BAB II
LANDASAN TEORI

2.1 Sistem Informasi Akuntansi

2.1.1 Pengertian Sistem Informasi Akuntansi

Romney & Steinbart (2021, p. 29) suatu sistem adalah sekumpulan dua atau lebih komponen yang saling berhubungan dan berinteraksi untuk mencapai suatu tujuan, sasaran, atau memecahkan suatu masalah yang ada. Kebanyakan sistem terdiri dari subsistem yang lebih kecil kemudian sistem tersebut yang mendukung sistem yang lebih besar. Jika perusahaan atau organisasi semakin besar dan sistemnya semakin rumit, maka perusahaan tersebut semakin sulit untuk mencapai tujuan yang sudah ditentukan. Sistem memiliki tiga karakteristik yang berupa komponen, proses, dan tujuan. Komponen termasuk unsur yang bersifat terlihat (*tangible*) sedangkan proses dan tujuan tergolong sebagai unsur yang bersifat tidak terlihat (*intangible*).

Sistem yang terdapat dalam proses bisnis dikenal dengan istilah Sistem Informasi Akuntansi (SIA). Sistem Informasi Akuntansi (SIA) yang didefinisikan oleh Romney & Steinbart (2021, p. 36) merupakan sistem yang mengumpulkan, mencatat, menyimpan, dan memproses data untuk menghasilkan informasi bagi pengambil keputusan. Terdapat 6 komponen dasar yang termasuk dalam Sistem Informasi Akuntansi (SIA), yaitu:

1. Sumber daya manusia yang menggunakan sistem, diantaranya akuntan dan *top level management*.
2. Prosedur dan instruksi yang digunakan untuk mengumpulkan, memproses, dan menyimpan data berupa Standar Operasional Prosedur (SOP).
3. Data tentang organisasi dan kegiatan usahanya.
4. *Software* yang digunakan untuk mengolah data.
5. Infrastruktur teknologi informasi, termasuk komputer, perangkat *peripheral*, dan perangkat komunikasi jaringan yang digunakan dalam SIA.
6. Pengendalian Internal dan langkah-langkah keamanan yang melindungi data SIA.

Sistem Informasi Akuntansi (SIA) berperan untuk menambah nilai bisnis. Sebuah sistem dapat menjadikan suatu proses bisnis dapat lebih efektif. Dengan sistem ini, komunikasi berbagai komponen menjadi lebih teratur. Jaringan komunikasi akan menghasilkan informasi yang tepat waktu dan dapat diandalkan untuk pengambilan keputusan yang lebih baik. Oleh karena itu, melalui pengambilan keputusan yang akurat, perusahaan menjadi lebih unggul dan kompetitif.

2.1.2 Fungsi, Manfaat, dan Risiko Sistem Informasi Akuntansi

Sistem Informasi Akuntansi (SIA) melaksanakan berbagai tugas dan fungsi dalam proses bisnis. Tugas yang pertama dimulai dari pengumpulan transaksi dan data yang terkait. Data tersebut kemudian akan menjalani proses berupa pengolahan dan/atau penyimpanan untuk keperluan di masa depan. Tugas tersebut juga

merupakan salah satu fungsi dari Sistem Informasi Akuntansi (SIA) yang diuraikan oleh Romney & Steinbart (2021) yaitu:

1. Sebagai sarana pengguna mengumpulkan, memproses, dan menyimpan data aktivitas akuntansi sebuah perusahaan.
2. Sebagai objek yang membantu menjalankan kegiatan pengawasan terhadap pengguna sistem beserta data yang ada di dalamnya.
3. Membantu mengolah informasi yang dibutuhkan sebagai pertimbangan dalam proses pengambilan keputusan.
4. Memudahkan pelaksanaan dan *controlling* terhadap kegiatan pelaporan dan penyajian data keuangan.

Dari 4 fungsi yang sudah diuraikan, Romney & Steinbart (2021) juga menyimpulkan bahwa Sistem Informasi Akuntansi (SIA) memberikan manfaat yang signifikan bagi para penggunanya diantaranya:

1. Tersedianya informasi yang sistematis, akurat, dan dapat diakses sesuai kebutuhan pengguna sehingga dapat memudahkan perusahaan melakukan kegiatan bisnisnya sesuai dengan rencana.
2. Mengurangi risiko terjadinya pengeluaran tak terduga akibat kesalahan dalam mengolah data akuntansi.
3. Meningkatkan efektivitas dan efisiensi tim keuangan perusahaan dalam mengolah data keuangan perusahaan.
4. Meningkatkan kemampuan pengambilan keputusan yang berkaitan dengan kondisi keuangan perusahaan oleh divisi lain sampai dengan *top-level management*.

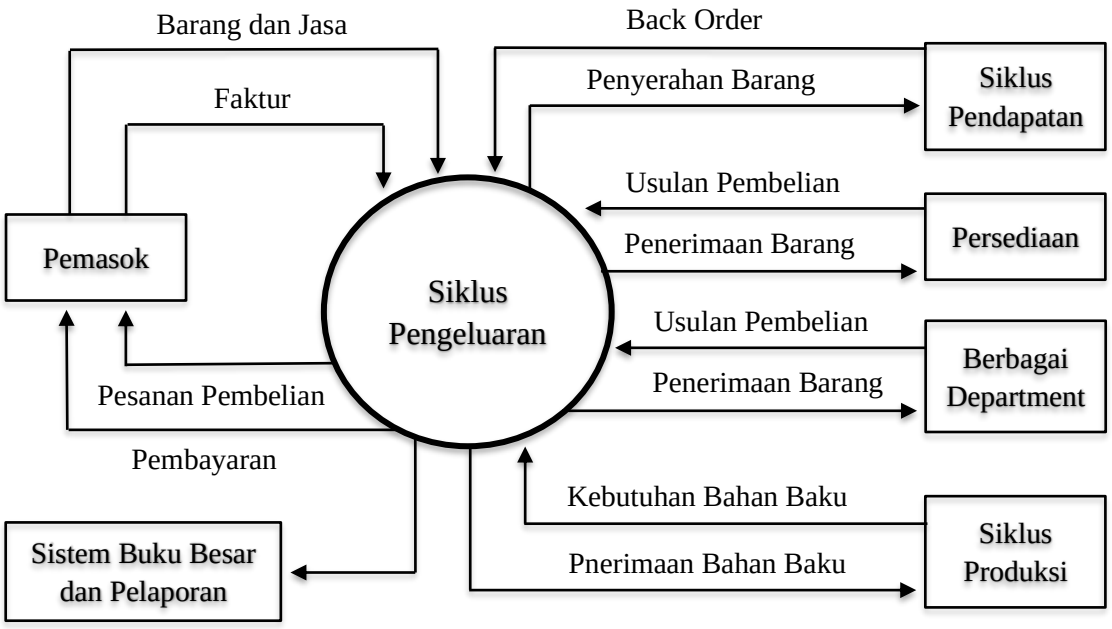
Namun selain mempelajari manfaat dan fungsi, perusahaan juga perlu mempertimbangkan risiko apa yang akan didapatkan sebelum menggunakan dan saat menggunakan SIA. Menurut Romney & Steinbart (2021, p. 335), risiko atas SIA dapat diidentifikasi melalui jenis risiko secara individual, kemungkinan terjadinya, dampaknya atas sistem, dampaknya atas unit kerja lain, dan tergolong kategori risiko inheren atau residual. Risiko inheren adalah kerentanan sistem terhadap suatu masalah apabila tidak ada usaha untuk pengendalian internal nya, sedangkan Risiko Residual adalah risiko yang masih ada dan ada kemungkinan terjadi setelah dilakukannya usaha pengendalian internal. Perusahaan wajib menilai risiko inheren terlebih dahulu, kemudian menilai kemungkinan adanya risiko residual dari rancangan sistem pengendalian internal yang sudah perusahaan susun.

2.2 Siklus Pengeluaran

2.2.1 Sistem Informasi Akuntansi Siklus Pengeluaran

Menurut Romney & Steinbart (2021, p. 34), siklus pengeluaran merupakan aktivitas bisnis dan pemrosesan informasi yang berulang dalam kegiatan pembelian dan pembayaran barang dan jasa. Istilah sederhananya siklus pengeluaran adalah suatu kegiatan yang terkait dengan pembelian inventaris dengan tujuan untuk dijual kembali atau bahan mentah dengan imbalan uang tunai atau hutang yang akan dibayar di masa depan. Tujuan utama dari siklus pengeluaran adalah untuk meminimalkan total biaya untuk memperoleh dan memelihara persediaan, serta berbagai aktivitas yang dilakukan perusahaan, seperti aktivitas pengadaan dan pemeliharaan.

2.2.2 Aktivitas Dasar Siklus Pengeluaran



Sumber: Diolah oleh penulis

Diagram diatas disebut dengan Diagram Konteks Siklus Pengeluaran. Diagram Konteks Siklus Pengeluaran merupakan diagram atau gambar yang digunakan untuk menjelaskan secara garis besar arus data dalam proses bisnis siklus pengeluaran. Jika dilihat dalam diagram konteks diatas, sebuah siklus pengeluaran melibatkan beberapa kegiatan yang berkaitan dengan pembelian bahan baku dan persediaan barang dan jasa. Kegiatan ini termasuk mengidentifikasikan dan mencatat semua pengeluaran, menyiapkan pesanan pembelian, menerima barang, dan mencatatnya sebagai persediaan. Romney & Steinbart (2021) menjelaskan terdapat 4 aktivitas dasar dalam siklus pengeluaran, yaitu:

1. *Ordering Materials, Supplies, and Services*

Aktivitas pertama yang akan dilakukan dalam siklus pengeluaran adalah memesan *inventory* atau *equipment*. Pada tahap ini perlu melibatkan mengidentifikasi apa, kapan, dan berapa banyak barang yang akan dibeli kemudian

memilih dari pemasok mana barang akan dibeli. Ada beberapa faktor yang menjadi pertimbangan ketika memilih pemasok, antara lain harga, kualitas bahan, dan kendala yang terjadi dalam melakukan pengiriman.

Setiap aktivitas dasar yang ada di dalam siklus pengeluaran memiliki risiko serta ancaman nya masing-masing. Pada aktivitas pertama yaitu pemesanan terdapat beberapa ancaman yang muncul. Ancaman umum yang kadang terjadi adalah data induk yang tidak akurat atau tidak valid. Kesalahan dalam data master pemasok dapat menyebabkan pesanan dari pemasok yang tidak disetujui, pembelian bahan baku berkualitas rendah, pengiriman terlambat, pengiriman pembayaran ke alamat yang salah, dan melakukan pembayaran palsu kepada pemasok fiktif. Untuk mengurangi risiko-risiko yang disebabkan oleh ancaman diatas, akses ke master data harus dibatasi untuk mengurangi ancaman data yang tidak akurat. Akses ke master data dapat dibatasi dengan menggunakan *username* dan *password*, sehingga hanya beberapa pegawai yang bertanggung jawab di bagian tersebut yang dapat mengakses master data.

Tabel II. 1 Ancaman dan Pengendalian Aktivitas *Ordering*

Aktivitas Pemesanan (Ordering)		
No.	**Ancaman**	**Pengendalian**
1	Data induk yang tidak akurat / tidak valid	Pembatasan akses terhadap data induk, Pengendalian integritas pemrosesan data, dan Tinjauan atas keseluruhan perubahan terhadap data induk.
2	Kehilangan / Penghancuran Data	Backup data dan melakukan prosedur pemulihan bencana
3	Kekurangan / Kelebihan Persediaan	Sistem persediaan menggunakan perpetual, Diberikan kode bar atau tabel, dan Dilakukannya stockopname secara periodik
4	Membeli Barang yang tidak dibutuhkan	Sistem persediaan menggunakan perpetual, Tinjauan dan persetujuan permintaan pembelian, dan fungsi pembelian tersentralisasi
5	Membeli Barang yang berkualitas inferior	Membeli hanya dari pemasok yang telah disetujui, Tinjauan dan Persetujuan pembelian dari pemasok baru
6	Pemasok tidak dapat diandalkan	Pembatasan akses terhadap data induk, Pengendalian integritas pemrosesan data, dan Tinjauan atas keseluruhan perubahan terhadap data induk.
7	Membeli dari pemasok yang tidak diotorisasi	Meminta pemasok memiliki sertifikat kualitas (ISO 9000) dan mengumpulkan serta mengawasi data kinerja pengiriman pemasok

Sumber: Diolah oleh penulis

2. *Receiving Materials, Supplies, and Services*

Aktivitas kedua dalam siklus pengeluaran adalah penerimaan dan penyimpanan barang pesanan. Kedua langkah tersebut memiliki proses yang berbeda karena masing-masing dilakukan oleh fungsi perusahaan yang berbeda juga. Departemen penerimaan bertanggung jawab untuk menerima pengiriman barang dari pemasok. Kemudian akan dilaporkan ke manajer gudang dan kepala departemen produksi. Departemen Penyimpanan Barang selanjutnya akan bertanggung jawab untuk menginformasikan kepada Manajer Gudang bahwa penerimaan barang pesanan harus menginformasikan kepada fungsi pengendalian persediaan. Ini dilakukan untuk memperbarui catatan inventaris.

Setelah barang sampai, penerima barang akan membandingkan nomor pesanan pembelian dengan dokumen pesanan pembelian untuk memastikan bahwa barang yang dikirim adalah barang yang dipesan. Petugas penerima kemudian akan menghitung jumlah barang yang diterima. Sebelum memindahkan barang ke gudang atau pabrik, penerima barang juga harus memeriksa setiap pengiriman untuk memastikan tidak ada barang yang rusak, barang berkualitas buruk, dan lainnya. Jika kedua kasus tersebut terjadi, departemen pembelian harus menyelesaikan situasi tersebut dengan pemasok. Hal tersebut bisa saja terjadi dan termasuk dalam ancaman/risiko yang mungkin saja terjadi pada aktivitas penerimaan, seperti pencurian persediaan. Pencurian persediaan adalah salah satu ancaman yang ada pada aktivitas penerimaan.

Beberapa prosedur pengendalian dapat digunakan untuk melindungi persediaan dari kehilangan. Pertama, persediaan harus disimpan di lokasi yang aman dengan akses terbatas, seperti di dalam ruangan yang dilengkapi dengan CCTV ataupun password untuk memasuki ruangan tersebut. Kedua, semua transfer persediaan dalam suatu perusahaan atau instansi pemerintah harus didokumentasikan antara pegawai penerimaan dan persediaan. Ketiga, penting untuk menghitung persediaan yang ada di tangan (*stock opname*) secara berkala dan mencocokan perhitungan tersebut dengan persediaan. Tahap terakhir yang dapat dilakukan dalam rangka pengendalian adalah pemisahan tugas antara yang menerima barang dengan yang menyimpan barang.

Tabel II. 2 Ancaman dan Pengendalian Aktivitas *Receiving*

Aktivitas Penerimaan (Receiving)		
No.	**Ancaman / Risiko**	**Pengendalian**
1	Menerima barang yang tidak dipesan	Mensyaratkan keberadaan pesanan pembelian yang disetujui sebelum menerima setiap pengiriman
2	Kesalahan dalam perhitungan	Melakukan insentif, mengonfigurasi sistem ERP, dan penggunaan kode batang dan label RFID
3	Memverifikasi penerimaan jasa	Pengendalian anggaran dan melakukan audit secara berkala
4	Pencurian persediaan	Pembatasan akses fisik atas persediaan, mendokumentasikan atas seluruh transfer persediaan, Melakukan stockopname secara periodik dan rekonsiliasi kuantitas

Sumber: Diolah oleh penulis

3. *Approving Supplier Invoices*

Aktivitas ketiga dalam siklus pengeluaran adalah menyetujui tagihan dari pemasok untuk dibayar. Departemen Utang akan menyetujui pembayaran faktur pemasok. Setelah menerima barang, akan ada kewajiban untuk membayar pemasok. Namun, untuk efisiensi, sebagian besar perusahaan hanya mencatat hutang dagang setelah faktur pemasok diterima dan disetujui. Kemudian ketika faktur diterima, departemen hutang harus mencocokkannya dengan pesanan pembelian dan laporan penerimaan. Kombinasi antara ketiga dokumen tersebut yang digunakan untuk pembayaran ke pemasok disebut dengan *voucher package*.

Jika terdapat kesalahan dalam aktivitas menyetujui faktur pemasok, hal tersebut bisa saja dianggap sebagai ancaman dan itu mungkin termasuk dalam kesalahan pada bagian faktur pemasok dan juga kesalahan tambahan dalam laporan keuangan dan kinerja. Kesalahan dalam faktur pemasok seringkali terjadi dalam aktivitas ini, seperti adanya ketidaksesuaian antara harga yang dicantumkan dengan harga aktual

yang dibebankan atau adanya salah hitung dari total jatuh tempo yang ada. Oleh karena itu, keakuratan matematis dari faktur pemasok harus diverifikasi dan harga serta jumlah yang tercantum di dalamnya harus dibandingkan terlebih dahulu dengan yang ditunjukkan dalam pesanan pembelian dan laporan penerimaan. Ancaman lain yang dapat terjadi adalah kesalahan dalam mencatat dan memposting pembayaran ke pemasok dapat menyebabkan kesalahan tambahan dalam pelaporan keuangan dan kinerja, yang pada akhirnya menyebabkan pengambilan keputusan yang buruk. Pengendalian dalam entri data dan kontrol pemrosesan untuk memastikan integritas pemrosesan diperlukan untuk mencegah jenis risiko/ancaman ini.

Tabel II. 3 Ancaman dan Pengendalian Aktivitas *Approving*

Aktivitas Persetujuan (Approving)		
No.	**Ancaman / Risiko**	**Pengendalian**
1	Kesalahan dalam faktur pemasok	Verifikasi atas keakuratan faktur, Mensyaratkan tanda terima secara detail, ERS, Pembatasan akses ke data induk pemasok, Verifikasi tagihan biaya pengiriman
2	Kesalahan dalam memposting ke utang	Melakukan pengendalian edit entri data, dan Rekonsiliasi catatan utang yang detail dengan GG

Sumber: Diolah oleh penulis

4. *Cash Disbursements*

Aktivitas terakhir yang ada dalam siklus pengeluaran adalah melakukan pembayaran kas kepada pemasok. Kasir memiliki tanggung jawab untuk melapor kepada bendahara dan juga membayarkannya kepada pemasok. Adanya pemisahan tugas penanggung jawab kas yang dilakukan oleh kasir, dari fungsi otorisasi dan pencatatan kas, masing-masing harus dilakukan oleh departemen pembelian dan

Departemen Utang. Lalu pembayaran dibuat ketika Departemen Utang dagang mengirimkan *voucher package* ke kasir.

Jika dalam suatu waktu pada aktivitas *cash disbursement* terdapat permasalahan dimana perusahaan membayar untuk barang yang tidak diterima. Hal tersebut bisa diklasifikasikan ke dalam risiko atau ancaman yang dapat terjadi pada aktivitas terakhir di siklus pengeluaran. Membayar barang yang pernah diterima merupakan salah satu ancaman yang mungkin terjadi dalam aktivitas terakhir pada siklus pengeluaran. Solusi terbaik untuk mengatasi ancaman ini adalah dengan membandingkan kuantitas yang tertulis pada faktur pemasok dengan kuantitas yang dimasukkan oleh pihak pengendalian persediaan yang menerima transfer barang dari bagian penerimaan. Pengendalian persediaan sangat dibutuhkan untuk memverifikasi kuantitas pada laporan penerimaan sebelum dapat digunakan untuk mendukung pembayaran faktur pemasok.

Tabel II. 4 Ancaman dan Pengendalian Aktivitas *Cash Disbursement*

Aktivitas Pengeluaran Kas		
No.	**Ancaman / Risiko**	**Pengendalian**
1	Kegagalan untuk memanfaatkan diskon bagi pembayaran tepat waktu	Pengisian faktur berdasarkan jatuh tempo untuk diskon dan adanya Anggaran arus kas
2	Pembayaran untuk barang yang tidak diterima	Mensyaratkan bahwa seluruh faktur pemasok dicocokkan dengan dokumen pendukung yang diakui baik oleh penerimaan dan pengendalian persediaan
3	Pembayaran duplikat	Kebijikan untuk membayar hanya dari salinan asli atas faktur pemasok, Mensyaratkan sebuah paket voucher yang lengkap untuk semua pembayaran
4	Pencurian kas	Keamanan fisik atas cek kosong dan mesin penandatanganan cek, Akuntansi periodik atas seluruh cek yang dinomori secara urut oleh kasir, Pengendalian akses terhadap terminal EFT

Sumber: Diolah oleh penulis

2.2.3 Proses Bisnis Pengeluaran Dalam Instansi Pemerintah

Gambar II. 1 Proses Bisnis Siklus Pengeluaran

Sumber: Modul Satker Manajemen Pembayaran Integrasi dan Koneksitas Proses

Berdasarkan Peraturan Menteri Keuangan Nomor 178/PMK.05/2018 tentang Perubahan atas Peraturan Menteri Keuangan Nomor 190/PMK.05/2012 tentang Cara Pembayaran Dalam Rangka Pelaksanaan Anggaran Pendapatan dan Belanja Negara, mekanisme pembayaran diklasifikasikan menjadi dua jenis, yaitu:

a. Pembayaran UP

Berdasarkan Peraturan Pemerintah Nomor 50 Tahun 2018, Uang persediaan adalah uang muka kerja dalam jumlah tertentu yang diberikan kepada Bendahara Pengeluaran untuk membiayai kegiatan operasional sehari-hari Satuan Kerja atau membiayai pengeluaran yang menurut sifat dan tujuannya tidak mungkin dilakukan melalui mekanisme pembayaran langsung. Pembayaran dengan UP yang dapat dilakukan oleh Bendahara Pengeluaran kepada 1 penerima/penyedia barang atau jasa paling banyak sebesar Rp50.000.000 kecuali untuk pembayaran honorarium dan perjalanan dinas. Dimana pada setiap akhir hari kerja, uang tunai yang berasal

dari UP yang harus ada pada Kas Bendahara Pengeluaran paling banyak sebesar Rp50.000.000. UP merupakan uang muka kerja yang diberikan dari Kuasa BUN kepada Bendahara Pengeluaran yang dapat dimintakan penggantian (*revolving)* dengan syarat UP yang telah digunakan, sepanjang dana yang dapat dibayarkan dengan UP masih tersedia dalam DIPA. Pergantian UP dilakukan apabila UP telah digunakan paling sedikit 50%.

Uang Persediaan (UP) dapat digunakan untuk pengeluaran-pengeluaran dari beberapa jenis belanja, antara lain:

1) Belanja Barang

Peraturan Menteri Keuangan Nomor 102/PMK.02/2018 menyatakan bahwa:

> *Belanja barang dan jasa adalah pengeluaran untuk menampung pembelian barang dan/ atau jasa yang habis pakai untuk memproduksi barang dan/ jasa yang dipasarkan maupun yang tidak dipasarkan dan pengadaan barang yang dimaksudkan untuk diserahkan atau dijual kepada masyarakat atau Pemerintah Daerah dan belanja perjalanan.*

Belanja barang meliputi belanja barang untuk kegiatan operasional dan non-operasional, pengeluaran untuk pengganti pajak dalam rangka hibah *Millenium Challenge Corporation* (MCC), belanja kontribusi pada organisasi internasional dan *trust fund*, serta belanja kontribusi pemerintah, dan belanja barang yang menghasilkan persediaan untuk kegiatan operasional maupun non-operasional. Pada saat pengajuan Uang Persediaan untuk belanja barang dalam hal pengeluaran, diperlukan dokumen-dokumen yang perlu dilengkapi sebagai syarat pengajuan antara lain Kuitansi, Surat Perintah Kerja/Kontrak, BAST, SIUP Rekanan, NPWP Rekanan, Rekening koran rekanan, Lampiran SSE Pajak. Belanja barang dan jasa diwakili dengan kode akun 52.

2) Belanja Modal

Peraturan Menteri Keuangan Nomor 102/PMK.02/2018 menjelaskan belanja modal adalah pengeluaran untuk pembayaran perolehan AT dan/ atau aset lainnya atau menambah nilai AT dan/ atau aset lainnya yang memberi manfaat lebih dari satu periode akuntansi dan melebihi batas minimal kapitalisasi AT/ aset lainnya yang ditetapkan Pemerintah. Belanja modal digunakan untuk, Belanja Modal Tanah, Belanja Modal Peralatan dan Mesin, Belanja Modal Gedung dan Bangunan, Belanja Modal Jalan, Irigasi, dan Jaringan, Belanja Modal lainnya, dan Belanja Modal BLU. Belanja modal diwakili dengan kode akun 53.

b. Pembayaran LS

Pembayaran Langsung (LS) adalah pembayaran yang dilakukan langsung kepada Bendahara Pengeluaran/penerima hak lainnya atas dasar perjanjian kerja, surat keputusan, surat tugas atau surat perintah kerja lainnya melalui penerbitan Surat Perintah Membayar Langsung. Pembayaran melalui LS dapat dilakukan oleh KPPN. Pembayaran LS dapat digunakan untuk pengeluaran-pengeluaran seperti belanja pegawai, belanja barang, belanja modal, belanja bantuan sosial, belanja pembayaran kewajiban utang, belanja subsidi, belanja hibah, dan belanja lain-lain.

2.3 Bendahara

Pada sektor publik maupun sektor komersial, terjadinya siklus pengeluaran dikelola dan dipertanggungjawabkan oleh seorang yang berwenang salah satunya adalah bendahara. Bendahara pada sektor publik terbagi menjadi dua yaitu Bendahara Penerimaan dan Bendahara Pengeluaran.

2.3.1 Definisi Bendahara

Berdasarkan UU No 1 Tahun 2004 tentang Perbendaharaan Negara, Bendahara adalah setiap orang atau badan yang diberi tugas untuk dan atas nama negara/daerah, menerima, menyimpan, dan membayar/menyerahkan uang atau surat berharga atau barang-barang negara/daerah. Pengelolaan APBN harus dilakukan oleh Pejabat Perbendaharaan Negara, yang merupakan orang yang memiliki tugas dan wewenang dalam pengelolaan keuangan yang ada pada setiap Kementerian/Lembaga sampai dengan Satuan Kerja sebagai unit terkecil mulai dari fungsi perencanaan, pelaksanaan, dan pertanggungjawaban.

Terdapat dua macam bendahara sektor publik yaitu, Bendahara Penerimaan dan Bendahara Pengeluaran. Perbedaan yang paling mendasar antara kedua jenis bendahara tersebut adalah pada pengelolaannya. Bendahara Penerimaan mengelola pendapatan sedangkan Bendahara Pengeluaran mengelola belanja.

a. Bendahara Penerimaan

Bendahara Penerimaan adalah orang yang ditunjuk untuk menerima, menyimpan, menyetorkan, menatausahakan, dan mempertanggungjawabkan uang pendapatan negara/daerah dalam rangka pelaksanaan APBN/APBD pada kantor/satuan kerja kementerian negara/lembaga/pemerintah daerah. Bendahara Penerimaan wajib menggunakan formulir SSBP/SSP/lainnya yang dipersamakan dengan SSBP/SSP untuk menyetorkan pendapatan negara ke kas negara.

b. Bendahara Pengeluaran

Bendahara Pengeluaran adalah orang yang ditunjuk untuk menerima, menyimpan, membayarkan, menatausahakan, dan mempertanggungjawabkan uang

untuk keperluan Belanja Negara dalam pelaksanaan APBN pada Kantor/Satker Kementerian Negara/Lembaga. Terdapat Bendahara Pengeluaran Pembantu yang memiliki tugas untuk membantu Bendahara Pengeluaran dalam melaksanakan pembayaran kepada yang berhak guna kelancaran pelaksanaan kegiatan tertentu.

2.4 Sistem Pengendalian Internal

2.4.1 Pengertian Sistem Pengendalian Internal

Berdasarkan Peraturan Pemerintah N0. 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah, Sistem Pengendalian Intern adalah proses yang integral pada Tindakan dan kegiatan yang dilakukan secara terus menerus oleh pimpinan dan seluruh pegawai untuk memberikan keyakinan yang efektif dan efisien, keandalan pelaporan keuangan, pengamanan aset negara, dan ketaatan terhadap peraturan perundang-undangan. Selain berdasarkan Peraturan Pemerintah, pengendalian internal ternyata juga dibahas pada tahun 1992 oleh *Committee of Sponsoring Organizations of the Treadway Commission* Amerika Serikat. Pengendalian internal menurut COSO adalah proses yang melibatkan dewan komisaris, manajemen, dan personil lain yang dirancang untuk memberikan keyakinan memadai untuk mencapai tiga tujuan yakni efektivitas dan efisiensi operasi, keandalan laporan keuangan, dan kepatuhan terhadap hukum dan peraturan yang berlaku. Walaupun memiliki pengertian dengan tata bahasa yang berbeda-beda, tetapi pengertian pengendalian internal tetap merujuk pada fokus yang sama begitupun dengan tujuannya.

2.4.2 Fungsi Pengendalian Internal

Setelah menjelaskan beberapa pendapat mengenai pengertian dan tujuan dari pengendalian internal, Romney & Steinbart (2021, p. 324.) juga mengemukakan bahwa pengendalian internal juga menjalankan tiga fungsi penting, yaitu:

1) Pengendalian Preventif (*Preventive Control*)

Pengendalian preventif merupakan salah satu pengendalian yang dirancang untuk mencegah terjadinya masalah. Entitas dapat mengambil semua tindakan pencegahan yang ada, tetapi tetap bergantung pada keputusan manajemen seperti keputusan kriteria saat merekrut pegawai, keputusan batas otorisasi atas data, dan sebagainya.

2) Pengendalian Detektif (*Detective Control*)

Pengendalian detektif ini dirancang untuk mendeteksi risiko pengendalian yang tidak dapat dihindari oleh entitas, seperti duplikat pemeriksaan perhitungan, penyusunan rekonsiliasi bank dan neraca saldo.

3) Pengendalian Korektif (*Corrective Control*)

Adanya pengendalian korektif ini ada untuk membantu entitas dalam mengidentifikasi dan memperbaiki masalah dan memulihkan keadaan entitas dari kesalahan yang dihasilkan. Contohnya termasuk memperbaiki kesalahan entri data, memelihara salinan cadangan file, dan sebagainya.

Jika Romney & Steinbart menguraikan tiga fungsi penting dalam pengendalian secara umum, maka dalam lingkungan pemerintahan setiap instansi memiliki ketentuan yang dibuat sebagai dasar dalam melakukan pengendalian internal terkait proses bisnis. Berdasarkan Peraturan Menteri Perhubungan Nomor 25 Tahun 2018

tentang Tata Cara Penyelenggaraan Sistem Pengendalian Intern Pemerintah di Lingkungan Kementerian Perhubungan Pasal 2 dijelaskan fungsi pengendalian intern di lingkungan Kementerian Perhubungan adalah untuk mencapai pengelolaan keuangan negara yang efektif, efisien, transparan dan akuntabel, Menteri melakukan pengendalian atas penyelenggaraan kegiatan pemerintahan di lingkungan Kementerian Perhubungan.

2.5 Sistem Pengendalian Intern Pemerintah

Berdasarkan Peraturan Pemerintah No. 60 Tahun 2008 Sistem Pengendalian Intern Pemerintah (SPIP) adalah proses yang integral pada tindakan dan kegiatan yang dilakukan secara terus menerus oleh pimpinan dan seluruh pegawai untuk memberikan keyakinan yang memadai atas tercapainya tujuan organisasi melalui kegiatan yang efektif dan efisien, keandalan pelaporan keuangan, pengamanan asset negara, dan ketaatan terhadap peraturan perundang-undangan. Dalam pengertian tersebut sudah dapat disimpulkan bahwa pengertian dari SPIP tersebut mengarahkan pada empat tujuan yang ingin dicapai melalui dibangunnya SPIP antara lain:

a. Kegiatan yang efektif dan efisien
b. Laporan keuangan yang dapat diandalkan
c. Pengamanan aset negara
d. Ketaatan terhadap peraturan perundang-undangan

Terbitnya Peraturan Pemerintah No. 60 Tahun 2008 tentang SPIP, selain sebagai Amanah dari reformasi di bidang keuangan negara, juga ditunjukkan untuk mengatasi permasalahan yang dihadapi oleh pemerintah. Peran sistem pengendalian

intern instansi pemerintah masih banyak diperhatikan oleh semua pihak. Hal ini mungkin disebabkan oleh sejumlah insiden terkait dengan kegagalan sistem pengendalian intern dalam pengelolaan bisnis dan pemerintah. Kelemahan penyelenggaraan sistem pengendalian intern juga bisa terjadi karena masih banyak ditemukan keterbatasan dan hambatan dalam pelaksanaannya.

Dalam pelaksanaan nya SPIP terdiri dari 5 unsur yang hampir sama dengan yang dijelaskan oleh Romney & Steinbart, yaitu

a. Lingkungan pengendalian
b. Penilaian risiko
c. Kegiatan pengendalian
d. Informasi dan komunikasi
e. Pemantauan pengendalian intern

Gambar II. 2 Keterkaitan Unsur Unsur SPIP

Sumber: Pedoman Teknis Umum Penyelenggaraan SPIP

Kelima unsur diatas saling terkait. Gambar di atas juga menjelaskan proses pengendalian dipadukan dengan tindakan dan kegiatan yang dilakukan secara terus

menerus oleh pimpinan dan seluruh pegawai. Oleh karena itu, yang menjadi fondasi kuat dari pengendalian adalah orang-orang (SDM) di dalam suatu organisasi yang membentuk lingkungan pengendalian yang baik dalam rangka mencapai visi dan misi yang ingin dicapai instansi pemerintah.

Kegiatan pengendalian atas pengelolaan sistem informasi, dilakukan untuk memastikan akurasi dan kelengkapan informasi, termasuk pengendalian umum dan pengendalian aplikasi.

1) Pengendalian Umum

Pengendalian umum berkaitan dengan seluruh aktivitas komputer, seperti yang terkait dengan rencana instansi pemerintah atas aktivitas pemrosesan data dan pemisahan fungsi. Dalam Pedoman Teknik Penyelenggaraan SPIP Sub Unsur Pengendalian Atas Pengelolaan Sistem Informasi (3.3), kegiatan yang termasuk dalam pengendalian umum meliputi:

a. Pengamanan Sistem Informasi

Jika pengendalian intern tergolong baik, sistem informasi memerlukan upaya untuk melindungi dokumen dan program dari pengungkapan yang tidak diotorisasi, serta dari kerusakan/kehancuran yang tidak disengaja. Instansi pemerintah juga harus mengidentifikasi semua kemungkinan ancaman atau bahaya terhadap peralatan dan operasi selama pemrosesan data. Setelah diidentifikasi, instansi pemerintah juga harus menyiapkan langkah-langkah mitigasi/pengendalian untuk menangani ancaman ini. Pengamanan sistem informasi sekurang-kurangnya mencakup kegiatan, pelaksanaan penilaian risiko secara berkala yang komprehensif, pengembangan rencana yang secara

jelas menggambarkan program pengamanan, serta kebijakan dan prosedur yang mendukungnya, penetapan organisasi untuk menerapkan dan mengelola rencana keamanan, dan lain-lain.

b. Pengendalian data akses

Instansi pemerintah juga harus melakukan pengendalian atas akses ke sistem komputer untuk mencegah penyalahgunaan sistem informasi dan menjaga keamanan *hardware, software*, maupun perangkat terkait lainnya dari penggunaan yang tidak sah. Oleh karena itu, hanya pegawai-pegawai tertentu yang berwenang yang dapat memasuki lingkungan sistem informasi dan mengakses sistem. Sebagai contoh, banyak instansi pemerintah yang telah menerapkan *physical security control* atau biasa disebut dengan pengendalian keamanan fisik, misalnya memakai kartu akses ruangan untuk memasuki suatu ruangan penyimpanan. Contoh penerapan lain dalam bidang ini, seperti penerapan *logical security control* atau biasa disebut dengan pengendalian keamanan logis, contoh penerapan di lapangan adalah melalui penggunaan kode akses (*password*) untuk memasuki suatu sistem jaringan komunikasi.

c. Pengendalian atas pengembangan dan perubahan perangkat lunak aplikasi

Instansi pemerintah juga harus selalu waspada dalam mengendalikan perkembangan dan perubahan perangkat lunak aplikasi, seperti kegiatan otorisasi untuk fungsi pemrosesan sistem informasi dan modifikasi program.

d. Pengendalian atas perangkat lunak sistem

Perangkat lunak sistem dapat dikontrol melalui berbagai aktivitas, seperti membatasi akses ke perangkat lunak sistem sesuai dengan otorisasi kerja dan

dan dokumentasi atas otorisasi akses, pengendalian dan pemantauan akses dan penggunaan perangkat lunak sistem, dan lain-lain.

e. Pemisahan tugas

Pemisahan tugas mensyaratkan bahwa wewenang dan tanggung jawab dalam pengelolaan sistem informasi harus secara jelas dibagi ke dalam beberapa fungsi. Hal ini dilakukan karena prosedur yang dilakukan oleh pegawai berbeda dalam sistem informasi manual dengan sistem informasi berbasis komputer mungkin akan digabung ke dalam fungsi pemrosesan pada komputer.

f. Kontinuitas pelayanan

Setiap instansi pemerintah harus memiliki rencana untuk kejadian tidak terduga, seperti bagaimana menerapkan langkah-langkah keamanan apabila terjadi kebakaran, sabotase, bencana alam, dan terorisme, untuk memastikan bahwa kegiatan pelayanan instansi tidak terganggu.

2) Pengendalian Aplikasi

Pengendalian aplikasi berkaitan erat dengan pekerjaan pemrosesan tertentu dalam fasilitas komputer yang berkaitan dengan input data, *file*, program, dan *output* aplikasi komputer tertentu, bukan sistem komputer secara umum. Tujuan dari pengendalian aplikasi adalah untuk menjaga keakuratan *output* sistem, file data, dan catatan-catatan transaksi/kejadian. Dalam Pedoman Teknik Penyelenggaraan SPIP Sub Unsur Pengendalian Atas Pengelolaan Sistem Informasi (3.3), kegiatan yang termasuk dalam pengendalian aplikasi terdiri atas:

a. Pengendalian otorisasi

Dalam pengendalian otorisasi ini, setidaknya instansi pemerintah harus melakukan pengendalian dan pengesahan terhadap dokumen sumber, membatasi akses ke terminal entri data, dan menggunakan *file* induk serta laporan khusus untuk memastikan bahwa seluruh data yang diproses diotorisasi.

b. Pengendalian kelengkapan

Pengendalian kelengkapan, dirancang untuk mengatasi sistem informasi menghasilkan laporan yang tidak lengkap, karena tidak semua data telah dimasukkan ke dalam sistem informasi.

c. Pengendalian akurasi

Pengendalian akurasi dapat dilakukan dengan penggunaan desain entri data untuk mendukung akurasi data, pelaksanaan validasi data unruk mengidentifikasi data yang salah dapat dilakukan melalui program edit pada komputer, pencatatan, pelaporan, investigasi, dan perbaikan data yang salah dengan cepat, dan reviu atas laporan keluaran untuk mempertahankan akurasi dan validitas data dapat dilakukan oleh pegawai yang mengendalikan data dan oleh pemakai laporan keuangan.

d. Pengendalian terhadap keandalan pemrosesan dan *file* data

Pengendalian terhadap keandalan pemrosesan dan *file* data, sekurang-kurangnya mencakup penggunaan prosedur yang memastikan bahwa hanya program dan *file* data versi terkini yang digunakan selama pemrosesan. Kebijakan dan prosedur ini harus tertulis dan dikomunikasikan kepada seluruh pegawai.