hari. Komunikasi menjadi sarana yang memungkinkan personel memahami tanggung jawab pengendalian internal serta keberartiannya dalam mencapai tujuan.

5. *Monitoring & Evaluation*. Evaluasi berkelanjutan, evaluasi terpisah, atau kombinasi keduanya digunakan untuk memastikan apakah masing-masing dari lima komponen pengendalian internal, termasuk pengendalian untuk mempengaruhi prinsip-prinsip dalam setiap komponen, ada dan berfungsi. Temuan-temuan dievaluasi dan kekurangan-kekurangan dikomunikasikan secara tepat waktu, dan masalah-masalah serius dilaporkan kepada manajemen senior dan dewan direksi.

Internal control khususnya *control activities*, memegang peran sentral dalam melindungi aset suatu organisasi, memastikan ketepatan informasi keuangan, dan meningkatkan efisiensi operasional. Kegiatan pengendalian merujuk pada kebijakan dan prosedur spesifik yang diterapkan oleh manajemen untuk mencapai tujuan organisasi dan mengurangi risiko. Salah satu alasan utama mengapa kegiatan pengendalian sangat penting adalah perannya dalam mencegah dan mendeteksi kesalahan dan penipuan.

Dengan menerapkan kegiatan pengendalian yang kokoh, organisasi dapat mengurangi kemungkinan transaksi tanpa izin, penyajian laporan keuangan yang salah, dan ketidakberesan lainnya. Selain itu, kegiatan pengendalian turut berkontribusi pada keandalan pelaporan keuangan, karena membantu memastikan

informasi keuangan akurat, lengkap, dan sesuai dengan peraturan dan standar yang berlaku. Kegiatan pengendalian yang efektif juga meningkatkan efisiensi operasional dengan menyederhanakan proses dan mendorong tanggung jawab di kalangan karyawan. Pada intinya, sistem kegiatan pengendalian yang dirancang dengan baik dan diimplementasikan dengan benar sangat penting untuk menjaga integritas operasional, pelaporan keuangan, dan tata kelola organisasi. Sistem ini memberikan keyakinan kepada para pemangku kepentingan, termasuk manajemen, investor, dan otoritas regulasi, terhadap keandalan informasi keuangan organisasi dan efektivitas pengendalian internalnya.

Bagian *monitoring & evaluation* menjadi fondasi yang penting dalam memastikan efektivitasnya. *Monitoring & evaluation* berperan sebagai mekanisme pengawasan yang berkesinambungan, memungkinkan organisasi untuk mengidentifikasi dan mengevaluasi efisiensi serta keberlanjutan sistem *internal control* yang telah diterapkan. Dengan adanya monitoring evaluation, organisasi dapat secara proaktif mendeteksi potensi risiko, memonitor pelaksanaan kebijakan, dan mengukur kinerja operasional secara terus-menerus. Hal ini tidak hanya membantu mencegah kemungkinan pelanggaran atau penyalahgunaan, tetapi juga mendukung perbaikan berkelanjutan terhadap proses bisnis. Lebih lanjut, *monitoring evaluation* menjadi alat yang efektif untuk meningkatkan akuntabilitas dan transparansi organisasi, memastikan bahwa tujuan organisasi tercapai dengan tepat dan sesuai dengan norma-norma yang berlaku. Dengan demikian, *internal control* pada elemen *monitoring evaluation* bukan hanya sekadar kepatuhan terhadap peraturan, tetapi juga kunci untuk meningkatkan kinerja organisasi secara keseluruhan.

Dua aspek yang dijabarkan di atas merupakan aspek *internal control* yang menjadi fokus pada penelitian ini dikarenakan AIS, berdasarkan tinjauan literatur terkaitnya (penjelasan lebih lanjut akan dipaparkan pada bagian selanjutnya), merupakan sistem yang memberikan mekanisme otomatisasi dan otorisasi terhadap fungsi pengawasan aktivitas transaksi dan evaluasi perusahaan.

Tabel 2.2 COSO Elemen *Control Activity* dan *Monitoring & Evaluation*

COSO *Element*	*Point of Focus*	*Keywords*
Control activity	A. *Integrates with risk assessment*: Melakukan peninjauan ulang terhadap penilaian risiko bisnis yang ditujukan untuk penyusunan rancang bangun pengendalian transaksi pada setiap siklus akuntansi. B. *Considers entity-specific factors*: Mengembangkan dan menerapkan aktivitas pengawasan yang merespons risiko-risiko teridentifikasi pada setiap fungsi usaha (misal: penjualan, pembelian, penerimaan kas, dan sebagainya) beserta dengan alur bisnisnya yang spesifik. C. *Determines relevant business processes*: Suatu organisasi mempertimbangkan struktur, kebijakan, prosedur, dan kewenangan serta tanggung jawab yang diberikan atas keberlangsungan usahanya untuk menanggapi risiko yang teridentifikasi. D. *Evaluates a mix of control activity types*: Organisasi secara	

	hati-hati mempertimbangkan jenis tindakan individu atau kombinasi tindakan tertentu yang secara efektif mampu merespons risiko tersebut. E. *Considers at what level activities are applied*: Penempatan kontrol yang tepat dan efektif pada aktivitas bisnis tertentu berdasarkan penugasan personel. F. *Addresses segregation of duties*: Merancang desain pengendalian yang menempatkan dua orang otorisator sebagai pengawas satu fungsi transaksi yang memungkinkan dua orang tersebut untuk saling mengawasi satu sama lain.	
Monitoring	A. *Selection* (Pemilihan): Merujuk pada proses penentuan kriteria dan parameter untuk memilih program, kebijakan, atau proyek yang akan dievaluasi. B. *Development* (Pengembangan): Mencakup langkah-langkah untuk merancang dan mengembangkan instrumen, metode, dan kerangka kerja evaluasi yang melibatkan perencanaan sistem evaluasi.	Parameter Merancang dan mengembangkan

	C. *Performance* (Kinerja): Merujuk pada hasil dan pencapaian program yang sedang dievaluasi beserta dengan parameter penilaiannya. Evaluasi kinerja tahap ini bertujuan untuk menilai sejauh mana tujuan dan sasaran telah tercapai, serta untuk mengidentifikasi faktor-faktor yang mempengaruhi hasilnya.	Hasil dan pencapaian
	D. *Evaluation* (Evaluasi): Merupakan proses penilaian sistematis terhadap suatu program atau kebijakan. Evaluasi dapat dilakukan secara ongoing (berkelanjutan) atau sebagai evaluasi terpisah. Evaluasi mencakup pemantauan terus-menerus terhadap implementasi dan dampak program sepanjang waktu.	Penilaian sistematis
	E. *Assurance* (Jaminan): Merujuk pada langkah-langkah yang diambil untuk memastikan bahwa data yang dikumpulkan dan hasil evaluasi dapat diandalkan, akurat, dapat diterima, dan digunakan oleh semua pihak berkepentingan.	Memastikan, Digunakan oleh semua pihak berkepentingan
	F. *Presence* (Keberadaan):	Relevan

	Mencakup sejauh mana program dan kebijakan yang telah dinilai masih relevan dalam konteks usaha yang dijalankan. Ini juga melibatkan pemantauan untuk memastikan bahwa program tersebut masih berjalan dan dapat memberikan manfaat yang diharapkan. G. *Function* (Fungsi): Evaluasi suatu bagian fungsi organisasi mampu mengidentifikasi perubahan yang diperlukan untuk meningkatkan kinerja atau untuk menyesuaikan program dengan kebutuhan yang berkembang.	Mengidentifikasi perubahan
Evaluation	A. *Evaluate* (Evaluasi): Melibatkan penilaian atau pemeriksaan menyeluruh terhadap sistem atau proses internal untuk mengidentifikasi kelemahan atau kekurangan yang mungkin ada dalam kontrol internal. Hal ini bertujuan untuk menilai efektivitas dan efisiensi kontrol internal yang telah diimplementasikan dan mengidentifikasi kekurangan yang mungkin mempengaruhi keberlanjutan operasi	Penilaian atau pemeriksaan menyeluruh terhadap sistem

	perusahaan. B. *Communicate* (Komunikasi): Merupakan prosedur penyampaian informasi mengenai temuan evaluasi kepada pihak-pihak yang berkepentingan, seperti manajemen senior, dewan direksi, atau pihak terkait lainnya. Hal ini bertujuan untuk memastikan bahwa informasi tentang kelemahan dalam kontrol internal dapat tersampaikan dengan jelas dan tepat waktu kepada pihak yang dapat mengambil tindakan korektif. C. *Corrective Action* (Tindakan Korektif): Merupakan tindakan yang diambil untuk memperbaiki atau mengatasi kelemahan atau kekurangan yang teridentifikasi selama evaluasi kontrol internal. Yang bertujuan untuk memastikan bahwa masalah yang diidentifikasi tidak hanya diketahui, tetapi juga ditanggapi secara aktif dengan menerapkan perbaikan atau perubahan yang diperlukan dalam sistem atau	

	proses internal.	

Sumber: COSO, 2013

2.3 *Internal Control Deficiency* (ICD)

Menurut Putri (2021), *Internal Control Deficiency* (ICD) adalah keadaan di mana sistem pengendalian internal suatu perusahaan tidak berfungsi dengan baik atau tidak memadai. ICD merupakan masalah signifikan yang mempengaruhi organisasi di berbagai industri, karena mengacu pada kelemahan dalam struktur pengendalian internal perusahaan yang dapat menyebabkan kesalahan, penipuan, atau ketidakpatuhan terhadap peraturan. Kesenjangan dalam sistem *internal control* dapat mempengaruhi pencapaian tujuan perusahaan, seperti keandalan laporan keuangan, efektivitas dan efisiensi operasional, dan ketaatan terhadap peraturan yang berlaku. Maka dari itu perusahaan perlu mengeksplorasi konsep ICD secara rinci, mengkaji penyebab, dan konsekuensinya. Dengan memahami kompleksitas ICD, organisasi dapat berupaya menerapkan sistem *internal control* yang kuat untuk memitigasi risiko dan meningkatkan operasi mereka secara keseluruhan.

Dikutip dari Pathlock Team (2023), terdapat beberapa kategori kelemahan dalam *internal control*. Pertama, kelemahan teknis dalam *internal control*. Kelemahan dalam pengendalian teknis melibatkan kontrol keamanan teknis, seperti perangkat keras dan perangkat lunak. Perubahan teknologi, pemeliharaan, atau kegagalan konfigurasi dapat menjadi pemicu kelemahan dalam pengendalian teknis. Sebagai contoh, jika sistem informasi perusahaan mengalami pelanggaran keamanan pada perangkat keras atau perangkat lunak, hal ini dapat dianggap sebagai kelemahan teknis. Contoh konkret adalah kerentanan *EternalBlue* yang ditemukan pada protokol *Windows SMB* pada tahun 2017, yang menyebabkan serangan terhadap sistem *Windows*. Kedua, kelemahan operasional dalam *internal control.* Kelemahan dalam pengendalian operasional terkait dengan keamanan operasional (*OpSec*), yang menekankan pemantauan operasional dan penerapan manajemen risiko dalam kegiatan bisnis sehari-hari.

Faktor manusia dapat menjadi penyebab utama kelemahan pengendalian operasional. Efektivitas pengendalian operasional dapat terpengaruh jika karyawan

yang bertanggung jawab tidak mematuhi standar dan kebijakan yang telah ditetapkan. Respons cepat terhadap insiden adalah contoh konkret pengendalian operasional yang sangat tergantung pada waktu, di mana intervensi yang lambat dapat mengurangi efektivitas respons terhadap insiden keamanan. Ketiga, kelemahan administratif dalam *internal control*. Kelemahan dalam pengendalian keamanan administratif, juga dikenal sebagai pengendalian prosedural, disebabkan oleh ketidakpatuhan yang konsisten terhadap standar dan peraturan yang telah ditetapkan. Sebagai contoh, kontrol administratif seperti pencadangan rutin sistem penting mungkin menjadi tidak efektif jika tidak ada pelaksanaan yang konsisten.

Pencadangan data akan bermanfaat jika dilakukan secara rutin, dan verifikasi kemampuan harus dilakukan secara teratur. Keempat, kelemahan dalam pengendalian arsitektur internal. Pengendalian arsitektur mengacu pada fokus menciptakan sistem terpadu untuk mengelola dan mengurangi risiko lingkungan teknologi informasi. Kelemahan dalam pengendalian arsitektur seringkali terkait dengan perubahan konfigurasi perangkat keras atau perangkat lunak. Kurangnya pemantauan atau persetujuan yang tidak tepat terhadap perubahan tersebut dapat merusak integritas arsitektur keamanan. Setiap perubahan yang mempengaruhi elemen arsitektur keamanan organisasi memiliki potensi menjadi kelemahan dalam pengendalian arsitektur.

Pathlock Team (2023), juga menyatakan bahwa terdapat banyak faktor yang dapat memicu timbulnya ICD dalam perusahaan, diantaranya:

1. Pemisahan tugas yang kurang memadai: Terjadi ketika tanggung jawab tidak dipisahkan dengan jelas, yang dapat menimbulkan konflik kepentingan dan kesalahan dalam pelaporan keuangan.

2. Kegagalan dalam mengevaluasi risiko secara berkelanjutan: Organisasi mungkin tidak secara rutin menilai dan memperbarui sistem pengendalian internal, sehingga membuatnya rentan terhadap risiko dan ancaman baru.

3. Kurangnya pengawasan dari manajemen: Pengawasan yang tidak memadai dari pihak manajemen dapat menyebabkan melemahnya lingkungan pengendalian internal.

4. Ketergantungan yang berlebihan pada aplikasi akuntansi atau alat pihak ketiga lainnya: Ketergantungan yang berlebihan pada sistem eksternal dapat mengakibatkan struktur pengendalian internal menjadi lemah.

ICD dapat menyebabkan banyak konsekuensi yang serius, seperti:

1. Kesalahan dalam presentasi materi dalam laporan keuangan. Kekurangan dalam sistem *internal control* dapat menyebabkan kesalahan atau kecurangan dalam penyajian informasi keuangan, yang pada dapat membuat laporan keuangan perusahaan menjadi tidak dapat diandalkan (Frankenfield et al., 2023).

2. Kehilangan kepercayaan investor dan pihak-pihak yang berkepentingan. Kelemahan dalam pengendalian internal dapat mengikis kepercayaan investor dan pihak-pihak yang berkepentingan, sehingga organisasi mengalami kesulitan dalam upaya peningkatan modal atau penarikan mitra (Wadhwa, 2023).

3. Kerusakan reputasi: Organisasi dengan pengendalian internal yang lemah mungkin menghadapi publisitas negatif dan merusak reputasi saat kekurangan tersebut ditemukan dan diumumkan (Wadhwa, 2023).

4. Ketidakpatuhan terhadap peraturan: Pengendalian internal yang kurang memadai dapat mengakibatkan pelanggaran terhadap peraturan industri, yang selanjutnya dapat berujung pada denda, penalti, dan konsekuensi hukum (Pathlock Team, 2023).

Dengan memahami kategori, penyebab, dan dampak yang mungkin terjadi akibat adanya ICD perusahaan perlu menerapkan suatu sistem *internal control* yang kuat guna mengurangi risiko dan meningkatkan efisiensi operasional secara menyeluruh.

2.4 *Fraud Schemes*

Menurut Kranacher (2020), *Fraud schemes* dapat terjadi dalam beberapa tahap, dan seringkali melibatkan beberapa pihak yang bekerja sama untuk mencapai

tujuan penipuan mereka. Terdapat beberapa faktor yang dapat memicu terjadinya fraud, seperti tekanan (*pressure*), kesempatan (*opportunity*), dan rasionalisasi (*rationalization*). Tekanan mungkin berasal dari masalah keuangan pribadi, sementara peluang dapat muncul akibat kelemahan dalam sistem *internal control* perusahaan. Rasionalisasi, di sisi lain, muncul ketika pelaku merasa memiliki alasan moral atau etis untuk melakukan tindakan kecurangan tersebut.

Salah satu komponen dalam *fraud schemes* yang seringkali terjadi dalam perusahaan adalah *asset misappropriation*. *Asset misappropriation* mengacu pada penggelapan atau penyalahgunaan aset perusahaan oleh individu di dalam organisasi. Ini bisa mencakup pencurian fisik, manipulasi laporan keuangan, atau pengalihan dana perusahaan untuk keuntungan pribadi. Dalam *fraud tree*, bagian yang berkaitan dengan *asset misappropriation* dapat dibagi lebih rinci untuk mengidentifikasi cara-cara spesifik di mana penyalahgunaan aset dapat terjadi. Sebagai contoh, salah satu cabang dalam *fraud tree* terkait dengan *asset misappropriation* adalah pencurian fisik barang atau inventaris. Ini bisa melibatkan karyawan yang memiliki akses ke gudang atau ruang penyimpanan dan menggunakan kesempatan tersebut untuk mencuri barang secara fisik. Faktor-faktor yang memungkinkan terjadinya pencurian fisik dapat melibatkan kelemahan dalam sistem pengawasan atau kebijakan yang tidak memadai terkait dengan akses dan pemantauan gudang.

Selain *asset misappropriation*, bagian lain dari *fraud tree* yang relevan dengan fraud schemes dalam perusahaan adalah "*theft of cash on hand*." Pencurian uang tunai yang ada di perusahaan dapat terjadi melalui berbagai cara, seperti pencurian fisik dari kasir atau manipulasi transaksi keuangan. Seorang karyawan yang memiliki akses ke uang tunai perusahaan dapat mencoba untuk memanfaatkan situasi tersebut untuk keuntungan pribadi. Dalam *fraud tree*, cabang terkait dengan *theft of cash on hand* dapat mencakup subkategori seperti pencurian uang tunai dari kas register, manipulasi catatan transaksi, atau pemanfaatan celah dalam sistem akuntansi. Identifikasi potensi kelemahan dalam sistem *internal control* perusahaan, seperti kurangnya rekonsiliasi yang ketat, dapat membantu mencegah terjadinya pencurian uang tunai.

Pentingnya pencegahan *fraud* dalam perusahaan tidak dapat diabaikan. Perusahaan harus mengimplementasikan kebijakan-kebijakan yang kuat, membangun sistem *internal control* yang efektif, dan memberikan pelatihan kepada karyawan mengenai etika bisnis dan konsekuensi hukum dari melakukan *fraud*. Selain itu, perusahaan juga perlu secara rutin melakukan audit internal untuk mengidentifikasi potensi risiko dan memastikan bahwa sistem pengendalian internal berfungsi sebagaimana mestinya. Dalam menghadapi fenomena *fraud schemes,* pendekatan holistik yang mencakup pendidikan, pencegahan, dan deteksi diperlukan.

Pemberdayaan karyawan dengan pengetahuan tentang etika bisnis dan risiko *fraud* dapat membantu menciptakan budaya organisasi yang tidak mentolerir tindakan curang. Selain itu, penggunaan teknologi canggih seperti AIS, analisis data dan pemantauan transaksi dapat membantu mendeteksi pola-pola yang mencurigakan dan mengurangi risiko terjadinya *fraud* dalam perusahaan. Dengan upaya bersama dan kesadaran yang tinggi terhadap potensi risiko, perusahaan dapat meminimalkan kerugian akibat fraud dan menjaga integritas operasional dan finansial mereka.

2.5 Penelitian Terdahulu

Tabel 2.3 Penelitian Terdahulu

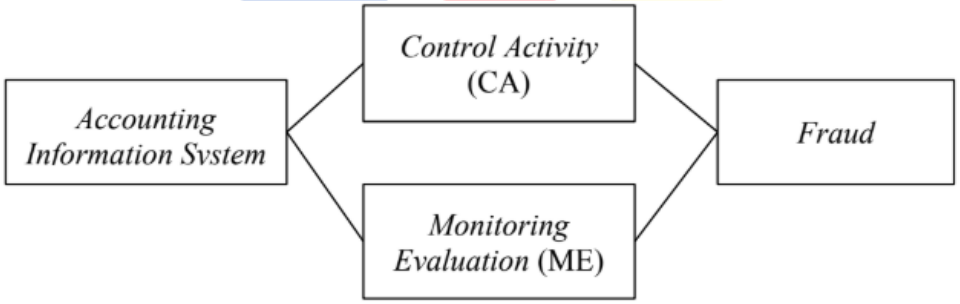
No.	Nama Peneliti (Tahun Penelitian)	Judul Penelitian	Metode Penelitian	Hasil Penelitian
1	Manik Arsa (2022)	Analisis Sistem Pengendalian Intern Pengeluaran Kas pada CV. Manik Arsa	Analisis deskriptif kualitatif	Ditemukan kelemahan dalam sistem pengendalian internal pengeluaran kas, seperti tidak adanya bukti dokumen dengan kode angka, kurangnya surat permintaan kas kecil, dan pembagian tugas yang belum terorganisir dengan baik. Hal ini menyebabkan rekam jejak akuntansi kurang akurat.
2	Tiarno & Budiwitjaksono (2023)	Analisis Sistem Pengendalian Internal Kas dan Setara Kas untuk Mencegah Fraud di Rumah Sakit XYZ dengan Menerapkan Kerangka Kerja COSO	Metode kualitatif dan menerapkan pendekatan deskriptif, yakni studi kasus dengan pendekatan kerangka kerja COSO	Sistem pengendalian internal yang lemah dapat meningkatkan risiko kesalahan dan kecurangan dalam aktivitas penerimaan dan pengeluaran kas. Penerapan kerangka kerja COSO membantu meningkatkan efektivitas pengendalian internal.
3	Luo (2017)	Evaluasi Penerapan Pengendalian Internal atas Proses Bisnis Pendapatan pada PT X	Metode kualitatif deskriptif, yakni evaluasi deskriptif terhadap	Kurangnya optimalisasi pengendalian internal menyebabkan kualitas data pendapatan kurang akurat, meningkatkan

			proses bisnis pendapatan	risiko kesalahan dan kecurangan dalam pencatatan pendapatan.
4	Christiandimar Firste Putrajana Pilat (2016)	Evaluasi Penerapan Sistem Pengendalian Intern Penerimaan Kas pada Perusahaan Kontraktor PT. Lumbung Berkat Indonesia	Studi kasus dengan pendekatan kualitatif	Ditemukan bahwa kurangnya pemisahan fungsi antara kas dan dana kas kecil, serta tidak adanya asuransi untuk kas yang ada di tangan, meningkatkan risiko terjadinya kecurangan dan pencurian kas.

Sumber: data diolah oleh penulis, 2025

2.6 Kerangka Pemikiran

Gambar 2.1 Kerangka Pemikiran



Sumber: gambar diolah oleh penulis, 2025